DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Predisposto ai sensi dell'articolo 34, comma 1, punto G) del D.Lgs 196/2003 e del suo Allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza" (art. da 33 a 36 del Codice)

Il presente documento è finalizzato a delineare l'insieme delle misure di sicurezza, organizzative, fisiche, logistiche e logiche, da adottare per il trattamento dei dati personali effettuato dal seguente Titolare:

Istituto Comprensivo Quartieri Nuovi *.con sede in Via Lanzi ANCONA Codice fiscale 93084530422*, il cui Rappresentante Legale pro-tempore è il Dirigente Scolastico Dott. Giulio Ottaviani *Codice fiscale TTVGLI52T20F496B*

Il Titolare *ha* nominato un Responsabile per la sicurezza, nella persona del sig. GIORGINI STEFANO *Codice fiscaleGRGSFN55M22F634K*, Direttore Generale dei Servizi Amministrativi, Dipendente con contratto a tempo indeterminato, di questa Amministrazione, con lettera prot. N. 2555/C1 del 11/05/2007, che ha collaborato alla stesura del presente documento e lo firma in calce insieme al Titolare.

Descrizione della sede fisica e della struttura organizzativa del Titolare:

La scuola è articolata nelle seguenti sedi, aventi le caratteristiche sotto esposte:

SEDE N. 1 - centrale sita nel comune di Ancona in via Lanzi s.n.c., dove, nella scuola secondaria di 1^ grado "Michelangelo", frequentano N. 276 alunni e lavorano N. 1 Dirigente Scolastico, N. 1 Collaboratore Vicario del Dirigente, N. 29 Docenti, N. 1 Direttore Generale dei Servizi Amministrativi, N. 5 Assistenti Amministrativi , N 4 Collaboratori Scolastici.

SEDE N. 2 - periferica : scuola primaria "Rodari" sita nel comune di Ancona in via Brecce Bianche dove frequentano N. 304 alunni e lavorano N. 36 Docenti, N. 5 Collaboratori Scolastici;

SEDE N.3 - periferica : scuola primaria "Falcone" sita nel comune di Ancona in Piazza S.d'Acquisto dove frequentano N. 206 alunni, e lavorano N. 18 Docenti, N. 2 Collaboratori Scolastici.

SEDE N.4 - periferica : scuola dell'infanzia "Primavera" sita nel comune di Ancona in Via Brecce Bianche N. 72/A dove frequentano N. 78 alunni, e lavorano N. 9 Docenti e N. 2 Collaboratori Scolastici.

SEDE N.5 - periferica : scuola dell'infanzia "Ginestra" sita nel comune di Ancona in Via Flavia dove frequentano N. 81 alunni, e lavorano N. 7 Docenti e N. 2 Collaboratori Scolastici.

SEDE N.6 - periferica : scuola dell'infanzia di Passo Varano sita nel comune di Ancona in frazione Passo Varano dove frequentano N. 77 alunni, e lavorano N. 8 Docenti e N.2 Collaboratori Scolastici.

SEDE N.7 - periferica : scuola dell'infanzia di "La Gabbianella" sita nel comune di Ancona in Via Togliatti dove frequentano N. 62 alunni, e lavorano N. 6 Docenti e N.2 Collaboratori Scolastici.

Allegati al presente documento, di cui costituiscono parte integrante:

- All. 1 : Descrizione analitica dei trattamenti di dati personali eseguiti in forma cartacea o elettronica
- All. 2 : Descrizione dei locali in cui vengono trattati dati personali e analisi dei rischi fisici
- All. 3 : Descrizione dei computer con cui vengono trattati dati (e descrizione se appartengono a reti interne chiuse e se sono collegati con l'esterno tramite Internet o la rete intranet del MIUR)
- All. 4 : Descrizione degli archivi cartacei ed elettronici esistenti e utilizzati, indicazione degli Incaricati di ciascun trattamento, analisi dei rischi fisici dei locali che li ospitano, individuazione degli archivi ad acceso controllato.
- All. 5 : Descrizione delle procedure di sicurezza utilizzate
- All. 6 : descrizioni delle comunicazioni di dati anche ai fini della verifica di legittimità e dell'adozione di apposito regolamento
- All. 7 : Mansionario delle funzioni in relazione al trattamento dei dati e piano di formazione differenziato in relazione alle funzioni stesse
- All. 8 : Piano operativo per il back-up, il Disaster Recovery, la continuità operativa
- All. 9 : Misure incrementative della sicurezza dei dati
- All. 9-2 : Misure in applicazione di Provvedimenti del Garante a carattere generale
- All. 10 : Verifica sistema di autorizzazione
- All. 11 : Relazione al Bilancio
- All. 12 : Ricognizione dei rischi riguardo Amministratori di Sistema e Assimilati
- All. 13 : Nomine Amministratori di Sistema e Assimilati
- All. 14 : Elenco Aggiornato Amministratori di Sistema e Assimilati
- All. 15 : Verifica annuale attività Amministratori di Sistema e Assimilati

INDICE

1) Elenco dei trattamenti di dati personali (regola 19.1.)

2) Distribuzione dei compiti e delle responsabilità (regola 19.2.)

3) Analisi dei rischi che incombono sui dati (regola 19.3.)

4) Misure in essere e da adottare (regola 19.4.)

5) Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5.)

6) Pianificazione degli interventi formativi previsti (regola 19.6.)

7) Trattamenti affidati all'esterno (regola 19.7.)

8) cifratura dei dati o separazione dei dati identificativi (regola 19.8)

1) Elenco dei trattamenti di dati personali (regola 19.1)

Tabella 1.1. Elenco dei trattamenti: informazioni di base.

1		2		3	4	5
Identificativo del Trattamento		**Natura dei dati trattati S**	**G**	**Struttura di riferimento**	**Altre strutture concorrenti al trattamento**	**Descrizione degli strumenti utilizzati**
Descrizione sintetica						
Tr.1	Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.	S	G	Dirigente Scolastico DSGA e Uffici di Segreteria	Collaboratori del D.S., Collaboratori scolastici, RSPP e addetti SPP, Medico Competente (se nominato)	Documenti cartacei, registri , computers e marcatempo
Tr.2	Dipendenti e assimilati:Gestione del contenzioso e procedimenti disciplinari	S	G	Dirigente Scolastico DSGA e Uffici di Segreteria		Documenti cartacei e computers
Tr.3	Organismi collegiali e commissioni istituzionali	S	G	Dirigente Scolastico DSGA e Uffici di Segreteria	Collaboratori del D.S., Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei e computers
Tr.4	Attività propedeutiche all' avvio dell'anno scolastico	S	G	Dirigente Scolastico DSGA e Uffici di Segreteria	Collaboratori del D.S., Docenti, Collaboratori scolastici,	Documenti cartacei, registri e computers
Tr.5	Attività educativa, didattica e formativa, di valutazione	S	G	Dirigente Scolastico DSGA e Uffici di Segreteria	Collaboratori del D.S., Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei, registri e computers
Tr.6	Rapporti scuola – famiglie : gestione del contenzioso	S	G	Dirigente Scolastico DSGA e Uffici di Segreteria		Documenti cartacei e computers
Tr.7	Fornitori e clienti			Dirigente Scolastico DSGA e Uffici di Segreteria	Collaboratori del D.S., Docenti nelle commissioni, Membri di organi Collegiali, Collaboratori scolastici,	Documenti cartacei e computers
Tr.8	Gestione finanziaria e contabile			Dirigente Scolastico DSGA e Uffici di Segreteria	Collaboratori del D.S.	Documenti cartacei, registri e computers
Tr.9	Gestione Istituzionale			Dirigente Scolastico DSGA e Uffici di Segreteria	Collaboratori del D.S.	Documenti cartacei, registro protocollo, e computers
Tr.10	Gestione sito web dell'istituto			Dirigente Scolastico Incaricati sito web		Documenti cartacei e computers

N.B. Per informazioni più accurate vedi allegato 1.
In questa tabella, per completezza, sono stati indicati anche i trattamenti cartacei.

Tabella 1.2. Elenco dei trattamenti con strumenti elettronici: descrizione degli strumenti utilizzati

1	2	3	4	5
Identificativo del Trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
Tr.1	Vedi Allegato 4	Vedi Allegato 4	Computer e marcatempo	Internet – rete interna
Tr.2	Solo files di testo	Vedi Allegato 4	Computer	rete interna
Tr.3	Vedi Allegato 4	Vedi Allegato 4	Computer	rete interna
Tr.4	Vedi Allegato 4	Vedi Allegato 4	Computer	Internet – rete interna
Tr.5	Vedi Allegato 4	Vedi Allegato 4	Computer	Internet – rete interna
Tr.6	Solo files di testo	Vedi Allegato 4	Computer	rete interna
Tr.7	Vedi Allegato 4	Vedi Allegato 4	Computer	Internet – rete interna
Tr.8	Vedi Allegato 4	Vedi Allegato 4	Computer	Internet – rete interna
Tr.9	Vedi Allegato 4	Vedi Allegato 4	Computer	Internet – rete interna
Tr.10	Vedi Allegato 4	Vedi Allegato 4	Computer	Internet – rete interna

Tabella 1.3

LEGENDA:
PCx=codice del computer (v.allegato 3) con i relativi codici descrittivi
es . PC03-I-R1-S**, segue il segno dei 2 punti per separarlo dal codice dell'archivio.**
AP= armadio di protezione dati + numero progressivo. Esso non raccoglie necessariamente un archivio omogeneo ma soprattutto dati, materiali, floppy disk e CD che abbisognano di un grado elevato di protezione o di archiviazione separata. Tale armadio deve disporre di serratura robusta, deve stare di regola chiuso, trovarsi preferibilmente in una stanza> ben protetta dalle intrusioni, la chiave dev'essere gestita dal Titolare, dal Responsabile (se esiste) ed eventualmente da un Incaricato responsabilizzato e che riceva adeguate istruzioni.
AE= achivio elettronico informatico + numero progressivo (es. AE03
AB= dischi di back-up di archivio elettronico informatico + numero progressivo
AD= dispositivo di Back-up
Es finale: PC03-I-R1-S:AE3 oppure AP01**:**AB21 oppure AD:AB21

LEGENDA:
Descrizione della tipologia di dato trattato:

N= Comune o neutro,
S= Sensibile
G=Giudiziario
X=Sensibile relativo a stato di salute o abitudini sessuali
P=Particolare degno di particolare protezione.
Esempio: (NSG) oppure (NSGXP)
Esempio finale : *PCx-R1-I:AE01(NSGXP)*

Tabella 1.3 Elenco delle base dati informatiche

(Trattamenti: Tr. 4, Tr.5, Tr.6, Tr.3) Anagrafica/carriera Alunni, memorizzato nel computer	PC05-I-R1-S:**AE01(NSGXP)**
(Trattamenti: Tr.5) Voti/Esami Alunni, memorizzato nel computer	PC05-I-R1-S:**AE02 (NP)**
(Trattamenti: Tr.5) Assenze Alunni, memorizzato nel computer	PC05-I-R1S:**AE03 (NSGXP)** PC08-I-R1-C:**AE03 (NSGXP)**
(Trattamenti: Tr.1) Stipendi Dipendenti:memorizzato nel computer	PC05-I-R1-S:**AE04(NSGXP)**
(Trattamenti: Tr.1) Assenze Dipendenti:memorizzato nel computer	PC05-I-R1-S:**AE05(NSGXP)**
(Trattamenti: Tr.8) Gestione Finanziaria/contabilità:memorizzato nel computer	PC05-I-R1-S:**AE06(NP)**
(Trattamenti: Tr.1, Tr.5) Gestione Orario classi/docenti:memorizzato nel computer	PC08-I-R1-C:**AE07 (NP)**
(Trattamenti: Tr.4, Tr.5) Storico Anagrafica/carriera Alunni, memorizzato in CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB01 (NSGXP)**
(Trattamenti: Tr.5) Storico Voti/Esami Alunni, memorizzato in CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB02 (NP)**
(Trattamenti: Tr.5) Storico Assenze Alunni, memorizzato in CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB03 (NSGXP)**
(Trattamenti: Tr.1) Storico Stipendi Dipendenti:memorizzato in CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB04 (NSGXP)**
(Trattamenti: Tr.1) Storico Assenze Dipendenti:memorizzato in floppy disk o CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB05 (NSGXP)**
(Trattamenti: Tr.8, Tr9) Storico Gestione Finanziaria/contabilità:memorizzato in floppy disk o CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB06 (NP)**

(Trattamenti: Tr.1, Tr.5) Storico gestione Orario classi/docenti:memorizzato nel computer	PC08-I-R1-C:**AE07 (NP)**
(Trattamenti: Tr.1, Tr4, Tr5, Tr6, Tr7,Tr8, Tr.9) Archivio Corrente Posta Elettronica:memorizzato nel computer	PC08-I-R1-C:**AE08 (NP)**
(Trattamenti: Tr.1, Tr4, Tr5, Tr6, Tr7,Tr8, Tr.9) Archivio Storico Posta Elettronica :memorizzato nel computer	PC08-I-R1-C:**AE08 (NP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Dirigente Scolastico :memorizzati nel computer	PC11-R1-C:**AE09 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di DGSA:memorizzati nel computer	PC06-R1-C:**AE10 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Lofiego G. :memorizzati nel computer	PC01-R1-C:**AE11 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Tricomi S. :memorizzati nel computer	PC02-R1-C:**AE12 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Castellucci R. :memorizzati nel computer	PC03-R1-C:**AE13 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Menghi R. :memorizzati nel computer	PC09-R1-C:**AE14 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di . Ass. Ammin. Marinelli S. :memorizzati nel computer	PC07-R1-C:**AE15 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Lucconi L. :memorizzati nel computer	PC08-R1-C:**AE16 (NSGXP)**
(Trattamenti: Tutti) Storico Documenti elettronici vari (word,excel e simili) memorizzato nel computer	Da PC01 a PC11 tranne PC05
(Trattamenti: Tr.10) Archivio Corrente sito web	PC08-R1-C:**AE17 (NP)**
(Trattamenti: Tr.10) Archivio Storico sito web	PC08-R1-C:**AE18 (NP)**
(Trattamenti: Tr.4, Tr.5, Tr.6) Back-up di Anagrafica/carriera Alunni,armadio di protezione dati	AP02**:AB01 (NSGXP)**
(Trattamenti: Tr.5) Back-up di Voti/Esami Alunni,armadio di protezione dati	AP02**:AB02 (NP)**
(Trattamenti: Tr.5) Back-up di Assenze Alunni,armadio di protezione dati	AP02**:AB03 (NSGXP)**
(Trattamenti: Tr.1) Back-up di Stipendi Dipendenti:armadio di protezione dati	AP02**:AB04 (NSGXP)**
(Trattamenti: Tr.1) Back-up di Assenze Dipendenti:armadio di protezione dati	AP02**:AB05 (NSGXP)**
(Trattamenti: Tr.8, Tr.9) Back-up di Gestione Finanziaria/contabilità:armadio di protezione dati	AP02**:AB06 (NP)**

N.B. Negli allegati ci sono ulteriori informazioni e chiarimenti

Tipologia di connessione:

nell'allegato elenco i computers aventi la lettera "R" nell'identificativo sono in rete interna; i computers aventi la lettera "I" nell'identificativo sono collegati ad Internet.

2) Distribuzione dei compiti e delle responsabilità (regola 19.2)

Tabella 2.1. Strutture preposte ai trattamenti.

1	2	3	4
Struttura:	**Responsabile:**	**Trattamenti operati dalla struttura:**	**Compiti della struttura:**
Dirigente Scolastico	Dirigente Scolastico	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate
INCARICATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE:			
Collaboratori del DS	Dirigente Scolastico	Tutti (potenzialmente)	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Segreteria	D.G.S.A.	Tutti Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Corpo Docente	Dirigente Scolastico	Tr.3, Tr.4, Tr.5, Tr.7, Tr.8, Tr.9, Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc,)
Collaboratori scolastici	D.G.S.A.	Tutti, ma con attività di supporto. Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni, docenti e familiari
Membri ESTERNI di Organi Collegiali	Dirigente Scolastico	Tr.3 e tutti gli altri (tranne Tr.6) limitatamente alle strette esigenze della funzione	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché il CDI e la GE decisioni di tipo amministrativo, finanziario, regolamentare
INCARICATI INTERNI CON COMPITI SPECIFICI O ULTERIORI:			
Incaricato del Backup periodico	Responsabile dei trattamenti in questione	Tutti, ma limitatamente alla funzione	Esegue il backup almeno settimanale degli archivi informatici contenenti dati personali. .
Custode delle chiavi degli archivi ad accesso controllato. E vice-custode delle chiavi.	Responsabile dei trattamenti in questione	Tutti i trattamenti non informatici, ma limitatamente alla funzione	E' l'unico detentore delle chiavi degli archivi ad accesso controllato e consegna all'Incaricato autorizzato all'accesso a un certo archivio la relativa chiave; la riceve di ritorno non appena cessata l'attività. Il vice lo sostituisce in caso di assenza.
Custode delle passwords	Responsabile dei trattamenti in questione	Tutti i trattamenti informatici , ma limitatamente alla funzione	Da ogni Incaricato munito di accesso al computer mediante password, ad ogni scadenza della password (3 mesi) riceve una busta chiusa contenente la password, da tenere a disposizione in caso di necessità di accesso agli archivi elettronici di quell'Incaricato quando è assente
Addetti al S.P.P.,	Dirigente Scolastico	I trattamenti relativi all'applicazione della normativa 81 o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle	Applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale

		funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e commissioni istituzionali Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	
RLS – rappresentante dei lavoratori per la sicurezza	Nessuno in questa funzione	Diritto di consultazione di tutti i documenti e materiali informatici strettamente inerenti alla funzione e risultanti come diritto di conoscenza	Contributo all'applicazione normativa Dlgs 81/08 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale; verifica ecc.
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap	Dirigente Scolastico	tutti i trattamenti informatizzati e non relativi all'attività Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	Gestione di alunni con handicap didattico grave
Incaricato della creazione e gestione del sito web	Dirigente Scolastico	i trattamenti informatici, rigorosamente nei limiti relativi alle seguenti funzioni: Tr.10 Gestione sito web dell'istituto	Creazione e gestione del sito web dell'Istituto
AMMINISTRATORE DI SISTEMA	Dirigente Scolastico	I trattamenti informatici rigorosamente nei limiti relativi alle funzioni	Creazione degli account utente con consegna delle credenziali delle credenziali, eliminazione di account non più in uso, impostazione e supervisione del backup ed esecuzione delle prove e verifiche nonché delle procedure di "disaster recovery"
RESPONSABILI INTERNI DI TRATTAMENTO:			
RESPONSABILE DI TRATTAMENTO: Direttore Servizi Generali Amm.vi	Dirigente Scolastico	Tutti i trattamenti, limitatamente alla gestione amministrativo-contabile e alla gestione delle attività dei Collaboratori Scolastici.	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
INCARICATI ESTERNI:			
RSPP	Dirigente Scolastico	I trattamenti relativi all'applicazione della normativa 81 o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e commissioni istituzionali	Applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale

		Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	
Incaricato Tecnico Esterno della Manutenzione del software e dell'Hardware e coordinatore del "Disaster recovery" e delle prove di ripristino	Dirigente Scolastico	tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni	Manutenzione dell'hardware e del software dei computers. Coordina l'impostazione del piano di recupero in caso di disastro informatico che comporti l'inagibilità del sistema o la perdita di dati personali. Coordina le prove obbligatorie di efficienza del backup e di ripristino dei dati dalla copia di salvataggio
Educatore esterno – Tirocinante	Dirigente Scolastico	i seguenti trattamenti non informatici: Tr.4 - Attività propedeutiche all' avvio dell'anno scolastico Tr.5 - Attività educativa e formativa, , rigorosamente nei limiti relativi alle funzioni	Attività di animazione ed educazione a favore degli alunni della scuola; sostegno a favore degli alunni portatori H

Ulteriori notizie sono negli allegati

3) Analisi dei rischi che incombono sui dati (regola 19.3)

Tabella 3.1. Analisi dei rischi

1		2		3
Evento		**Impatto sulla sicurezza dei dati**		**Rif .misure d'azione**
		Descrizione	Gravità stimata	
Comportamenti degli operatori	Furto delle credenziali di autenticazione	Accesso non autorizzato al computer	bassa	Istruzioni agli Incaricati (all.5), formazione, azione del "Custode delle Parole-chiave", controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate
	carenza di consapevolezza, disattenzione o incuria	Le credenziali perdono riservatezza o dati sono inutilmente resi visibili	bassa	Come precedente
	comportamenti sleali o fraudolenti	Accesso per fini personali ai dati (che però sono poco appetibili), che vengono conosciuti da Incaricati che non ne hanno diritto	bassa	Come precedente, inoltre: eventuale creazione di profili di autorizzazione diversificati e utilizzo cifratura per i rari files contenenti dati sensibili, giudiziari o particolari importanti.
	errore materiale	Cancellazione o perdita di dati	Bassa (esiste copia cartacea di tutto)	Formazione degli incaricati, profilo di autorizzazione che non consenta la formattazione dei dischi fissi o la cancellazione di files importanti. (Con l'attuale server di proprietà comunale, la funzione non è autorizzata)
Eventi relativi agli strumenti	azione di *virus* informatici o di codici malefici	Cancellazione di dati, malfunzionamenti o blocco del sistema, trasmissione casuale di dati a indirizzi di posta elettronica memorizzati, confusione con incapacità di individuare dati utili	elevata	Regolare aggiornamento dell'antivirus e del software (patches) , con istruzioni agli incaricati e monitoraggio di controllo sull'effettiva attuazione, istruzioni a individuare e prevenire le situazioni a rischio (vedi allegato 5),
	spamming (posta indesiderata e disturbante) o altre tecniche di sabotaggio	Confusione con rischio di non individuazione di messaggi utili o di loro cancellazione per errore	Medio/alta	Eventuale implementazione di un filtro antispamming, formazione degli Incaricati a riconoscere i messaggi di disturbo e a gestire le regole di assegnazione dei messaggi di posta elettronica alle varie cartelle
	malfunzionamento, indisponibilità o degrado degli strumenti	Malfunzionamenti o blocco del sistema	media	Manutenzione programmata, formazione ad individuare i sintomi di malfunzionamento per un rapido intervento, piano di backup - Distaster Recovery e di continuità operativa
	accessi esterni telematici non autorizzati	Visione indebita di dati o sabotaggio	Bassa (i dati non sono appetibili e il loro valore si basa sull'originale cartaceo)	Installazione di Firewall, con regolare aggiornamento
	intercettazione di informazioni in rete	Visione indebita di dati	minima	Eventuale adozione di cifratura o firma elettronica per proteggere i dati più gravi (allo studio)
Eventi relativi	accessi non autorizzati	Sabotaggio delle	Sabotaggio:	Solidità degli infissi dei locali, chiusura

al contesto	a locali/reparti ad accesso ristretto	macchine, con eventuale perdita di dati; accesso abusivo se le credenziali fossero lasciate disponibili	media Altro: bassa	a chiave quando non presidiati, installazione di allarme antifurto, eventuali estintori ad anidride carbonica per non danneggiare i computers (disponibilità Ente Locale), istruzioni a tutti gli operatori (v. all. 5)
	asportazione e furto di strumenti contenenti dati	Perdita di dati , rallentamento o blocco dell'attività per carenza di computer	Probabilità media, gravità elevata	Come punto precedente, Inoltre, regolare back-up dei dati, piano di back-up - Distaster Recovery e di continuità operativa
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati , rallentamento o blocco dell'attività per carenza di computer	Probabilità minima, gravità massima	Come punto precedente, [allarme antincendio],inoltre sensibilizzazione e formazione degli Incaricati e dei Collaboratori Scolastici. Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti (già eseguita). Uso di protezioni antifulmine e contro sovratensioni elettriche (previsto [già attuato]). Verifica della logistica degli apparecchi e del loro corretto posizionamento. Custodia dei dischi di back-up in armadio chiuso
	guasto ai sistemi complementari (impianto elettrico)	Perdita di dati e blocco del sistema	media	Gruppo di continuità (già installato)
	guasto ai sistemi complementari (climatizzazione)	Surriscaldamento dei computers e in particolare della scheda madre o altre componenti, con possibilità di guasto	bassa	Allo studio una miglior ventilazione dei computers (revisione regolare delle ventole interne e loro potenziamento). Verifica della logistica degli apparecchi e del loro corretto posizionamento.
	errori umani nella gestione della sicurezza fisica	Danni agli strumenti, con possibile perdita di dati e malfunzionamenti	media	Formazione e sensibilizzazione di tutti gli Incaricati, compresi Operatori delle pulizie e Collaboratori .Scolastici per il controllo. Verifica della logistica degli apparecchi e del loro corretto posizionamento.

4) Misure in essere e da adottare (regola 19.4).

Tab. 4.1. Le misure di sicurezza adottate o da adottare

Nell'allegato 9 sono indicate ulteriori misure da adottare

1	2	3	4	5	6	7	8
Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Rif. scheda analitica	Misura già in essere (con data di effettività)	Misura da adottare (con data di effettività prevista)	Periodicità e responsabilità dei controlli
Istruzioni agli Incaricati (all.5)	Comportamenti inadeguati o errati degli operatori, incuria, ecc. : Furto delle credenziali di autenticazione ; carenza di consapevolezza, disattenzione o incuria; comportamenti sleali o fraudolenti; azione di *virus* informatico o di codici malefici *spamming (posta indesiderata e disturbante)* o altre tecniche di sabotaggio malfunzionamento, indisponibilità o degrado degli strumenti accessi esterni telematici non autorizzati intercettazione di informazioni in rete errore materiale	Tutti	Tutte	Allegato 5	Ottobre-Nov2004 Marzo 2008 Gennaio 2010		mensile Titolare/ Responsabile,
formazione		idem	idem	All. 6	Nov-Dic 2004 marzo 2008 Aprile 2008 Settembre 2010	Maggio 2011	annuale Titolare/ Responsabile,
azione del "Custode delle Parole-chiave",		Trattamenti con dati sensibili o giudiziari (da Tr1 a Tr6).	idem				mensile Titolare/ Responsabile,
controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate		Idem	idem	All.2	Ottobre 2004 marzo 2008 gennaio 2010		mensile Titolare/ Responsabile,
eventuale creazione di profili di autorizzazione diversificati		Non adottato	idem				
Utilizzo di files cifrati per i rari files contenenti dati sensibili, giudiziari o particolari importanti.		Non adottato					
profilo di autorizzazione che non consenta la formattazione dei dischi fissi o la cancellazione di files importanti.		Non adottato	Idem				
Regolare aggiornamento dell'antivirus e del software (patches) : istruzioni agli incaricati	Eventi relativi agli strumenti: azione di *virus* informatici o di codici malefici; *spamming*	Tutti	tutte	All. 5	Ottobre 2004	Aprile 2011	mensile Titolare/ Responsabile,
istruzioni a individuare e prevenire le situazioni a rischio (vedi allegato 5)		Idem	idem	All. 5	Dic 2004 Gennaio 2010		semestrale Titolare/Responsabile,

Eventuale implementazione di un filtro antispamming	*(posta indesiderata e disturbante)* o altre tecniche di sabotaggio; malfunzionamento, indisponibilità o degrado degli strumenti; accessi esterni telematici non autorizzati; intercettazione di informazioni in rete	idem	idem				semestrale Titolare/Responsabile,
formazione degli Incaricati a riconoscere i messaggi di disturbo e a gestire le regole di assegnazione dei messaggi di posta elettronica alle varie cartelle		idem	idem	All. 5	Gennaio 2005 Gennaio 2010		semestrale Titolare/Responsabile,
Manutenzione programmata		idem	idem				semestrale Titolare/Responsabile,
Formazione ad individuare i sintomi di malfunzionamento per un rapido intervento		idem	idem		Gennaio 2005 Gennaio 2010		annuale Titolare/Responsabile,
piano di backup - Distaster Recovery e di continuità operativa		idem	idem	All. 8	Maggio 2005 Gennaio 2010	Maggio 2011	semestrale Titolare/Responsabile,
Installazione di Firewall, con regolare aggiornamento		idem	idem		Settembre 2004		semestrale Titolare/ Responsabile,
Eventuale adozione di cifratura o firma elettronica per proteggere i dati più gravi (allo studio)		Non adottato	Non adottato		Non dovuto	Non dovuto	
Verifica ed eventuale miglioramento della solidità degli infissi dei locali	Eventi relativi al contesto: accessi non autorizzati a locali/reparti ad accesso ristretto; asportazione e furto di strumenti contenenti dati; eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria; guasto ai sistemi complementari (impianto elettrico); guasto ai sistemi complementari (climatizzazione); errori umani nella gestione della sicurezza fisica	Tutti	Tutti	All. 1	Settembre 2004		semestrale Titolare/ Responsabile
Chiusura a chiave dei locali quando non presidiati : istruzioni a tutti gli operatori		idem	idem	All. 5	Gennaio 2004 Gennaio 2010		mensile Titolare/ Responsabile,
installazione di allarme antifurto		idem	idem		2000		annuale Titolare /Responsabile,
disponibilità di estintori ad anidride carbonica per non danneggiare i computers		idem	idem			Secondo disponibilità del Comune	annuale Titolare/ Responsabile,
Regolare back-up dei dati, piano di back-up - Distaster Recovery e di continuità operativa		idem	idem		Luglio 2007		mensile Titolare/ Responsabile,
Custodia dei dischi di back-up in armadio chiuso.		idem	idem		Gennaio 2004		semestrale Titolare/ Responsabile,
Sensibilizzazione e formazione degli Assistenti Amministrativi e dei Collaboratori Scolastici		idem	idem	All. 5	Nov-dic 2005 Marzo 2008 Settembre 2009		mensile Titolare/ Responsabile,
Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti		idem	idem		Settembre 2004		annuale Titolare/ Responsabile,
Uso di protezioni antifulmine e contro sovratensioni elettriche		idem	idem			Secondo disponibilità del Comune	annuale Titolare,/ responsabile,
Verifica della logistica degli apparecchi e del loro corretto posizionamento.		idem	idem		Gennaio 2005 Gennaio 2010		semestrale Titolare/ Responsabile,
Gruppo di continuità		idem	idem		2000		annuale Titolare/ responsabile,
Studio una miglior ventilazione dei computers (revisione regolare delle ventole interne e loro potenziamento).		idem	idem				annuale Titolare/ Responsabile,
Formazione e sensibilizzazione di tutti gli Incaricati, compresi Operatori delle pulizie e Collaboratori .Scolastici per il controllo.		idem	idem		Dicembre 2005 Marzo2008 Settembre 2009		mensile Titolare/ Responsabile,

Nuove misure incrementative della sicurezza:							
Soluzioni incrementative della sicurezza (vedi allegato 9)	Rischi fisici	idem	idem			Secondo disponibilità finanziaria	Mensile Titolare Responsabile
Soluzioni incrementative della sicurezza (vedi allegato 9)	Rischi sicurezza dati	idem	idem			Idem	mensile Titolare Responsabile,
Soluzioni incrementative della sicurezza (vedi allegato 9)	Rischi sistemi di supporto.	idem	idem			idem	mensile Titolare/ Responsabile,

5) Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

Tab. 5.1.- Back-up archivi elettronici

1		2	3	4	5
Salvataggio					
Data base		Dati sensibili o giudiziari contenuti	Criteri individuati per il salvataggio (procedure operative in essere)	Ubicazione di conservazione delle copie	Struttura operativa incaricata del salvataggio
(Trattamenti: Tr. 4, Tr.5, Tr.7, Tr.3) Anagrafica/carriera Alunni, memorizzato nel computer	PC05-R1-S:**AE01**	SG	Back-up ogni settimana, su dischi alternati bisettimanalmente in modo da utilizzare supporti diversi da quelli utilizzati la volta precedente (vedi allegato 8)	Stanza: 1,2	Segreteria
(Trattamenti: Tr.5) Voti/Esami Alunni, memorizzato nel computer	PC08-R1-C:**AE02**	SG	idem	Stanza: 1,4	idem
(Trattamenti: Tr.5) Assenze Alunni, memorizzato nel computer	PC05-I-R1-S:**AE03**	SG	idem	Stanza 1,2	idem
(Trattamenti: Tr.1) Stipendi Dipendenti:memorizzato nel computer	PC05-I-R1-S:**AE04**	SG	idem	Stanza: 1,2	Segreteria
(Trattamenti: Tr.1) Assenze Dipendenti:memorizzato nel computer	PC05-I-R1-S:**AE05**	SG	idem	Stanza: 1,2	Segreteria
(Trattamenti: Tr.8) Gestione Finanziaria/contabilità:memorizzato nel computer	PC05-I-R1-S:**AE06**	SG	idem	Stanza: 1,2	Segreteria
(Trattamenti: Tr.1, Tr.5) Gestione Orario classi/docenti:memorizzato nel computer	PC08-I-R1-C:**AE07**		idem	Stanza: 1,4	Segreteria
(Trattamenti Tr.1, Tr.2,Tr.3, Tr.4, Tr.5, Tr.6, Tr.7, Tr.8, Tr.9) Gestione della posta elettronica	PC06-08-R1**AE10**	SG	Idem	Stanza: 1.2	Segreteria

Tab. 5.2. PIANIFICAZIONE PROVE DI RIPRISTINO DEI DATI

1	1 bis	2	3
Rispristino			
Data base/archivio		Scheda operativa	Pianificazione delle prove di ripristino
(Trattamenti: Tr. 4, Tr.5, Tr.6, Tr.3) Anagrafica/carriera Alunni, memorizzato nel computer	PC05-I-R1-S:**AE01**	V. allegato 8	Maggio 2011
(Trattamenti: Tr.5) Voti/Esami Alunni, memorizzato nel computer	PC05-I-R1-S:**AE02**	V. allegato 8	Maggio 2011
(Trattamenti: Tr.5) Assenze Alunni, memorizzato nel computer	PC05-I-R1-S:**AE03**	V. allegato 8	Maggio 2011
(Trattamenti: Tr.1) Stipendi Dipendenti:memorizzato nel computer	PC05-I-R1-S:**AE04**	V. allegato 8	Maggio 2011
(Trattamenti: Tr.1) Assenze Dipendenti:memorizzato nel computer	PC05-I-R1-S:**AE05**	V. allegato 8	Maggio 2011
(Trattamenti: Tr.8) Gestione Finanziaria/contabilità:memorizzato nel computer	PC05-I-R1-S:**AE06**	V. allegato 8	Maggio 2011
(Trattamenti: Tr.1, Tr.5) Gestione Orario classi/docenti:memorizzato nel computer	PC05-I-R1-S:**AE07**	V. allegato 8	Maggio 2011

6) Pianificazione degli interventi formativi previsti (regola 19.6)

Tab. 6.1

INCARICATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE:	**Formazione prevista tra il 31.03.2010 e il 31.3.2011**
Collaboratori del DS	Numero persone da formare: 0 Numero di persone già formate: 2. E già stato fornito il <Kit formazione privacy>, manuale completo divulgativo sulla privacy, consultabile a video, anche navigando tra files, e stampabile. ***Sarà comunque effettuata una formazione su le nuove misure minime di sicurezza nella gestione e cancellazione dei supporti informatici (Provvedimento a carattere generale del garante, ottobre 2008): è stato acquisito il kit Cod. 185 comprendente un corso di formazione illustrato.***.
Segreteria	Numero persone da formare e aggiornare: 0 Numero di persone già formate: 5 E' la categoria che ha le maggiori esigenze di formazione (dando per scontato che il Titolare e il Responsabile provvedano alla propria formazione, frequentando corsi o studiando libri e dispense). Essendo state emanate nell'ultimo anno dal Garante Privacy le <"LINEE GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI DI LAVORATORI PER FINALITÀ DI GESTIONE DEL RAPPORTO DI LAVORO IN AMBITO PUBBLICO" > e le < LAVORO: LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET> si ritiene di progettare una specifica formazione per il Dirigente e la Segreteria. Lo strumento formativo sarà costituito dai due opuscoli di illustrazione delle due linee guida. Ogni membro della segreteria riceverà il materiale illustrativo e poi verranno tenute almeno 2 riunioni tematiche introdotte dal DSGA. **Periodo:** maggio 2011 e novembre 2011 Vengono inoltre forniti: **1)** manuale completo divulgativo sulla privacy, consultabile a video, anche navigando tra files, e stampabile. **2) Per il DSGA e gli Assistenti Amministrativi che si occupano di personale:** **formazione sulle prescrizioni del Garante in materia di gestione dei dipendenti. Trattasi di:** **a) Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico - 14 giugno 2007 (G.U. 13 luglio 2007, n. 161)** **b) Lavoro: le linee guida del Garante per posta elettronica e internet (Gazzetta Ufficiale n. 58 del 10 marzo 2007)** **Sull'argomento è stato *già acquisito un manuale per applicarlo operativamente***
Corpo Docente	Numero persone da formare: 37 Numero di persone già formate: 82 Nel corso delle periodiche riunioni degli Organi Collegiali il Titolare illustrerà l'argomento e se ne potrà discutere. Si inviterà anche un esperto per una breve relazione. Il tema principale sarà le novità e soprattutto le nuove chiarezze introdotte dal <Regolamento dati sensibili> in vigore dal 2007. Si approfondirà in particolare il tema: "Dati sensibili: è vietato chiedere agli alunni dati sensibili che non siano strettamente indispensabili per l'attività formativa." **Periodo:** maggio 2011 e novembre 2011 Si prenderà in esame anche IL VADEMECUM DEL GARANTE PRIVACY SULLA SCUOLA. E' prevista la distribuzione all'inizio del prossimo anno scolastico (settembre-ottobre) di unl facsimile del VADEMECUM
Collaboratori scolastici	Numero persone da formare: 3 Numero di persone già formate: 16 Viene fornito il <Compendio di livello base > della normativa privacy. Ma soprattutto si farà affidamento su alcune riunioni con illustrazione del tema fatta in modo semplice ed elementare da parte del Titolare o del DGSA.. **Periodo:** maggio 2011 e novembre 2011
Membri ESTERNI di Organi Collegiali	Numero persone da formare: 88 Numero di persone già formate: 0 Viene fornito il <Compendio di livello base > della normativa privacy. Nel corso delle periodiche riunioni degli Organi Collegiali il Dirigente illustrerà brevemente l'argomento e se ne potrà discutere. Si inviterà anche un esperto per una breve relazione. **Periodo:** maggio 2011 e novembre 2011
INCARICATI INTERNI CON COMPITI	

SPECIFICI O ULTERIORI:	
Incaricato del Backup periodico	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Custode delle chiavi degli archivi ad accesso controllato. E vice-custode delle chiavi.	[x] Già formato [ ] Da formare] E' previsto un breve colloquio con il DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Custode delle passwords	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Addetti al S.P.P.	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap	Numero persone da formare: 6 Numero di persone già formate: 6. E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e settembre 2011
Incaricato esterno per la creazione e gestione del sito web	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il Dirigente o del DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
AMMINISTRATORE DI SISTEMA	x] Già formato [ ] Da formare E' previsto un breve colloquio con il DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 201
RESPONSABILI INTERNI DI TRATTAMENTO:	
RESPONSABILE DI TRATTAMENTI: Direttore Servizi Generali Amm.vi [se nominato]	[x] Già formato [ ] Da formare Viene fornito il <Kit formazione privacy>, manuale completo divulgativo sulla privacy, consultabile a video, anche navigando tra files. E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
INCARICATI ESTERNI:	
RSPP	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Incaricato Tecnico Esterno della Manutenzione del Software	[x] Già formato [] Da formare E' previsto un breve colloquio con il Dirigente o del DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Incaricato Tecnico Esterno della Manutenzione del dell'Hardware	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il Dirigente o del DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Docente o animatore Esterno [se esistente]	[ ] Già formato [x] Da formare Viene fornito il <Compendio di livello base > della normativa privacy (uno dei files del <Kit formazione privacy>) E' previsto un breve colloquio con il Dirigente o del DSGA per verifica e approfondimento. **Periodo:** al momento dell'incarico

N.B. Gli interventi formativi sono meglio descritti nell'allegato 7

7) Trattamenti affidati all'esterno (regola 19.7)

Tab. 7.1.

Attività esternalizzata	Descrizione sintetica	Dati personali , sensibili o giudiziari interessati	Soggetto esterno	Descrizione dei criteri per l'adozione delle misure
Nessuna				

-

8) Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

(Non riguarda la scuola, ma solo gli esercenti le professioni sanitarie).

Dichiarazioni finali e di impegno

Si è proceduto a effettuare la prescritta verifica almeno annuale dei profili di autorizzazione assegnati a Incaricati e Responsabili (Vedi documentazione in allegato 10).

Dell'avvenuta redazione del presente documento e delle politiche per la sicurezza verrà data comunicazione in sede di approvazione del bilancio consuntivo e apparirà nella relazione accompagnatoria dello stesso (come da previsione contenuta nell'allegato 11)

Obiettivo di questo Istituto è incrementare la sicurezza dei dati su supporto sia informatico che cartaceo e dei relativi archivi, pertanto si è proceduto ad un'attenta verifica delle condizioni di sicurezza degli archivi, in particolare quelli, separati o meno, contenenti dati sensibili/giudiziari. A seguito dell'analisi, saranno effettuati interventi incrementativi della sicurezza. Di questi propositi c'è previsione più accurata negli allegati di questo documento.

31 marzo 2011 Firma del Titolare _____

Firma del Responsabile _____

Assunta al protocollo dell'Istituto in data 31 MARZO 2011 col numero 1696/A3

Allegato 1 - Elenco dei trattamenti di dati personali

eseguiti in forma cartacea o elettronica (art. 19 punto 1 del dell'allegato B) e delle modalità di raccolta, di trattamento, di conservazione e di comunicazione o diffusione

Le schede che seguono SONO ISPIRATE ESATTAMENTE AL "Regolamento dati sensibili e giudiziari" approvato dal MPI per tutte le scuole statali.

Ogni scheda rappresenta la classificazione di un certo trattamento (o gruppo di trattamenti consimili).
Le prime 5 schede sono desunte esattamente dal predetto Regolamento (la sesta nel regolamento è trattata con il numero 7), con un unico ampliamento che si troverà nella scheda 3

In ogni scheda sono indicati chiaramente i tipi di dati che possono essere lecitamente trattati e quali operazioni possono essere lecitamente eseguite. Delle comunicazioni di dati sensibili o giudiziari, che è questione più complessa, si occuperà, invece, l'"Allegato 6 – Comunicazioni di dati".

I trattamenti classificati dal numero 7 al numero 10 non sono presenti nel Regolamento, perché non implicano uso di dati sensibili o giudiziari, ma solo di dati comuni. Era però necessario avere anche queste ulteriori categorie per classificare tutti i trattamenti effettivamente svolti.

Indice:

Tr.1	**Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.**
Tr.2	**Dipendenti ed assimilati :Gestione del contenzioso e procedimenti disciplinari**
Tr.3	**Organismi collegiali e commissioni istituzionali**
Tr.4	**Attività propedeutiche all' avvio dell'anno scolastico**
Tr.5	**Attività educativa, didattica e formativa, di valutazione**
Tr.6	**Rapporti scuola – famiglie : gestione del contenzioso**
Tr.7	**Fornitori e clienti**
Tr.8	**Gestione finanziaria e contabile**
Tr.09	**Gestione Istituzionale**
Tr.10	**Gestione sito web dell'istituto**

Tr.1 - Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.

Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente, dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato (Il trattamento concerne tutti i dati, anche sensibili e giudiziari, in alcuni casi anche di familiari o terzi, relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro) (vedi Scheda 1 del <Regolamento> di cui al Decreto n. 305/2006 approvato dal M.P.I.)

TIPI DI DATI TRATTABILI (solo se assolutamente indispensabili per fini strettamente istituzionali !):

DATI COMUNI [X] **DATI PARTICOLARI** [X] **DATI SENSIBILI:**

CONVINZIONI [X] **religiose** [X] **filosofiche** [X] **sindacali** [X] **d'altro genere**
STATO DI SALUTE [X] **patologie attuali** [X] **patologie pregresse** [X] **terapie in corso** [X] **dati sulla salute relativi anche ai familiari**
VITA SESSUALE [X] (solo in caso di rettificazione di attribuzione di sesso)
DATI DI CARATTERE GIUDIZIARIO (Art. 4, comma 1, lett. E), del Codice) [X]

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: [X] presso gli interessati [X] presso terzi
ELABORAZIONE: [X] in forma cartacea [X] con modalità informatizzate
Registrazione [X], **Organizzazione** [X], **conservazione** [X], **consultazione** [X], **modificazione** [X], **selezione** [X], **estrazione** [X], **utilizzo** [X], **blocco** [X], **cancellazione** [X] **distruzione** [X]
Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: solo nei casi previsti dal Regolamento MPI per questo trattamento (vedi elenco tra poche righe*)

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI , tranne i casi obbligatori per legge, ma con particolari accorgimenti (esempio graduatorie, ma sostituendo la notazione <portatore di handicap> con un codice; il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione degli altri dati sensibili e dei dati giudiziari: solo se previsto espressamente da norme di legge o regolamento e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

INTERCONNESSIONI E RAFFRONTI DI DATI CON ALTRO TITOLARE: Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;

(*) **Destinatari consentiti per comunicazioni di dati sensibili:**

- **Amministrazioni certificanti** in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000 (in questo caso sono consentiti anche l'INTERCONNESSIONI e il RAFFRONTI DI DATI CON ALTRO TITOLARE)
- **Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;**
- Organi preposti al riconoscimento della **causa di servizio/equo indennizzo**, ai sensi del D.P.R, n. 29 ottobre 2001, n. 461.(Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermita' da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonche' per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie)

- Organi preposti alla **vigilanza in materia di igiene e sicurezza sui luoghi di lavoro** (d.lg. n. 626/1994 [*non allegata perché comunque notissima*]– norme in materia di prevenzione e sicurezza nei luoghi di lavoro.
- **Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza** a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o **infortuni sul lavoro a**i sensi del D.P.R. n. 1124/1965 (testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali).
- Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della Legge 12 marzo 1999, n. 68 (Norme per il diritto al lavoro dei disabili) Norme per il diritto al lavoro dei disabili
- **Organizzazioni sindacali** per gli adempimenti connessi al **versamento delle quote di iscrizione e per la gestione dei permessi sindacali;**
- Pubbliche Amministrazioni presso *le* quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- **Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica** ai sensi della Legge 18 luglio 2003, n. 186 (Norme sullo stato giuridico degli insegnanti di religione cattolica degli istituti e delle scuole di ogni ordine e grado).
- **Organi di contro**llo (Corte dei Conti e MEF): al fine dei controllo di legittimità e annotazione della spesa **dei provvedimenti di stato giuridico ed economico del personale** ex Legge 14 gennaio 1994, n. 20 (Disposizioni in materia di giurisdizione e controllo della Corte dei Conti.) e D.P.R. 20 febbraio 1998, n. 38 (Regolamento recante le attribuzioni dei dipartimenti del ministero del tesoro, del bilancio e della programmazione economica, nonche' disposizioni in materia di organizzazione e di personale, a norma dell'articolo 7, comma 3, della legge 3 aprile 1997, n. 94)
- **Agenzia delle Entrate: ai fini degli obblighi fiscali del personale** ex:

  - Legge 30 dicembre 1991, n. 413 (disposizioni per ampliare le basi imponibili, per razionalizzare, facilitare e potenziare l'attività di accertamento; disposizioni per la valutazione obbligatoria dei beni immobili delle imprese, nonché per riformare il contenzioso e per la definizione agevolata dei rapporti tributari pendenti; delega al presidente della repubblica per la concessione di amnistia per reati tributari; istituzioni dei centri di assistenza fiscale e del conto fiscale);

  - MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335 (Riforma del sistema pensionistico obbligatorio e complementare).
- **Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive** (art. 50, comma 3, D.Lgs.30 marzo 2001, n. 165 - Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche. Il comma 3 recita: << 3 . Le amministrazioni pubbliche sono tenute a fornire alla Presidenza del Consiglio dei ministri - Dipartimento della funzione pubblica - il numero complessivo ed i nominativi dei beneficiari dei permessi sindacali.>>).

Tr.2 - DIPENDENTI E ASSIMILATI: Gestione del contenzioso e procedimenti disciplinari

Gestione del contenzioso e procedimenti disciplinari (Il trattamento concerne tutti i dati, anche sensibili e giudiziari, necessari o indispensabili alle attività relative alla difesa in giudizio nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili) (vedi Scheda 2 del <Regolamento> di cui al Decreto n. 305/2006 approvato dal M.P.I.)

TIPI DI DATI TRATTABILI solo se assolutamente indispensabili per fini strettamente istituzionali !):

DATI COMUNI X **DATI PARTICOLARI** X **DATI SENSIBILI:**

ORIGINE X **razziale** X **etnica**

CONVINZIONI X **religiose** X **filosofiche** X **politiche** X **sindacali** X **d'altro genere**
STATO DI SALUTE X **patologie attuali** X **patologie pregresse** X **terapie in corso** X **dati sulla salute relativi anche ai familiari**
VITA SESSUALE X
DATI DI CARATTERE GIUDIZIARIO (Art. 4, comma 1, lett. E), del Codice) X

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: X presso gli interessati X presso terzi
ELABORAZIONE: X in forma cartacea X con modalità informatizzate
Registrazione X**, Organizzazione** X**, conservazione** X**, consultazione** X**, modificazione** X**, selezione** X**, estrazione** X**, utilizzo** X**, blocco** X**, cancellazione** X **distruzione** X
Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: solo nei casi previsti dal Regolamento MPI per questo trattamento (vedi elenco tra poche righe*)

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI , tranne i casi obbligatori per legge, ma con particolari accorgimenti (esempio graduatorie, ma sostituendo la notazione <portatore di handicap> con un codice; il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione degli altri dati sensibili e dei dati giudiziari: solo se previsto espressamente da norme di legge o regolamento e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

(*) **Destinatari consentiti per comunicazioni di dati sensibili:**

- Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento **dei tentativi obbligatori di conciliazione** dinanzi a Collegi di conciliazione ex D.Lgs.30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.);
- **Organi arbitrali: per le svolgimento delle procedure arbitrali ai sensi dei CCNL dì settore**;
- **Avvocature dello Stato**: per la difesa erariale e consulenza presso gli organi di giustizia;
- **Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria: per l'esercizio dell'azione di giustizia;**
- **Liberi professionisti, ai fini di patrocinio o di consulenza**, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudIziale.

Tr.3 - Organismi collegiali e commissioni istituzionali

Organismi collegiali e commissioni istituzionali (Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali. Il trattamento concerne tutti i dati, anche sensibili, in alcuni casi anche di familiari o terzi, necessari o indispensabili per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme dell'ordinamento scolastico, nonché i dati comuni necessari alla gestione di tali organismi.) (vedi Scheda 3 del <Regolamento> di cui al Decreto n. 305/2006 approvato dal M.P.I., relativa alla sola attivazione di tali organismi)

<<Il trattamento dei dati sensibili è necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del MIUR e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali. Il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentati delle organizzazioni sindacali.>>. Come si vede abbiamo aggiunto la <gestione> di tali organi, la quale non ha, eprò, l'autorizzazione a tartare dati sensibili, che è lecito trattare solo <per attivare gli organismi collegiali e le commissioni istituzionali>]

TIPI DI DATI TRATTABILI solo se assolutamente indispensabili per fini strettamente istituzionali !):

DATI COMUNI [X] **DATI PARTICOLARI** [X] **DATI SENSIBILI:**

CONVINZIONI [X] **sindacali (trattabili esclusivamente per attivare tali organismi o commissioni)**

DATI DI CARATTERE GIUDIZIARIO (Art. 4, comma 1, lett. E), del Codice) [X] (trattabili esclusivamente per attivare tali organismi o commissioni)

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: [X] presso gli interessati [X] presso terzi
ELABORAZIONE: [X] in forma cartacea [X] con modalità informatizzate
Registrazione [X]**, Organizzazione** [X]**, conservazione** [X]**, consultazione** [X]**, modificazione** [X]**, selezione** [X]**, estrazione** [X]**, utilizzo** [X]**, blocco** [X]**, cancellazione** [X] **distruzione** [X]
Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: NO

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI , tranne i casi obbligatori per legge, ma con particolari accorgimenti (esempio graduatorie, ma sostituendo la notazione <portatore di handicap> con un codice; il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione degli altri dati sensibili e dei dati giudiziari: solo se previsto espressamente da norme di legge o regolamento e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Tr.4 - Attività propedeutiche all' avvio dell'anno scolastico

Attività propedeutiche all' avvio dell'anno scolastico (Il trattamento concerne tutti i dati, necessari o indispensabili, in alcuni casi anche di familiari o terzi, forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio oppure forniti ad altre istituzioni scolastiche per le stesse finalità)

TIPI DI DATI TRATTABILI solo se assolutamente indispensabili per fini strettamente istituzionali !):

DATI COMUNI [X] **DATI PARTICOLARI** [X] **DATI SENSIBILI:**

ORIGINE [X] **razziale** [X] **etnica**

CONVINZIONI [X] **religiose** [X] **d'altro genere**

STATO DI SALUTE [X] **patologie attuali** [X] **patologie pregresse** [X] **terapie in corso** [X] **dati sulla salute relativi anche ai familiari**

DATI DI CARATTERE GIUDIZIARIO (Art. 4, comma 1, lett. E), del Codice) [X]

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: [X] presso gli interessati [X] presso terzi
ELABORAZIONE: [X] in forma cartacea [X] con modalità informatizzate
Registrazione [X], **Organizzazione** [X], **conservazione** [X], **consultazione** [X], **modificazione** [X], **selezione** [X], **estrazione** [X], **utilizzo** [X], **blocco** [X], **cancellazione** [X], **distruzione** [X], **Raffronto interno al Titolare** [X]

Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: solo nei casi previsti dal Regolamento MPI per questo trattamento (vedi elenco tra poche righe*)

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI , tranne i casi obbligatori per legge, ma con particolari accorgimenti (esempio graduatorie, ma sostituendo la notazione <portatore di handicap> con un codice; il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione degli altri dati sensibili e dei dati giudiziari: solo se previsto espressamente da norme di legge o regolamento e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

(*) **Destinatari consentiti per comunicazioni di dati sensibili:**

- agli Enti Locali per la fornitura dei servizi ai sensi del D.Lgs. 32 marzo 1998, n. 112 , limitatamente ai dati indispensabili all'erogazione del servizio [Il D.Lgs tratta: Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59]
- ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
- **alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap** di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n.104 (Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate (GU 17.02.1992 N. 39 SO) Materia: handicap (anche di familiari), pubblico impiego e servizi pubblici, Assistenza, previdenza e assicurazioni).

Tr.5 - Attività educativa, didattica e formativa, di valutazione

Attività educativa, didattica e formativa, di valutazione (Il trattamento concerne tutti i dati, anche sensibili e giudiziari, necessari o indispensabili all'espletamento delle attività educative, didattiche e formative, curriculari ed extracurricuiari, di valutazione ed orientamento, di scrutini ed esami) (vedi Scheda 4 del <Regolamento> di cui al Decreto n. 305/2006 approvato dal M.P.I.)

TIPI DI DATI TRATTABILI solo se assolutamente indispensabili per fini strettamente istituzionali !):

DATI COMUNI [X] **DATI PARTICOLARI** [X] **DATI SENSIBILI:**

ORIGINE [X] **razziale** [X] **etnica**

CONVINZIONI [X] **religiose** [X] **filosofiche** [X] **politiche** [X] **d'altro genere**

STATO DI SALUTE [X] **patologie attuali** [X] **patologie pregresse** [X] **terapie in corso** [X] **dati sulla salute relativi anche ai familiari**

VITA SESSUALE [X] **DATI DI CARATTERE GIUDIZIARIO** (Art. 4, comma 1, lett. E), del Codice) [X]

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: [X] presso gli interessati [X] presso terzi

ELABORAZIONE: [X] in forma cartacea [X] con modalità informatizzate

Registrazione [X], **Organizzazione** [X], **conservazione** [X], **consultazione** [X], **modificazione** [X], **selezione** [X], **estrazione** [X], **utilizzo** [X], **blocco** [X], **cancellazione** [X] , **distruzione** [X] , **Raffronto interno al Titolare** [X]

Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: solo nei casi previsti dal Regolamento MPI per questo trattamento (vedi elenco tra poche righe*)

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI , tranne i casi obbligatori per legge, ma con particolari accorgimenti (esempio graduatorie, ma sostituendo la notazione <portatore di handicap> con un codice; il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione degli altri dati sensibili e dei dati giudiziari: solo se previsto espressamente da norme di legge o regolamento e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

(*) **Destinatari consentiti per comunicazioni di dati sensibili:**

- **Alle altre istituzioni scolastiche, statali e non statali**, **per** la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
- agli **Enti Locali per** la fornitura dei servizi ai sensi del D.Lgs. 32 marzo 1998, n. 112 , limitatamente ai dati indispensabili all'erogazione del servizio (Il D.Lgs tratta: Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59)
- ai **gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica**, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
- **agli Istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;**
- **all'INAIL per la denuncia di infortuni** ai sensi del D.P.R. n. 1124/1965 (testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali).
- **alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione** e la verifica del Piano Educativo Individuale, ai sensi della Legge 5 febbraio 1992, n.104 (Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate (GU 17.02.1992 N. 39 SO) Materia: handicap (anche di familiari), pubblico impiego e servizi pubblici, Assistenza, previdenza e assicurazioni).
- **ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro,** ai sensi della Legge 24 giugno 1997, n. 196 (1) e del D. Lgsl. 21 aprile 2005, n. 77 (2) e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio.
  (1) Tratta di: Norme in materia di promozione dell'occupazione
  (2) Tratta di: Definizione delle norme generali relative all'alternanza scuola-lavoro, a norma dell'articolo 4 della legge 28 marzo 2003, n. 53. (GU n. 103 del 05/05/2005)

Tr.6 - Rapporti scuola – famiglie : gestione del contenzioso

Rapporti scuola – famiglie : gestione del contenzioso (Il trattamento concerne tutti i dati, anche sensibili e giudiziari, in alcuni casi anche di familiari o terzi, necessari o indispensabili, alle attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni denunce all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, nonché tutte le attività relative alla difesa in giudizio) (vedi Scheda 7del <Regolamento> di cui al Decreto n. 305/2006 approvato dal M.P.I.)

TIPI DI DATI TRATTABILI solo se assolutamente indispensabili per fini strettamente istituzionali !):

DATI COMUNI [X] **DATI PARTICOLARI** [X] **DATI SENSIBILI:**

ORIGINE [X] **razziale** [X] **etnica**

CONVINZIONI [X] **religiose** [X] **filosofiche** [X] **politiche** [X] **sindacali** [X] **d'altro genere**

STATO DI SALUTE [X] **patologie attuali** [X] **patologie pregresse** [X] **terapie in corso** [X] **dati sulla salute relativi anche ai familiari**

VITA SESSUALE [X]

DATI DI CARATTERE GIUDIZIARIO (Art. 4, comma 1, lett. E), del Codice) [X]

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: [X] presso gli interessati [X] presso terzi

ELABORAZIONE: [X] in forma cartacea [X] con modalità informatizzate

Registrazione [X]**, Organizzazione** [X]**, conservazione** [X]**, consultazione** [X]**, modificazione** [X]**, selezione** [X]**, estrazione** [X]**, utilizzo** [X]**, blocco** [X]**, cancellazione** [X] **distruzione** [X]

Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: solo nei casi previsti dal Regolamento MPI per questo trattamento (vedi elenco tra poche righe*)

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI , tranne i casi obbligatori per legge, ma con particolari accorgimenti (esempio graduatorie, ma sostituendo la notazione <portatore di handicap> con un codice; il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione degli altri dati sensibili e dei dati giudiziari: solo se previsto espressamente da norme di legge o regolamento e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

(*) **Destinatari consentiti per comunicazioni di dati sensibili:**

- **Avvocature dello Stato,** per la difesa erariale e consulenza presso gli organi di giustizia;
- **Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;**
- **Liberi professionisti**, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.

Tr.7 - Fornitori e clienti

Fornitori e clienti (Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, necessari alle attività di vendita, acquisto o fornitura di beni, servizi o consulenze).

TIPI DI DATI TRATTABILI (solo se necessari e per fini strettamente istituzionali !):

DATI COMUNI X **DATI PARTICOLARI** X

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: X presso gli interessati X presso terzi

ELABORAZIONE: X in forma cartacea X con modalità informatizzate

Registrazione X**, Organizzazione** X**, conservazione** X**, consultazione** X**, modificazione** X**, selezione** X**, estrazione** X**, utilizzo** X**, blocco** X**, cancellazione** X **distruzione** X

Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: MAI

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI

Diffusione degli altri dati sensibili e dei dati giudiziari: MAI

Tr.8 - Gestione finanziaria e contabile

Gestione finanziaria e contabile (Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, necessari alle attività di gestione finanziaria e contabile e all'amministrazione del bilancio)

TIPI DI DATI TRATTABILI (solo se necessari per fini strettamente istituzionali !):

DATI COMUNI [X] **DATI PARTICOLARI** [X]

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: [X] presso gli interessati [X] presso terzi

ELABORAZIONE: [X] in forma cartacea [X] con modalità informatizzate

Registrazione [X], **Organizzazione** [X], **conservazione** [X], **consultazione** [X], **modificazione** [X], **selezione** [X], **estrazione** [X], **utilizzo** [X], **blocco** [X], **cancellazione** [X] **distruzione** [X]

Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: MAI

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI

Diffusione degli altri dati sensibili e dei dati giudiziari: MAI

Tr.09 - Gestione Istituzionale

Gestione Istituzionale (Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, non compresi nei precedenti trattamenti e necessari per la gestione dell'attività istituzionale)

TIPI DI DATI TRATTABILI (solo se necessari per fini strettamente istituzionali !):

DATI COMUNI [X] **DATI PARTICOLARI** [X]

OPERAZIONI CONSENTITE (per i soli dati comuni, SOLO SE NECESSARIE; per i dati sensibili e giudiziari, SOLO SE ASSOLUTAMENTE INDISPENSABILI):

RACCOLTA: [X] presso gli interessati [X] presso terzi

ELABORAZIONE: [X] in forma cartacea [X] con modalità informatizzate

Registrazione [X]**, Organizzazione** [X]**, conservazione** [X]**, consultazione** [X]**, modificazione** [X]**, selezione** [X]**, estrazione** [X]**, utilizzo** [X]**, blocco** [X]**, cancellazione** [X] **distruzione** [X]

Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: MAI

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI

Diffusione degli altri dati sensibili e dei dati giudiziari: MAI

Tr.10 - Gestione sito web dell'istituto

Gestione sito web dell'istituto (Il trattamento concerne solo dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, per le quali apposita disposizione di legge prevede la possibilità di diffusione)

[x] Questo trattamento è attivato

[ ] Questo trattamento non è attivato

TIPI DI DATI TRATTABILI (solo se necessari per fini strettamente istituzionali !):

DATI COMUNI X

OPERAZIONI CONSENTITE (SOLO SE NECESSARIE)

RACCOLTA: X presso gli interessati X presso terzi

ELABORAZIONE: X in forma cartacea X con modalità informatizzate

Registrazione X**, Organizzazione** X**, conservazione** X**, consultazione** X**, modificazione** X**, selezione** X**, estrazione** X**, utilizzo** X**, blocco** X**, cancellazione** X **distruzione** X

Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: MAI

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI

Diffusione degli altri dati sensibili e dei dati giudiziari: MAI

Allegato 2 – descrizione fisica dei locali e delle loro caratteristiche di rischio per gli archivi ivi conservati

La scuola è articolata nelle seguenti sedi, aventi le caratteristiche sotto esposte:

SEDE N. 1 - centrale sita nel comune di Ancona in via Lanzi s.n.c., dove, nella scuola secondaria di 1^ grado "Michelangelo", frequentano N. 276 alunni e lavorano N. 1 Dirigente Scolastico, N. 1 Collaboratore Vicario del Dirigente, N. 29 Docenti, N. 1 Direttore Generale dei Servizi Amministrativi, N. 5 Assistenti Amministrativi , N 4 Collaboratori Scolastici.

SEDE N. 2 - periferica : scuola primaria "Rodari" sita nel comune di Ancona in via Brecce Bianche dove frequentano N. 304 alunni e lavorano N. 36 Docenti, N. 5 Collaboratori Scolastici;

SEDE N.3 - periferica : scuola primaria "Falcone" sita nel comune di Ancona in Piazza S.d'Acquisto dove frequentano N. 206 alunni, e lavorano N. 18 Docenti, N. 2 Collaboratori Scolastici.

SEDE N.4 - periferica : scuola dell'infanzia "Primavera" sita nel comune di Ancona in Via Brecce Bianche N. 72/A dove frequentano N. 78 alunni, e lavorano N. 9 Docenti e N. 2 Collaboratori Scolastici.

SEDE N.5 - periferica : scuola dell'infanzia "Ginestra" sita nel comune di Ancona in Via Flavia dove frequentano N. 81 alunni, e lavorano N. 7 Docenti e N. 2 Collaboratori Scolastici.

SEDE N.6 - periferica : scuola dell'infanzia di Passo Varano sita nel comune di Ancona in frazione Passo Varano dove frequentano N. 77 alunni, e lavorano N. 8 Docenti e N.2 Collaboratori Scolastici.

SEDE N.7 - periferica : scuola dell'infanzia di "La Gabbianella" sita nel comune di Ancona in Via Togliatti dove frequentano N. 62 alunni, e lavorano N. 6 Docenti e N.2 Collaboratori Scolastici.

ELENCO DEI LOCALI CHE CONTENGONO ARCHIVI CARTACEI E STRUMENTAZIONE ELETTRONICA UTILIZZABILE PER TRATTARE DATI PERSONALI:

(N.B. la numerazione è costituita da un primo numero che identifica la sede e un secondo numero che identifica la stanza: d'ora in poi ogni stanza sarà così identificata univocamente)

Definizione sintetica della stanza: 1.1.xyzw *[xyzw vanno sostituiti con la lettera iniziale del giudizio. X rappresenta il giudizio sul grado di sicurezza del settore di edificio dov'è la stanza (vedi giudizio sintetico dell'edificio), y rappresenta il giudizio complessivo sul grado di sicurezza antintrusione dell'archivio posto nella stanza stessa, z il giudizio sul grado di protezione antincendio , w il giudizio sul rischio di eventi naturali che distruggano i documenti. Esempio di codifica, che servirà per il Documento Programmatico sulla Sicurezza: 1.2.bedd*

SEDE N. 1:

Il settore di questo edificio in cui risiedono tutti gli archivi e i computers:

a) è protetto da sistema elettronico antifurto
b) è protetto da sistema di rilevazione incendi collegato ad allarme in grado di allertare interventi esterni
c) non ha un custode
d) non è sottoposto a periodica ispezione antifurto durante le ore notturne
e) dispone di un sistema di infissi rivolti verso l'esterno che assicurano un grado discreto di resistenza all'intrusione
f) complessivamente la protezione antifurto è discreta
g) Definizione sintetica del grado di sicurezza di questo settore dell'edificio:1D (x=B o x=D o X=E a seconda del giudizio dato nel punto precedente)

Elenco delle stanze contenenti archivi, registri o computers:

1.1. stanza Dirigente scolastico, con archivio parziale corrente e storico di documenti con dati comuni e con possibile presenza di dati sensibili e giudiziari relativi a taluni studenti, taluni dipendenti, taluni professionisti collaboratori esterni, talune ditte fornitrici di materiali e servizi; inoltre il registro di protocollo riservato con relativo archivio, con dati comuni e la possibilità di contenere anche dati sensibili e giudiziari.
Dotazione di dispositivi elettronici: n. 1 computers, n. 1 stampante.
Dotazione di contenitori per archivi cartacei: n. 4 armadi per archivi cartacei, n. 3 contenitori per archivi cartacei, n. 1 schedari per archivi cartacei,

E’ protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: basse
Durante i periodi di chiusura della scuola è chiusa a chiave
1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell’edificio e di quelle specifiche della stanza e di quelle dei contenitori: discreto
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: discreto
3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso
Definizione sintetica della stanza: 1.1.D,D,D,B

1.2. stanza del DGSA, con archivio parziale corrente e storico di documenti con dati comuni e con possibile presenza di dati sensibili e giudiziari relativi a taluni studenti, a taluni dipendenti, a taluni professionisti collaboratori esterni, a talune ditte fornitrici di materiali e servizi; è presente una cassaforte per custodire valori e documenti riservatissimi.
Dotazione di dispositivi elettronici: n. 1 computers, n. 1 stampante. Dotazione di contenitori per archivi cartacei: n. 2 armadi per archivi cartacei, n. 1 schedario per archivi cartacei,

E’ protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: elevate
Durante i periodi di chiusura della scuola è chiusa a chiave
1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell’edificio e di quelle specifiche della stanza e di quelle dei contenitori: elevato
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: discreto
3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso
Definizione sintetica della stanza: 1.2.D,E,D,B

1.3 stanza della Segreteria Alunni , con archivio corrente e storico di documenti con dati comuni e con possibile presenza di dati sensibili e giudiziari relativi a tutti gli studenti e a talune ditte fornitrici di materiali e servizi. Stanza dell’ufficio protocollo, dove transitano per la protocollazione e in taluni casi per l’archiviazione: si tratta di dati comuni ma è e possibile la presenza di dati sensibili e giudiziari. Dotazione di dispositivi elettronici: n. 4 computers, n. 2 stampanti,n1telefax. Dotazione di contenitori per archivi cartacei: n. 5 armadi per archivi cartacei, n. 1 schedari per archivi cartacei,

E’ protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: discrete
Durante i periodi di chiusura della scuola è chiusa a chiave
1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell’edificio e di quelle specifiche della stanza e di quelle dei contenitori: discreto
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: discreto
3) Giudizio sul grado di rischio di eventi naturali (allagamenti, terremoti o altro) che potrebbero danneggiare dati: basso
Definizione sintetica della stanza: 1.3 D,D,D,B

1.4 stanza della Segreteria Personale , con archivio corrente e storico di documenti con dati comuni e con possibile presenza di dati sensibili e giudiziari relativi a tutti docenti in servizio a tempo indeterminato e a tempo determinato, a tutti i dipendenti ATA in servizio a tempo indeterminato e a tempo determinato, a taluni professionisti collaboratori esterni, a talune ditte fornitrici di materiali e servizi; tutti i documenti relativi al rapporto di lavoro, compresi in taluni casi documenti con dati particolari (informazioni reddituali a fini fiscali, quali mod. CUD, certificazioni di sostituto d’imposta, ecc.) nonché eventuali cartelle sanitarie personali sigillate ai fini dell’applicazione del D.Lgs 626/1994. Registro di classe con annotazione assenze degli alunni per motivi di salute e provvedimenti disciplinari. Dotazione di dispositivi elettronici: n. 4 computers, n. 1 stampante. Dotazione di contenitori per archivi cartacei: n. 4 armadi per archivi cartacei, n. 1 schedario per archivi cartacei,

E’ protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: elevato
Durante i periodi di chiusura della scuola è chiusa a chiave
1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell’edificio e di quelle specifiche della stanza e di quelle dei contenitori: elevato
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: discreto
3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso
Definizione sintetica della stanza: 1.4.D,E,D,B

1.5 sala insegnanti, con armadietti chiudibili a chiave dove i docenti tengono i registri contenenti i seguenti dati : annotazione delle assenze alunni per motivi di salute, voti e giudizi sul profitto degli alunni; i registri degli insegnanti di religione contengono l’elenco alunni che hanno scelto di avvalersi dell’insegnamento della religione cattolica; gli insegnanti di materie

letterarie conservano i temi svolti, che in rari casi contengono dati personali scritti dall'alunno su se stesso, la sua famiglia e altri.
Dotazione di dispositivi elettronici: n. 1 computers, n. 1 stampante.
Dotazione di contenitori per archivi cartacei: n. 3 armadi per archivi cartacei, n. 2 contenitori per archivi cartacei.

E' protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: discrete
Durante i periodi di chiusura della scuola è chiusa a chiave
1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell'edificio e di quelle specifiche della stanza e di quelle dei contenitori: discreto
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: basso
3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso
Definizione sintetica della stanza: 1.4 D,D,B,B

1.6 stanza dei collaboratori scolastici, dove sono depositati per breve tempo in attesa di consegna plichi chiusi contenenti documenti con dati potenzialmente sensibili e giudiziari e talora domande presentate alla scuola senza busta e quindi consultabili (si prescrive di metterli sempre in busta chiusa).
Dotazione di dispositivi elettronici: n. 3 fotocopiatori, n. 1 marcatempo rileva presenze manuale.

E'protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: basse
Durante i periodi di chiusura della scuola non è chiusa a chiave
1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell'edificio e di quelle specifiche della stanza e di quelle dei contenitori: basso
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: basso
3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso
Definizione sintetica della stanza: 1.6 D,B,B,B

1.7 stanza archivio storico personale non più in servizio nella scuola o comunque non più di competenza, archivio storico alunni, archivio storico contabilità e protocollo. Dotazione di contenitori per archivi cartacei: n. 4 scaffali per archivi cartacei.

E' protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: elevate

Durante i periodi di chiusura della scuola è chiusa a chiave

1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell'edificio e di quelle specifiche della stanza e di quelle dei contenitori: discreto

2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: elevato

3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso

Definizione sintetica della stanza: 1.7 D,D,E,B

SEDE N. 2:

Il settore di questo edificio in cui risiede il dispositivo elettronico:

a) é protetto da sistema elettronico antifurto
b) è protetto da sistema di rilevazione incendi collegato ad allarme in grado di allertare interventi esterni
c) non ha un custode
d) non è sottoposto a periodica ispezione antifurto durante le ore notturne
e) non dispone di un sistema di infissi rivolti verso l'esterno che assicurano un grado elevato di resistenza all'intrusione
f) complessivamente la protezione antifurto è bassa
g) Definizione sintetica del grado di sicurezza di questo settore dell'edificio:2B

2.1 Stanza ingresso edificio. Dotazione di dispositivi elettronici: n.1 marcatempo rileva presenze manuale

E' protetta da un allarme anti-intrusione

Caratteristiche di sicurezza della porta e degli infissi: basso

Durante i periodi di chiusura della scuola è chiusa a chiave

1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell'edificio e di quelle specifiche della stanza e di quelle dei contenitori: basso

2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: basso

3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso.

Definizione sintetica della stanza: 2.1 B,B,B,B

SEDE N. 3:

Il settore di questo edificio in cui risiede il dispositivo elettronico:

a) non è protetto da sistema elettronico antifurto
b) è protetto da sistema di rilevazione incendi collegato ad allarme in grado di allertare interventi esterni

c) non ha un custode

d) non è sottoposto a periodica ispezione antifurto durante le ore notturne

e) Non dispone di un sistema di infissi rivolti verso l'esterno che assicurano un grado elevato di resistenza all'intrusione

f) complessivamente la protezione antifurto è bassa

g) Definizione sintetica del grado di sicurezza di questo settore dell'edificio:3B

3.1 Corridoio 1^ piano edificio. Dotazione di dispositivi elettronici: n.1 marcatempo rileva presenze manuale

Non è protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: discreto
Durante i periodi di chiusura della scuola è chiusa a chiave
1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell'edificio e di quelle specifiche della stanza e di quelle dei contenitori: discreto
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: basso
3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso.
Definizione sintetica della stanza: 3.1 D,D,B,B

SEDE N. 4:

Il settore di questo edificio in cui risiede il dispositivo elettronico:

a) Non è protetto da sistema elettronico antifurto

b) è protetto da sistema di rilevazione incendi collegato ad allarme in grado di allertare interventi esterni

c) non ha un custode

d) non è sottoposto a periodica ispezione antifurto durante le ore notturne

e) non dispone di un sistema di infissi rivolti verso l'esterno che assicurano un grado elevato di resistenza all'intrusione

f) complessivamente la protezione antifurto è bassa

g) Definizione sintetica del grado di sicurezza di questo settore dell'edificio:2B

4.1 Stanza ingresso edificio. Dotazione di dispositivi elettronici: n.1 marcatempo rileva presenze manuale

Non è protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: basso
Durante i periodi di chiusura della scuola è chiusa a chiave

1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell'edificio e di quelle specifiche della stanza e di quelle dei contenitori: basso
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: basso
3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso.
Definizione sintetica della stanza: 4.1 B,B,B,B

SEDE N.5

Il settore di questo edificio in cui risiede il dispositivo elettronico:

a) Non è protetto da sistema elettronico antifurto
b) è protetto da sistema di rilevazione incendi collegato ad allarme in grado di allertare interventi esterni
c) non ha un custode
d) non è sottoposto a periodica ispezione antifurto durante le ore notturne
e) non dispone di un sistema di infissi rivolti verso l'esterno che assicurano un grado elevato di resistenza all'intrusione
f) complessivamente la protezione antifurto è bassa
g) Definizione sintetica del grado di sicurezza di questo settore dell'edificio:5B

5.1 Stanza ingresso edificio. Dotazione di dispositivi elettronici: n.1 marcatempo rileva presenze manuale

Non è protetta da un allarme anti-intrusione
Caratteristiche di sicurezza della porta e degli infissi: basso
Durante i periodi di chiusura della scuola è chiusa a chiave
1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell'edificio e di quelle specifiche della stanza e di quelle dei contenitori: basso
2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: basso
3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso.
Definizione sintetica della stanza: 5.1 B,B,B,B

SEDE N.6

Il settore di questo edificio in cui risiede il dispositivo elettronico:

a) Non è protetto da sistema elettronico antifurto

b) è protetto da sistema di rilevazione incendi collegato ad allarme in grado di allertare interventi esterni
c) non ha un custode
d) non è sottoposto a periodica ispezione antifurto durante le ore notturne
e) non dispone di un sistema di infissi rivolti verso l'esterno che assicurano un grado elevato di resistenza all'intrusione
f) complessivamente la protezione antifurto è bassa
g) Definizione sintetica del grado di sicurezza di questo settore dell'edificio:6B

6.1 Stanza interno edificio. Dotazione di dispositivi elettronici: n.1 marcatempo rileva presenze manuale

Non è protetta da un allarme anti-intrusione Caratteristiche di sicurezza della porta e degli infissi: basso Durante i periodi di chiusura della scuola è chiusa a chiave 1) Giudizio complessivo sul grado di sicurezza antintrusione tenendo conto delle protezioni generali dell'edificio e di quelle specifiche della stanza e di quelle dei contenitori: basso 2) Giudizio sul grado di protezione da incendi, che potrebbero danneggiare dati: basso 3) Giudizio sul grado di rischio di eventi naturali (allagamenti o altro) che potrebbero danneggiare dati: basso. Definizione sintetica della stanza: 6.1 B,B,B,B

SEDE N.7

Il settore di questo edificio risiedono archivi cartacei:

a) Non è protetto da sistema elettronico antifurto
b) è protetto da sistema di rilevazione incendi collegato ad allarme in grado di allertare interventi esterni
c) non ha un custode
d) non è sottoposto a periodica ispezione antifurto durante le ore notturne
e) non dispone di un sistema di infissi rivolti verso l'esterno che assicurano un grado elevato di resistenza all'intrusione
f) complessivamente la protezione antifurto è bassa
g) Definizione sintetica del grado di sicurezza di questo settore dell'edificio:6B

All. 3 - Descrizione dei computer, delle reti, delle connessioni a Internet e a reti esterne

LEGENDA:

- Ogni rete di computers (= almeno 2 computers intercomunicanti fra loro, di cui uno è il cosiddetto server) è identificata dalla lettera “R” seguita da un numero, nel caso ci siano più reti (ad esempio: rete di 2 computer intranet e rete di computer normali) , la rete sarà contraddistinta da un numero. Es, “R2”
- Ogni computer che tratta od ospita dati personali (sono esclusi pc ad uso didattico o personale) sarà identificato dalle lettere “PC” seguite da un numero progressivo, con la notazione “01”, “02”…”10”, “11” ecc. Esempio: “PC01”
- Ogni PC collegato ad internet o intranet è anche contraddistinto dall’apposizione del suffisso”I” preceduto da una lineetta. Es.: PC02-I
- Ogni PC facente parte di una rete è anche contraddistinto dall’apposizione del suffisso”Rx” preceduto da una lineetta. Es.: PC03-I-R1
- Ogni PC facente parte di una rete è anche contraddistinto dall’apposizione del suffisso”S” (=Server) o “C” (=Client), preceduto da una lineetta. Es.: PC03-I-R1-S
- Normalmente si intendono computers costituiti da postazioni fisse. Se è in uso un computer portatile che tratta dati personali, va aggiunto alla fine il suffisso –P (il dato è rilevante perché questo computer è sottoposto maggiormente al rischio di furto). Esempio: PC09-I-P
- In caso di collegamenti in rete tra computers siti in sedi fisicamente separate va indicato il suffisso “-E”

Esistono le seguenti reti di computers che trattano dati personali:

R1: rete interna della scuola, costituita da n. 11 computers

Esistono i seguenti dispositivi per collegamento a internet di computers che trattano dati personali:

- N. 1 router che consente l’accesso a intranet di più computer in rete che trattano dati personali

Esistono i seguenti dispositivi per la riproduzione digitale (scanner):

- N. 1 scanner al servizio di computer della scuola che trattano dati personali

Esistono i seguenti dispositivi per back-up (realizzazione copia di sicurezza):

- N. 3 dispositivi al servizio di computer della scuola che trattano dati personali, avente le seguenti caratteristiche: disco rigido modalità Raid; disco rigido rimuovibile; disco rigido.

Esistono i seguenti dispositivi per masterizzare CD:

- N. 8 masterizzatori al servizio di computer della scuola che trattano dati personali

Esistono i seguenti dispositivi per garantire la continuità dell’erogazione dell’energia elettrica (gruppi di continuità):

- N. 1 gruppi di continuità al servizio di computer della scuola che trattano dati personali

ELENCO DEI COMPUTERS CHE TRATTANO DATI PERSONALI

1) PC01-I-R1-C sistema operativo : windows xp
E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no
E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si
Note:
Trovasi nella stanza 1,4 D,E,D,B

2) PC02-I-R1-C sistema operativo : windows xp
E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no
E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si
Note:
Trovasi nella stanza 1,4 D,E,D,B

3) PC03-I-R1-C sistema operativo : windows xp
E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no
E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si
Note:
Trovasi nella stanza 1,4 D,E,D,B

4) PC04-I-R1-C sistema operativo : windows xp
E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no
E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si
Note:
Trovasi nella stanza 1,4 D,E,D,B

5) PC05-I-R1-S sistema operativo : windows 2000 server
E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? si
E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si
Note:
Trovasi nella stanza 1,2 D,E,D,B

6) PC06-I-R1-C sistema operativo : windows xp
E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no
E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si
Note:
Trovasi nella stanza 1,2 D,E,D,B

7) PC07-I-R1-C sistema operativo : windows xp
E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no
E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si
Note:
Trovasi nella stanza 1,3 D,D,D,B

8) PC08-I-R1-C sistema operativo : windows xp
E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no
E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si
Note:
Trovasi nella stanza 1,3 D,D,D,B

9) PC09-I-R1-C sistema operativo : windows xp

E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no

E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si

Note:

Trovasi nella stanza 1,3 D,D,D,B

10) PC010-I-R1-C sistema operativo : windows xp

E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no

E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si

Note:

Trovasi nella stanza 1,3 D,D,D,B

11) PC010-I-R1-C sistema operativo : windows xp

E' protetto da mancanza improvvisa di corrente elettrica, che potrebbe distruggere dati, mediante gruppo di continuità? no

E' protetto da fulmini o sbalzi di corrente mediante speciale presa protetta o mediante il gruppo di continuità utilizzato? si

Note:

Trovasi nella stanza 1,1 D,D,D,B

ALLEGATO 4 - ELENCO ARCHIVI CONTENENTI DATI PERSONALI:

NB:ogni archivio va inteso come raccolta "omogenea" di dati personali

LEGENDA:
x.y è il codice della stanza (v.allegato 2) con i relativi codici descrittivi del livello di sicurezza
es . 1.2BDEB, segue il segno dei 2 punti per separarlo dal codice dell'archivio.

AC= archivio cartaceo + numero progressivo (es. AC01)

AE= archivio elettronico informatico + numero progressivo

AP= armadio di protezione dati + numero progressivo. Esso non raccoglie necessariamente un archivio omogeneo ma soprattutto dati, materiali, floppy disk e CD che abbisognano di un grado elevato di protezione o di archiviazione separata. Tale armadio deve disporre di serratura robusta, deve stare di regola chiuso, trovarsi preferibilmente in una stanza ben protetta dalle intrusioni, la chiave dev'essere gestita dal Titolare, dal Responsabile ed eventualmente da un Incaricato responsabilizzato che riceva adeguate istruzioni.

Es finale:1.2BDEB:AE3

*Va poi, accanto a ogni codice di archivio aggiunto tra parentesi il codice che indica quale tipo di dati vi è contenuto:**N= comune o neutro, S= sensibile, G=Giudiziario, X=stato di salute o abitudini sessuali. P=Particolari degni di particolare protezione.***

ESEMPIO DEL RISULTATO FINALE:

Armadio di Protezione Dati nella stanza del Dirigente Scolastico (archivio del protocollo Riservato) stanza	x,y:**AP01(NSGXP)**
Archivio Storico Alunni nella stanza	x,y; **AC04(NSXP)**

ELENCO ARCHIVI CARTACEI CONTENENTI DATI PERSONALI:

(Tutti i trattamenti, in particolare Tr.2 e Tr.6) Armadio di Protezione Dati nella stanza del Dirigente Scolastico (archivio del protocollo Riservato) stanza	1,1DDDB:**AP01 (NSGXP)**
(Tutti i trattamenti, in particolare Tr.2 e Tr.6) Armadio di Protezione Dati nella stanza del DSGA	1,2DEDB:**AP02 (NSGXP)**
(Tutti i trattamenti, in particolare Tr.2 e Tr.6) Archivio corrente Riservato nella stanza ad accesso controllato	1,1DDDB:**AC01 (NSGXP**
(Tutti i trattamenti, in particolare Tr.2 e Tr.6) Archivio storico Riservato nella stanza ad accesso controllato	1,7DDEB: **AC02 (NSGXP)**
(Trattamenti: Tr.3, Tr.4, Tr.5, Tr.6)Archivio Corrente Alunni nella stanza ad accesso controllato	1,3DDDB:**AC03 (NSGXP)**
(Trattamenti: Tr.3, Tr.4, Tr.5, Tr.6)Archivio Storico Alunni nella stanza ad accesso controllato	1,7DDEB; **AC02 (NSGXP)**
(Trattamenti: Tr.4, Tr.5, Tr.6)Archivio Corrente Registri alunni nella stanza ad accesso controllato	1,3DDDB:**AC03 (NSXP)**
(Trattamenti: Tr.5)Archivio Storico Registri alunni nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSXP)**
(Trattamenti: Tr.5)Archivio Corrente Elaborati alunni nella stanza ad accesso controllato	1.5DDBB:**AC04 (NSGXP)**
(Trattamenti: Tr.5)Archivio Storico Elaborati alunni nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSGXP)**
(Trattamenti: Tr4, Tr.5, Tr6)Archivio Corrente Affari Generali Alunni nella stanza ad accesso controllato	1,3DDDB:**AC03 (NSGXP)**
(Trattamenti: Tr4, Tr.5, Tr6)Archivio Storico Affari Generali Alunni nella stanza ad accesso controllato	1,7DDEB; **AC02 (NSGXP)**
(Trattamenti: Tr1, Tr.2, Tr.3)Archivio Corrente Dipendenti nella stanza ad accesso controllato	1,4DEDB:**AC05 (NSGXP)**
(Trattamenti: Tr1, Tr.2, Tr.3)Archivio Storico Dipendenti nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSGXP)**
(Trattamenti: Tr1, Tr.2, Tr.3)Archivio Corrente Stipendi, previdenziali ecc. Dipendenti nella stanza ad accesso controllato	1,2DEDB:**AC06 (NSGXP)**
(Trattamenti: Tr1, Tr.2, Tr.3)Archivio Storico Stipendi, previdenziali ecc. Dipendenti nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSGXP)**
(Trattamenti: Tr1, Tr.2)Archivio Corrente prospetti e graduatorie nella stanza ad accesso controllato	1,4DEDB:**AC05 NSXP)**
(Trattamenti: Tr1, Tr.2)Archivio Storico prospetti e graduatorie nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSXP)**
(Trattamenti: Tr1, Tr.2)Archivio Corrente assenze dipendenti nella stanza ad accesso controllato	1,4DEDB:**AC07 (NSGXP)**
(Trattamenti: Tr1, Tr.2)Archivio Storico assenze dipendenti nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSGXP)**
(Trattamenti: Tr1, Tr.2, Tr3)Archivio Corrente Affari Generali dipendenti nella stanza ad accesso controllato	1,4DEDB:**AC05 (NSGXP)**
(Trattamenti: Tr1, Tr.2, Tr3)Archivio Storico Affari Generali dipendenti nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSGXP)**
(Trattamenti: Tr1, Tr.2, Tr3) Archivio Corrente Collaboratori Professionali (assimilati ai dipendenti) nella stanza ad accesso controllato	1,2DEDB:**AC06 (NSGXP)**
(Trattamenti: Tr1, Tr.2, Tr3) Archivio Storico Collaboratori Professionali (assimilati ai dipendenti) nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSGXP)**

(Trattamenti: Tr.7)Archivio Corrente Fornitori/Acquisti nella stanza ad accesso controllato	1,2DEDB:**AC06 (NP)**
(Trattamenti: Tr.8)Archivio Storico Fornitori/Acquisti nella stanza ad accesso controllato	1,7DDEB:**AC02 (NP)**
(Trattamenti: Tr.9)Archivio Corrente Gestione Finanziaria nella stanza ad accesso controllato	1,2DEDB:**AC06 (NP)**
(Trattamenti: Tr.9)Archivio Storico Gestione Finanziaria nella stanza ad accesso controllato	1,7DDEB:**AC02 (NP)**
(Trattamenti: Tr.3)Archivio Corrente Registri e atti del Consiglio d'Istituto e della Giunta Esecutiva nella stanza ad accesso controllato	1,1DDDB:**AC08 (NSGXP)**
(Trattamenti: Tr.3)Archivio Storico Registri e atti del Consiglio d'Istituto e della Giunta Esecutiva nella stanza ad accesso controllato	1,7DDEB:**AC02 (NSGXP)**
(Trattamenti: Tr.9)Archivio Corrente di corrispondenza generale (esclusa le corrispondenza con singoli che dispongano di Fascicolo Personale) nella stanza ad accesso controllato	1,4DEDB:**AC09 (NP)**
(Trattamenti: Tr.9) Archivio Storico di corrispondenza generale (esclusa le corrispondenza con singoli che dispongano di Fascicolo Personale) nella stanza ad accesso controllato	1,7DDEB:**AC02 (NP)**
(Trattamenti: Tr.9) Archivio Corrente Istituzionale/Protocollo – Affari Generali nella stanza ad accesso controllato	1,4DEDB:**AC09 (NP)**
(Trattamenti: Tr.9) Archivio Storico Istituzionale/Protocollo – Affari Generali nella stanza ad accesso controllato	1,7DDEB:**AC02 (NP)**
(Trattamenti: Tr.9) Archivio permanente di dati da conservare sempre nella stanza ad accesso controllato	1,7DDEB:**AC02 (NP)**

ELENCO ARCHIVI ELETTRONICI

LEGENDA:
PCx=codice del computer (v.allegato 3) con i relativi codici descrittivi

es . PC03-I-R1-S**, segue il segno dei 2 punti per separarlo dal codice dell'archivio.**

AP= armadio di protezione dati + numero progressivo. Esso non raccoglie necessariamente un archivio omogeneo ma soprattutto dati, materiali, floppy disk e CD che abbisognano di un grado elevato di protezione o di archiviazione separata. Tale armadio deve disporre di serratura robusta, deve stare di regola chiuso, trovarsi preferibilmente in una stanza ben protetta dalle intrusioni, la chiave dev'essere gestita dal Titolare, dal Responsabile ed eventualmente da un Incaricato responsabilizzato e che riceva adeguate istruzioni.

AE= achivio elettronico informatico + numero progressivo (es. AE03)

AB= dischi di back-up di archivio elettronico informatico + numero progressivo

AD= dispositivo di Back-up

Es finale: PC03-I-R1-S:AE3 oppure AP01**:**AB21 oppure AD:AB21

A questo punto, accanto a ogni codice di archivio cartaceo o elettronico va aggiunto tra parentesi il codice che indica quale tipo di dati vi è contenuto:N= comune o neutro, S= sensibile, G=Giudiziario,X=stato di salute o abitudini sessuali. P=Particolari degni di particolare protezione.

LEGENDA:
Descrizione della tipologia di dato trattato:

N= Comune o neutro,
S= Sensibile
G=Giudiziario
X=Sensibile relativo a stato di salute o abitudini sessuali
P=Particolare degno di particolare protezione. Esempio:
(NSG) oppure (NSGXP)

ESEMPIO DEL RISULTATO FINALE:

Anagrafica/carriera Alunni, memorizzato nel computer	*PCx-R1-I:**AE01(NSGXP)***
Archivio Storico Alunni nella armadio di protezione dati	*x.y**:AB10(N)***

Tabella 1.3 Elenco delle base dati informatiche

(Trattamenti: Tr. 4, Tr.5, Tr.6, Tr.3) Anagrafica/carriera Alunni, memorizzato nel computer	PC05-I-R1-S:**AE01(NSGXP)**
(Trattamenti: Tr.5) Voti/Esami Alunni, memorizzato nel computer	PC05-I-R1-S:**AE02 (NP)**
(Trattamenti: Tr.5) Assenze Alunni, memorizzato nel computer	PC05-I-R-1S:**AE03 (NSGXP)** PC08-I-R1-C:**AE03 (NSGXP)**
(Trattamenti: Tr.1) Stipendi Dipendenti:memorizzato nel computer	PC05-I-R1-S:**AE04(NSGXP)**
(Trattamenti: Tr.1) Assenze Dipendenti:memorizzato nel computer	PC05-I-R1-S:**AE05(NSGXP)**

(Trattamenti: Tr.8) Gestione Finanziaria/contabilità:memorizzato nel computer	PC05-I-R1-S:**AE06(NP)**
(Trattamenti: Tr.1, Tr.5) Gestione Orario classi/docenti:memorizzato nel computer	PC08-I-R1-C:**AE07 (NP)**
(Trattamenti: Tr.4, Tr.5) Storico Anagrafica/carriera Alunni, memorizzato in CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB01 (NSXP)**
(Trattamenti: Tr.5) Storico Voti/Esami Alunni, memorizzato in CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB02 (NP)**
(Trattamenti: Tr.5) Storico Assenze Alunni, memorizzato in CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB03 (NSXP)**
(Trattamenti: Tr.1) Storico Stipendi Dipendenti:memorizzato in CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB04 (NSGXP)**
(Trattamenti: Tr.1) Storico Assenze Dipendenti:memorizzato in floppy disk o CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB05 (NSGXP)**
(Trattamenti: Tr.8, Tr9) Storico Gestione Finanziaria/contabilità:memorizzato in floppy disk o CD collocati nell'Armadio Protezione Dati e nel disco fisso del computer PC05	AP02**:AB06 (NP)**
(Trattamenti: Tr.1, Tr4, Tr5, Tr6, Tr7,Tr8, Tr.9) Archivio Corrente Posta Elettronica:memorizzato nel computer	PC08-I-R1-C:**AE08 (NP)**
(Trattamenti: Tr.1, Tr4, Tr5, Tr6, Tr7,Tr8, Tr.9) Archivio Storico Posta Elettronica :memorizzato nel computer	PC08-I-R1-C:**AE08 (NP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Dirigente Scolastico:memorizzati nel computer	PC11-R1-C:**AE11 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di DGSA:memorizzati nel computer	PC06-R1-C:**AE12 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Lofiego G. :memorizzati nel computer	PC01-R1-C:**AE13 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Tricomi S. .memorizzati nel computer	PC02-R1-C:**AE14 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Castellucci R. :memorizzati nel computer	PC03-R1-C:**AE15 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Menghi R. :memorizzati nel computer	PC09-R1-C:**AE16 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass. Ammin Marinelli S.:memorizzati nel computer	PC07-R1-C:**AE17 (NSGXP)**
(Trattamenti: Tutti) Documenti elettronici vari (word,excel e simili) di Ass.Ammin. Lucconi L :memorizzati nel computer	PC08-R1-C:**AE18 (NSGXP)**
(Trattamenti: Tutti) Storico Documenti elettronici vari (word,excel e simili) memorizzato nel computer	Da PC01 a PC11 tranne PC05
(Trattamenti: Tr.10) Archivio Corrente sito web	PC08-R1-C:**AE18 (NP)**
(Trattamenti: Tr.10) Archivio Storico sito web	PC08-R1-C:**AE18 (NP)**
(Trattamenti: Tr.4, Tr.5, Tr.6) Back-up di Anagrafica/carriera Alunni,armadio di protezione dati	AP02**:AB01 (NSGXP)**
(Trattamenti: Tr.5) Back-up di Voti/Esami Alunni,armadio di protezione dati	AP02**:AB02 (NP)**

(Trattamenti: Tr.5) Back-up di Assenze Alunni,armadio di protezione dati	AP02**:AB03 (NSGXP)**
(Trattamenti: Tr.1) Back-up di Stipendi Dipendenti:armadio di protezione dati	AP02**:AB04 (NSGXP)**
(Trattamenti: Tr.1) Back-up di Assenze Dipendenti:armadio di protezione dati	AP02**:AB05 (NSGXP)**
(Trattamenti: Tr.8, Tr.9) Back-up di Gestione Finanziaria/contabilità:armadio di protezione dati	AP02**:AB06 (NP)**

All. 5 – Misure di protezione dei dati personali

Indice:

Sotto ogni voce è indicata la categoria che è tenuta ad applicare le istruzioni e le categorie che devono prenderne visione perché comunque interessate

1) Regole generali del 'Codice in materia di protezione dei dati personali' D.Lgs 196/2003 – pag. 53

Queste Istruzioni vanno applicate da tutte le categorie di Incaricati

2) Trattamenti dei dati personali su supporto cartaceo – pag. 54

Queste Istruzioni vanno applicate dalla categoria: Assistenti Amministrativi e DGSA, Collaboratori Scolastici per quanto di loro pertinenza.

Vanno lette per necessaria conoscenza dalle seguenti categorie: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto alla Segreteria

3) Trattamenti con strumenti elettronici – pag.59

Queste Istruzioni vanno applicate dalla categoria: Assistenti Amministrativi e DGSA, Collaboratori Scolastici per quanto di loro pertinenza.

Vanno lette per necessaria conoscenza dalle seguenti categorie: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto alla Segreteria

4) Trattamenti da parte dei Docenti – pag. 62

Queste Istruzioni vanno applicate dalla categoria: Docenti.

Vanno lette per necessaria conoscenza dalle seguenti categorie: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto ai docenti

5) Trattamenti da parte dei membri di organi collegiali (anche esterni alla scuola) – pag. 63

Queste Istruzioni vanno applicate dalla categoria: membri di organi collegiali.

Vanno lette per necessaria conoscenza dalle seguenti categorie: Collaboratori del Dirigente, Assistenti Amministrativi e DGSA in quanto di supporto, Collaboratori Scolastici in quanto di supporto

6) Trattamenti da parte dei Collaboratori Scolastici – pag. 63

Queste Istruzioni vanno applicate dalla categoria: Collaboratori Scolastici..

Vanno lette per necessaria conoscenza dalle seguenti categorie: Collaboratori del Dirigente, Assistenti Amministrativi e DGSA in quanto di supporto

1 - Regole generali del 'Codice in materia di protezione dei dati personali' D.Lgs 196/2003

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli Incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli Incaricati.

ELENCO MISURE DI PROTEZIONE CHE GLI INCARICATI DEVONO ATTUARE

(nel caso di impossibilità devono comunicarlo al Titolare o al Responsabile se esiste)

Va ricordato che il D.Lgs 196/2003 sancisce il dovere di mantenere integri i dati forniti dall'interessato finché non siano più necessari. Pertanto tra le misure di protezione dei dati vanno considerate anche quelle mirate a questo scopo (protezione degli archivi cartacei da furti, incendi ed altri eventi distruttivi; protezione degli archivi elettronici da sbalzi di corrente o eventi che danneggino il computer o le sue memorie, effettuazione di copie di sicurezza degli archivi elettronici con periodicità adeguata, ecc.)

2 - Trattamenti dei dati personali su supporto cartaceo

Queste Istruzioni vanno applicate dalla categoria: Assistenti Amministrativi e DGSA, Collaboratori Scolastici per quanto di loro pertinenza.

- Procedura di Protezione Dati **PP01: documenti in ingresso**

Per "documenti in ingresso", si intendono i documenti o i supporti contenenti dati personali acquisiti dalla scuola ai fini di un loro impiego in trattamento.

Relativamente al trattamento dei documenti in ingresso , è necessario adottare le cautele seguenti:

- i documenti in ingresso devono essere utilizzati soltanto da chi sia Incaricato al trattamento dei dati che contengono o dal Responsabile;
- l'Incaricato deve verificare:
  - la provenienza dei documenti;
  - che tali documenti siano effettivamente necessari al trattamento in questione;
  - la tipologia dei dati contenuti (comuni, sensibili, , giudiziari o altri dati particolari), al fine di individuare le modalità legittime ed idonee per il trattamento e le misure di sicurezza da attuare;
  - l'osservanza del principio di pertinenza e non eccedenza rispetto o alle finalità del trattamento, la completezza, la correttezza e l'aggiornamento dei dati;
- l'Incaricato deve valutare se è necessaria l'informativa (e, se è necessaria la postilla per i dati sensibili e giudiziari, di cui all'art. 22, in tal caso compilandola).

- Procedura di Protezione Dati **PP03: informativa per la raccolta di dati comuni o particolari**

Ogni raccolta di dati personali **comuni o particolari** dev'essere accompagnata dalla sottoscrizione per attestazione della presa visione dell'apposita informativa di cui all'art. 13, che è fornita dal Titolare.

Ogni istanza rivolta alla scuola deve essere redatta su un modulo che in calce riporti il testo dell'informativa di cui al punto precedente , in modo che la firma dell'istanza stessa funga anche da attestazione della presa visione dell'informativa stessa. Pertanto non si accettano istanze su fogli bianchi. Tassativamente vanno utilizzati gli appositi moduli che hanno la parte superiore bianca e in calce riportano l'informativa. In casi eccezionali l'informativa può essere applicata all'originale, però è necessaria coincidenza di data e un chiaro riferimento al documento a cui si riferisce.

Per quanto riguarda dipendenti, collaboratori, commissari d'esame ecc. al momento dell'inizio del rapporto l'informativa deve prevedere anche le probabili comunicazioni di dati personali alle varie istanze del MPI, alla Regione, al Tesoro, alla Ragioneria Provinciale dello Stato, all'INPS (se T.D.) o all'INPDAP, al Ministero Funzione Pubblica per l'anagrafe delle retribuzioni, alla scuola di provenienza e alla scuola a cui fossero trasferiti, ecc.

Informativa da inserire <u>obbligatoriamente</u> in tutte le dichiarazioni sostitutive di certificazione e di atto notorio:

Ai sensi dell'art. 48 del D. P. R. n. 445 del 28 dicembre 2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), è **<u>obbligatorio</u>** inserire l'informativa nella modulistica per la presentazione delle dichiarazioni sostitutive di certificazione e di atto notorio.

E' opportuno comunque inserire l'informativa in via generale in tutta la modulistica relativa alle istanze da presentare alla scuola. Si utilizzerà lo stesso testo dell'informativa di cui sopra.

- Procedura di Protezione Dati **PP05: informativa per la raccolta di dati sensibili o giudiziari**

Ogni raccolta di dati personali **sensibili o giudiziari** dev'essere accompagnata dalla sottoscrizione per attestazione della presa visione dell'apposita informativa di cui all'art. 13, che è fornita dal Titolare, diversa da quella per dati comuni perché richiede anche un completamento da parte dell'Incaricato. Infatti quest'ultimo deve indicare per quale precisa finalità serve il dato, citando tassativamente la legge o la disposizione a cui si riferisce la finalità dell'istanza, e indicando a chi il dato sarà comunicato (o potrebbe essere comunicato) o se il dato sarà diffuso.

Per quanto riguarda le relazioni mediche, va graffettata ad esse l'informativa, compilata come sopra.

Tra i soggetti a cui i dati sensibili potranno essere comunicati va sempre indicata, sia per gli alunni che per i dipendenti, anche la scuola, ovviamente al momento sconosciuta, alla quale potrebbero trasferirsi.

Anche la scheda della registrazione assenze va autorizzata da apposita informativa, se le assenze per motivi di salute sono indicate con un codice che le renda riconoscibili.

Al momento dell'istituzione di ciascun Fascicolo Personale l'Interessato deve autorizzarlo con apposita informativa che consenta anche di mandarlo alla scuola in cui si dovesse trasferire e devono essere citati i trattamenti di certificati medici sia per giustificare l'assenza, sia per ottenere esoneri o benefici, sia a scopo di godere le coperture assicurative Inail o dell' assicurazione privata della scuola, sia per le comunicazioni di legge alla Questura e all'Inail.

Nel caso sia raccolto un dato sensibile o giudiziario (ad esempio i certificati medici, i moduli che richiedono se l'Interessato ha riportato condanne oppure se è di sana e robusta costituzione, ecc.) va utilizzata l'apposita informativa,

- Procedura di Protezione Dati **PP07**: **firma l'Interessato o c'è sua delega scritta**

Qualunque trattamento di dati su richiesta dell'Interessato, se presentato da terzi dev'essere tassativamente autorizzato da delega. Ovviamente per gli alunni minorenni, il genitore o la persona esercente la patria potestà non ha bisogno di delega. Per eventuali alunni maggiorenni anche il genitore ha bisogno della delega.

La delega va allegata all'informativa o all'istanza o alla ricevuta.

- Procedura di Protezione Dati **PP09: documenti in uscita**

Per "documenti in uscita", si intendono i documenti o i supporti contenenti dati personali prodotti e rilasciati dalla scuola a soggetti esterni ad stessa.

L'Incaricato del trattamento deve trattare qualunque prodotto dell'elaborazione di dati personali, ancorchè non costituente documento definitivo, (appunti, stampe interrotte, stampe di prova, stampe elaborazioni temporanee ecc.) con le stesse cautele che sarebbero riservate alla a versione definitiva (v. misure relative ai trattamenti cartacei e informatizzati).

Prima di consegnare o spedire documenti, verificare che esistano in atti le necessarie, adeguate informative.

Nel caso di documenti in uscita è necessario all'atto della consegna o dell'invio, verificare che la persona che riceve il documento sia legittimata al ritiro e all'utilizzo (delega).

- Procedura di Protezione Dati **PP11: verifica della legittimità del trattamento in corso**

Di fronte a qualsiasi nuovo trattamento di dati, il Responsabile del trattamento stesso e l'Incaricato devono chiedersi se rientra nel preciso recinto di legittimità, delimitato dai seguenti paletti:

Il trattamento sia connesso con **l'esercizio delle funzioni istituzionali** (principio di **pertinenza)** e che esse non siano perseguibili attraverso il trattamento di dati anonimi.

1. Le modalità del trattamento siano tali da determinare il minimo sacrificio possibile del diritto alla riservatezza dell'Interessato (principio di **non eccedenza:** è illegittimo chiedere un dato in più di quello che è strettamente necessario).
2. Ogni fase del trattamento rispetti **le norme di legge e di regolamento.**
3. In ogni fase del trattamento siano adottate le **misure di sicurezza previste per la categoria alla quale il dato appartiene**
4. Se il dato è sensibile o giudiziario, siano rispettati i presupposti per avere la legittimazione a trattarlo
5. In caso di comunicazione o diffusione, che il dato rientri nelle categorie autorizzate

- Procedura di Protezione Dati **PP13**: **quando un alunno o un dipendente ci lascia definitivamente**

Gli vanno consegnati tutti i documenti contenenti dati personali che la scuola non sia obbligata a conservare. Nel caso non fosse possibile trattare direttamente con l'Interessato, si deve mandare un avviso per il ritiro. Nel frattempo i materiali da consegnare vanno posti in busta chiusa. Al ritiro va fatta firmare una ricevuta. Se passato un lasso ragionevole di tempo, l'interessato un suo delegato non si presenterà a ritirarli, si avvierà una procedura di distruzione dei documenti, con apposito verbale, ovviamente valutando prima se ci sono documenti che non sia opportuno eliminare (ad esempio, diplomi originali e simili) in conformità a quanto prescritto dalla normativa che regola lo scarto d'archivio.

In ogni caso qualunque fascicolo personale che transiti dall'archivio corrente a quello storico, dev'essere prima depurato di tutti dati personali non più necessari.

- Procedura di Protezione Dati **PP15: classificazione immediata di ogni documento/protocollo**

Non appena qualsiasi Incaricato si accorge che un documento contiene dati personali di livello superiore a "comune" o "anonimo" , deve scrivere in matita sull'angolo destro superiore del foglio la sigla descrivente il tipo di dato : "P" = dato particolare, "S"= dato sensibile, "G"= dato giudiziario.

- Procedura di Protezione Dati **PP17: trattamento appena un documento viene ricevuto**

L'Incaricato che riceve "brevi manu" allo sportello o in qualsiasi altro punto della scuola documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza ancora non collocati in busta chiusa, deve immediatamente metterli in busta chiusa e inserirli nella posta in arrivo per il Dirigente Scolastico.

- Procedura di Protezione Dati **PP19: circoscrivere al massimo il numero di Incaricati che trattano una pratica**

I documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza, devono essere visti e conosciuti dal minor numero possibile di Incaricati. Le pratiche relative a tali documenti devono essere seguite nell'intero iter possibilmente da una sola persona (compresa la fase di protocollo), salvo diversa disposizione del Dirigente o del Responsabile.

- Procedura di Protezione Dati **PP21: affidamento all'Incaricato sotto la sua responsabilità**

In generale qualsiasi documento o fascicolo contenente dati personali va trattenuto dall'Incaricato per il tempo strettamente necessario alla lavorazione e riposto nel suo archivio appena terminato il lavoro o alla fine della giornata lavorativa. Non devono essere lasciati sui tavoli o comunque fuori dai contenitori documenti o fascicoli contenenti dati personali.

Nei casi in cui i documenti con dati sensibili/giudiziari debbano essere trattati per un certo periodo di tempo, vengono mantenuti sotto la responsabilità dell'Incaricato per il più breve tempo possibile. L'Incaricato ha istruzione di elaborare le pratiche riferite a questi documenti in una stanza chiusa, ad accesso riservato almeno in quel momento, in modo che nessun altro possa sbirciarli o tanto meno trovarli momentaneamente abbandonati sul tavolo; nei momenti di non utilizzazione di conservarli dentro un cassetto o un armadio chiuso a chiave, del quale soltanto l'Incaricato ha la chiave.

- Procedura di Protezione Dati **PP23: custodia separata per i dati relativi allo stato di salute**

Per dati relativi allo stato di salute ed alle abitudini sessuali (reati di tipo sessuale, ecc.) c'è l'obbligo di **custodia separata** rispetto agli altri dati trattati per finalità che non richiedono il loro utilizzo.

- Procedura di Protezione Dati **PP25 : Regole generali per la sicurezza degli archivi**

Vanno poste in essere le misure necessarie a ridurre al minimo i rischi di:

- accesso fisico non autorizzato;
- furto o manomissione dei dati da parte di malintenzionati; distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

Gli archivi possono essere soltanto di due tipi:

1) a bassa sicurezza, per dati comuni o neutri, con accesso "selezionato" (il Titolare o il Responsabile decidono chi può entrarvi e gli danno la chiave personale o mettono a disposizione la chiave in modo che solo costoro possono utilizzarla). E' fondamentale assicurarsi che esista un numero definito di chiavi e che la chiave di riserva sia chiusa in luogo ben protetto. E' stato nominato con atto formale un Incaricato "Responsabile delle chiavi" che deve controllare.
2) Ad alta sicurezza, ovviamente per dati sensibili o giudiziari, con accesso non solo selezionato, ma anche "controllato": c'è una sola chiave disponibile e l'Incaricato che ne ha bisogno e che è autorizzato deve chiederla al "Responsabile delle chiavi". Chi accedesse fuori orario di lavoro, deve annotarlo in apposito registro. Nella scuola non c'è necessità di accedere fuori orario, quindi non c'è ragione che esista tale registro. Peraltro il Dirigente Scolastico, in quanto Titolare, ha libertà assoluta di accesso.

Dati personali comuni - protezione dall'accesso fisico non autorizzato : i documenti contenenti dati personali comuni sono conservati in archivi ad accesso selezionato: pertanto l'accesso ai dati è consentito ai soli Incaricati del trattamento.

I documenti possono essere estratti dall'archivio e affidati alla custodia dell'Incaricato del trattamento per il tempo strettamente necessario al trattamento medesimo: egli ha cura di garantirne la riservatezza e provvede al deposito in archivio al termine delle operazioni. Gli Incaricati che custodiscono dati personali su supporto cartaceo devono verificare che la dotazione di arredi (cassettiere, armadi ecc.) muniti di meccanismi di serratura adatta a garantire la sicurezza sia adeguata, altrimenti devono segnalare al Titolare la necessità di acquisirli.

Dati sensibili e giudiziari - protezione dall'accesso fisico non autorizzato**:** l'accesso è limitato agli Incaricati del trattamento. Gli archivi devono essere ad accesso controllato. I documenti contenenti dati sensibili e giudiziari devono essere conservati in elementi di arredo (armadi o cassettiere) muniti di serratura a chiave; la chiusura a chiave garantisce tanto la selezione del personale autorizzato ad accedere, quanto il controllo sugli accessi medesimi.

Protezione dei locali archivio contenenti dati personali sensibili :

-se i documenti contenenti dati personali sensibili sono archiviati in arredi (armadi o cassettiere) chiusi a chiave, l'accesso ai locali che li contengono può non essere soggetto a particolari restrizioni. Resta fermo l'obbligo per l'Incaricato e il Responsabile di verificare che gli elementi di arredo siano sempre chiusi e che vengano rispettate le misure relative alla gestione delle chiavi.

-se non c'è immediata disponibilità di arredi muniti di serratura per l'archiviazione dei documenti contenenti dati personali sensibili, gli archivi devono in ogni caso essere ubicati in appositi locali chiusi a chiave e, se appare agevole l'intrusione dall'esterno, muniti di sbarre. In tal caso il personale diverso dagli Incaricati del trattamento che vi accede i deve essere accompagnato da uno dei soggetti Incaricati del trattamento o dal custode delle chiavi, che deve verificare che non avvenga un accesso illecito ai dati sensibili ivi contenuti.

Ogni stanza-archivio deve essere chiusa a chiave quando non presenziata, anche se i documenti sono custoditi in contenitori chiusi a chiave, in quanto aumenta il livello di protezione dei dati stessi.

Protezione dal rischio di perdita dei dati dovuta ad eventi fisici

Un archivio è sottoposto al rischio di svariati tipi di eventi che possono provocare la distruzione o il danneggiamento dei documenti. Per ridurre al minimo questo rischio le principali misure da prendere sono le seguenti:

1)evitare eccessivi carichi d'incendio. 2) Utilizzare il più possibile contenitori chiusi 3) Applicare in modo assoluto il divieto di fumo dentro la stanza e nelle adiacenze 4) Non lasciare pertugi dove possano essere gettati materiali o liquidi 5) nelle vicinanze devono essere presenti idonei dispositivi antincendio 6) è auspicabile la presenza di un sensore antincendio, anche autonomo.

Misure logistiche :

Il personale addetto al trattamento di dati personali deve porre in essere le misure necessarie a ridurre al minimo i rischi di: accesso fisico non autorizzato; furto o manomissione dei dati da parte di malintenzionati; distruzione o perdita dei dati dovuta ad eventi fisici; perdita accidentale dei dati.

Chiusura a chiave dei contenitori metallici:

Gli armadi e contenitori che ospitano archivi vanno chiusi a chiave alla fine della giornata lavorativa e le chiavi vanno messe in luogo sicuro indicato dal DGSA o dal Custode delle chiavi.

- Procedura di Protezione Dati **PP27 : archiviazione separata**

I documenti contenenti dati sensibili, giudiziari o particolari ad alto livello di delicatezza vanno di norma chiusi in busta di carta, su cui è riportato nome dell'interessato, tipo di documento, data attuale e la scadenza per la eliminazione (se non conoscibile, mettere una data presunta seguita da un punto interrogativo). Per i documenti contenenti dati particolarmente sensibili, invece del nome sulla busta si deve scrivere un codice, la data attuale e la scadenza per l'eliminazione.

La corrispondenza tra codice e nome dell'interessato sarà riportata in un foglio o un quaderno, posto in una busta chiusa gestita dal Responsabile o dal Titolare, e posto in luogo sicurissimo e protetto.

La busta viene archiviata in uno degli Armadi cosiddetti "dei Dati Protetti" (permanentemente chiuso a chiave, ad accesso controllato, in una stanza normalmente chiusa a chiave quando non presenziata e protetta da antifurto).

Al posto del documento così protetto viene messo nel fascicolo un foglio con annotazione generica del tipo di documento, della sua collocazione e della scadenza di distruzione.

- Procedura di Protezione Dati **PP29: conservazione di registri e altri documenti utilizzati per anni scolastici precedenti e non più utilizzati**

Conservazione: molti documenti e registri sono utilizzati per un intero anno scolastico ma solo in quello. Tra questi, i documenti non più utilizzati negli anni seguenti (salvo ricorsi o richieste di accesso legittime) al termine dell'anno scolastico sono impacchettati a gruppi omogenei. Sull'involucro viene riportato il contenuto e l'eventuale scadenza per l'eliminazione. Vengono conservati in una stanza chiusa a chiave ad accesso selezionato. L'eliminazione dei documenti avviene mediante la Procedura di Protezione Dati **PP37**

- Procedura di Protezione Dati **PP31: archiviazione nel fascicolo personale**

I documenti non archiviati nell'Armadio di Protezione dati, finché l'alunno è iscritto o il dipendente è in servizio, vengono conservati nel fascicolo personale. In particolare alcuni dati si situano in una zona di confine tra dato particolare e dato sensibile (ad es. certificati medici generici privi di diagnosi), data la loro bassa pericolosità vengono mantenuti nel fascicolo personale, ma in una cartella separata, poi verrà valutata la possibilità di eliminarli con la procedura di Protezione Dati **PP37**. Il fascicolo personale è conservato nel relativo archivio corrente: in cassettiere metalliche chiuse a chiave negli orari non lavorativi e normalmente presidiate da almeno un Incaricato dei trattamenti (ovvero un dipendente assegnato alla segreteria), in una stanza in cui non sono ammessi di regola estranei, che viene chiusa a chiave al di fuori dell'orario lavorativo.

- Procedura di Protezione Dati **PP33: archiviazione nell'archivio storico**

Quando l'alunno ha cessato la frequenza o il dipendente ha cessato di essere in carico alla scuola, il relativo fascicolo personale viene depurato dei documenti non più necessari, in conformità a quanto prescritto dalla normativa che regola lo scarto d'archivio, quindi archiviato nel corrispondente archivio storico, collocato in una stanza chiusa a chiave, ad accesso selezionato.

- Procedura di Protezione Dati **PP35: scarto periodico dei documenti**

Scarto periodico dei documenti contenenti dati personali di qualunque livello , ai sensi dell'art. 11 comma e del D.Lgs 196/2003, vanno eliminati non appena cessa lo scopo per cui sono stati raccolti. Pertanto periodicamente, all'inizio di ogni anno solare per le pratiche che hanno questa cadenza, oppure all'inizio di ogni nuovo anno scolastico tutti gli archivi vengono passati al vaglio e vengono eliminati i documenti non più necessari, utilizzando la Procedura di Protezione Dati **PP37** in conformità a quanto prescritto dalla normativa che regola lo scarto d'archivio.

- Procedura di Protezione Dati **PP37: distruzione dei documenti**

La distruzione di documenti contenenti dati personali di qualunque livello avverrà con modalità di Protezione Dati per impedire che estranei prendano visione del contenuto o, peggio, se ne impadroniscano. Di queste operazioni si occupano solamente Incaricati, con la qualifica di Collaboratori Scolastici e Assistenti Amministrativi. Se possibile si utilizza un apparecchio che trincia la carta. Altrimenti si provvede a rendere comunque anonimi mediante tagli e cancellature indelebili i documenti sensibili, giudiziari e particolari ad alto rischio. Per gli altri ci si assicurerà che nessuno possa impadronirsene prima della distruzione (o riciclo o conferimento in discarica) da parte dell'ente a cui si conferiranno.

- Procedura di Protezione Dati **PP39: appunti, bozze e copie superflue**

Anche gli appunti, le bozze, le stampe intermedie, le fotocopie superflue costituiscono elemento di rischio, maggiorato quando trattasi di pratiche comprendenti anche documenti sensibili o giudiziari. Pertanto essi vanno distrutti con la prescritta procedura o , se necessario conservarli, archiviati insieme all'originale del documento sensibile o giudiziario.

- Procedura di Protezione Dati **PP41: cautele nella fase di fotocopiatura**

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere fotocopiati, hanno la precedenza su tutti gli altri e devono essere adottate opportune cautele affinché nessun altro ne possa prendere visione. Tranne impossibilità tecnica, l'operazione di fotocopiatura deve essere effettuata dall'Incaricato che tratta la pratica. L'Incaricato deve fare in modo che il documento non venga lasciato in giacenza vicino alla fotocopiatrice né prima né dopo la fotocopiatura. A maggior ragione questo si applica se l'operazione di fotocopiatura avviene in una stanza ad accesso libero.

- Procedura di Protezione Dati **PP43: la movimentazione da parte di terzi**

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere movimentati attraverso Collaboratori scolastici Incaricati, anche all'interno della scuola, devono essere collocati in busta chiusa. Anche la spedizione postale o la consegna in altro modo deve essere effettuata esclusivamente da Incaricati che abbiano ricevuto almeno l'autorizzazione a questo ambito di trattamento e che assicurino massima diligenza nella custodia dei plichi.

- Procedura di Protezione Dati **PP45: pulizia dei locali contenenti archivi**

L'accesso di dipendenti o estranei per la pulizia dei locali contenenti archivi cartacei dev'essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni, peraltro brevi, devono essere effettuate in presenza di un Incaricato della segreteria. Se vi sono contenuti dati sensibili sono chiudibili in contenitore, la pulizia deve essere effettuata esclusivamente alla presenza di un Incaricato del trattamento di tali dati.

- Procedura di Protezione Dati **PP47: ingresso di persone esterne per manutenzione**

L'accesso di dipendenti o estranei per la manutenzione dei locali contenenti archivi cartacei o delle attrezzature in tali stanze contenute, dev'essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni devono essere effettuate in presenza di un Incaricato. Se dati sensibili o giudiziari non sono chiudibili in contenitore, l'intervento deve essere effettuato esclusivamente alla presenza di un Incaricato del trattamento di tali dati.

- Procedura di Protezione Dati **PP49: ingresso di altre persone in segreteria e nell'Ufficio del D.S.**

Di norma l'ingresso in segreteria e nell'ufficio del Dirigente Scolastico, nelle ore lavorative, è riservato a chi vi lavora, al Dirigente e ai suoi collaboratori, ai Collaboratori scolastici che ne hanno motivo. Gli altri dipendenti e gli estranei di norma non possono accedere, salvo che ne facciano richiesta preventiva e ne ottengano l'autorizzazione di volta in volta.

Ciò viene previsto allo scopo di evitare che persone non autorizzate vedano anche involontariamente documenti riservati.

La segreteria deve essere chiusa a chiave quando non è presenziata da chi vi lavora. Possibilmente le pulizie devono essere organizzate in orari in cui vi sia almeno un Assistente Amministrativo presente.

3 - Trattamenti con strumenti elettronici

Queste Istruzioni vanno applicate dalla categoria: Assistenti Amministrativi e DGSA, Collaboratori Scolastici per quanto di loro pertinenza.

- Procedura di Protezione Dati **PP51: sistema di autorizzazione dell'accesso**

1. Il trattamento di dati personali con strumenti elettronici é consentito esclusivamente agli Incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione possono consistere in una di queste soluzioni:

a) un codice per l'identificazione dell'Incaricato (user-id o username o 'nome utente') fisso e parzialmente riservato (è noto al gestore del sistema, perché deve assegnarlo ed è visibile ai manutentori software), cui è associata una password segretissima variabile;

b) oppure in una tessera magnetica in possesso e uso esclusivo dell'Incaricato, associata a un codice di identificazione dell'Incaricato (user-id o username o 'nome utente') fisso e parzialmente riservato (è noto al gestore del sistema, perché deve assegnarlo ed è visibile ai manutentori software), cui è associata una password segretissima variabile.

3. Ad ogni Incaricato sono assegnate individualmente una o più credenziali per l'autenticazione.

4. Ogni Incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale (= password segreta o parola chiave) nonché la diligente custodia della tessera magnetica in possesso ed uso esclusivo dell'Incaricato (se esiste)

5. La parola chiave, quando é prevista dal sistema di autenticazione, dev'essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato (nomi o iniziali proprie o di parenti, date di nascita, e simili).

La parola chiave dev'essere modificata da ciascun Incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave dev'essere modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri Incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi vanno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali vanno disattivate anche in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali.

9. Gli Incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Non appena un Incaricato modifica la parola chiave, deve scriverla in un foglio, chiuderla in busta chiusa, all'esterno indicare "parola chiave del sig. … e la data). La busta va data al "Custode delle Password", che la riporrà in cassaforte o in altro armadio sicuro. Questa procedura è adottata per consentire al titolare di assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. Oppure nel caso che l'Incaricato "dimentichi" la password . Si ricorda che il Codice dice : "In tal caso la custodia delle copie delle credenziali é organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti Incaricati della loro custodia, i quali devono informare tempestivamente l'Incaricato dell'intervento effettuato."

11. Ovviamente le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione o all'uso personale o didattico.

Costituisce infrazione disciplinare gravissima scrivere una password o una user-id su fogli di carta o quaderni, tento peggio se in vicinanza del computer. E' vietato anche tenerla nel cassetto, benché chiuso a chiave. Se non si può memorizzarla, è consentito soltanto conservarla in un foglietto dentro il portafoglio, meglio se mascherata premettendo e posponendo un certo numero di lettere o cifre.

Sistema di autorizzazione

12. Quando per gli Incaricati sono individuati profili di autorizzazione di ambito diverso (per esempio per trattare dati sensibili o giudiziari) é utilizzato uno specifico sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun Incaricato o per classi omogenee di Incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

L'implementazione di questo sistema di autenticazione si fa in questo modo:

Il Titolare o il Responsabile individuano quali profili di autorizzazione sono necessari per gli Incaricati che utilizzano il computer. In pratica stabiliscono quali computers può usare ogni Incaricato, di quali cartelle (directories) ha necessità, quali altre cartelle vanno create, a quali cartelle possono accedere tutti gli Incaricati e a quali possono accedere solo alcuni e a quali soltanto un singolo Incaricato, quali devono essere cifrate e con quale tecnica.

L'Amministratore di sistema o un tecnico dovrà tradurre in pratica queste direttive, costruendo i necessari profili di autorizzazione differenziati per ciascun utilizzatore, al quale sarà consegnata la corrispondente credenziale di autenticazione (più d'una se necessario).

L'Amministratore di sistema o un tecnico dovrà provvedere anche a tradurre in pratica operativamente le altre indicazioni strategiche sulla gestione dei programmi e dei loro aggiornamenti, del backup, dell'antivirus, del firewall (protezione dagli accessi tramite internet) e dei sistemi di ripristino dati in caso di "disastro informatico" (disaster recovery=recupero del disastro).

- Procedura di Protezione Dati **PP53: salvataggio dei dati (back-up)**

Gli Incaricati sono tenuti a salvare i dati con frequenza almeno settimanale (lo dice il Codice). Pertanto procederanno al back-up su CD , che verranno riposti nell'armadio protetto di cui è Responsabile il DGSA e che deve restare sempre chiuso. Si ricorda che il Codice prescrive: "Devono essere adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni." Pertanto le copie di sicurezza devono essere aggiornate settimanalmente.

- Procedura di Protezione Dati **PP55 : cifratura dei file recanti dati idonei a rivelare lo stato di salute e la vita sessuale**

Tale procedura non è dovuta dalla scuola.

- Procedura di Protezione Dati **PP57 - Ulteriori misure in caso di trattamento di dati sensibili o giudiziari : Programmi firewall, dispositivi firewall**

Accessi abusivi logici (cioè eseguiti attraverso la logica del software)

I dati devono essere permanentemente protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale (accesso abusivo per via telematica da parte di operatori molto esperti nell'utilizzare la connessione della scuola a internet per introdursi nei computers durante il collegamento e copiare dati o manometterli; alcuni di loro sono definiti "hackers").

Molto utile è l'aggiornamento frequente del Sistema Operativo, tramite internet, gratuitamente presso il sito del produttore di tale software, il quale identifica i "buchi" del sistema operativo che consentono l'accesso indesiderato dall'esterno e vi rimedia mettendo a disposizione una "pezza" (patch) che copre il buco. Poiché le falle dei sistemi windows sono moltissime, le patches da caricare sono altrettante, quindi bisogna aggiornare spesso il software. Da notare che le patches servono anche contro i virus e simili perché anch'essi utilizzano le falle del sistema.

La protezione da queste "intrusioni logiche" viene effettuata con un apposito programma denominato "firewall" che intercetta ogni utilizzo delle porte di comunicazione del computer sia in entrata che in uscita e verifica se è autorizzato altrimenti lo blocca e chiede di autorizzare o meno la comunicazione.

- Procedura di Protezione Dati **PP59 - Ulteriori misure in caso di trattamento di dati sensibili o giudiziari : Programmi antivirus**

Virus, worms (vermi) e altri programmi maligni

I dati devono essere permanentemente protetti contro virus, worms, e altri programmi informatici che possono causare perdita di dati, malfunzionamenti, danni all'hardware, trasmissione all'esterno di files contenuti nel computer. Tali virus possono infettare i computers tramite l'uso di dischetti o l'accesso a certi siti internet o tramite la posta elettronica (in particolare i cosiddetti "allegati"). La protezione viene effettuata mediante l'utilizzo di un programma antivirus, acquistato dalla scuola e fornito agli Incaricati dal DGSA. Il programma antivirus deve essere aggiornato almeno ogni settimana (la norma prevede almeno 6 mesi, ma è sicuramente insufficiente, visto che ogni giorno nascono nuovi virus). L'Incaricato è tenuto a verificare che queste condizioni siano attuate e ad eseguire quanto è di sua pertinenza. Prima di aprire ciascun messaggio di posta elettronica l'Incaricato è tenuto a valutare se il messaggio proviene da mittente noto o plausibile, in caso contrario deve adottare particolari cautele. Non deve aprire allegati che abbiano estensione ".exe", ".pif", ".scr" a meno che non sia sicuro del mittente; se l'estensione appare doppia (esempio: ".pif.scr" non deve aprire comunque l'allegato). Inoltre deve valutare dal titolo dell'allegato se esso è plausibile e pertinente col mittente e con le attività di interesse della scuola.

- Procedura di Protezione Dati **PP61: uso dei supporti rimovibili**

I floppy disk, i CD e le pen-drive non devono essere utilizzati mai per memorizzare i file contenenti dati personali; tali files vanno invece memorizzati solo nel disco fisso di computers protetti da sistema di credenziali di accesso. Ciò al fine di evitare che chi si impadronisca di tali supporti rimovibili, possa accedere ai dati. I supporti rimovibili (floppy disk, i CD e le pen-drive) devono essere utilizzati esclusivamente per le copie di sicurezza (back-up) e subito devono essere riposti nel luogo sicuro indicato.

- Procedura di Protezione Dati **PP63**: **cautele nel riutilizzo dei supporti rimovibili**

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (= riformattando il disco e verificando l'avvenuta riformattazione; non basta assolutamente cancellare i files !)

- Procedura di Protezione Dati **PP65 – accesso di manutentori software o hardware**

Se una delle misure minime di sicurezza elencate sono attuate tramite l'intervento di soggetti esterni alla propria struttura, per provvedere alla esecuzione è assolutamente tassativo ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico di cui allegato B del D.Lgs 196/2003. Tale dichiarazione va consegnata al titolare.

In caso di manutenzione dell'hardware o del software da parte di persone esterne alla scuola o comunque non incaricate del trattamento dei dati contenuti in quel computer, un Incaricato deve controllare a vista le operazioni eseguite, in modo da verificare che non ci sia mai lettura o copia di dati né che siano indebitamente scoperte le parole chiave.

- Procedura di Protezione Dati **PP67: pulizia dei locali**

L'accesso di dipendenti o estranei per la pulizia dei locali contenenti dischi di back-up dev'essere effettuata solo con i contenitori chiusi a chiave. Se dati sensibili o giudiziari non sono chiudibili in contenitore, la pulizia deve essere effettuata alla presenza di un Incaricato del trattamento di tali dati. Durante l'accesso per la pulizia tutti i computers contenenti dati sensibili o giudiziari devono essere spenti (o in modalità salvaschermo con password di ripristino) oppure deve presenziare un Incaricato del trattamento di tali dati.

- Procedura di Protezione Dati **PP69: ingresso di persone esterne per manutenzione locali o impianti o attrezzature**

Stanze contenenti dischi di back-up : l'accesso di dipendenti o estranei per la manutenzione dei locali o delle attrezzature in tali stanze contenute, dev'essere effettuata solo con i contenitori chiusi a chiave. Se dati sensibili o giudiziari non sono chiudibili in contenitore, l'intervento deve essere effettuato alla presenza di un Incaricato del trattamento di tali dati. Durante l'accesso per l'intervento tutti i computers contenenti dati sensibili o giudiziari devono essere spenti oppure deve presenziare un Incaricato del trattamento di tali dati. Si noti che sottraendo un disco di back-up, un malintenzionato può ricostruire gli archivi della scuola, violando dati personali.

- Procedura di Protezione Dati **PP71: procedure ad ogni variazione degli Incaricati**

Se entra in servizio un Incaricato che ha accesso alle risorse informatiche il Responsabile o, in sua mancanza, il DGSA deve provvedere a fare in modo che sia in grado di ottenere un sistema di credenziali.

Se un Incaricato che ha accesso alle risorse informatiche cessa dal servizio o è assente per più di 6 mesi, il Responsabile o, in sua mancanza, il DGSA deve provvedere a fare in modo che sia annullato il suo sistema di credenziali.

- Procedura di Protezione Dati **PP73: scelta del software**

Nella scelta del software, va esplicitamente verificato se ogni programma è realizzato in modo da attuare le misure di sicurezza previste dal Codice. In particolare che sia consentito l'accesso multiplo basato su credenziali, che gli archivi siano cifrati, che i programmi che trattano sia dati non sensibili che dati sensibili siano in grado di archiviare quest'ultimi a parte e non li renda visibili insieme agli altri dati, ma sia necessario accedere specificamente ad essi, eventualmente con una seconda protezione con credenziali. Va richiesta una dichiarazione di conformità al D.Lgs 196/2003.

- Procedura di Protezione Dati **PP75: accesso ai dati in assenza dell'Incaricato**

Qualora, in caso di assenza dell'Incaricato assegnatario della dotazione informatica, si renda necessario per ragioni improrogabili l'utilizzo di dati accessibili in via esclusiva con i suoi codici di accesso è necessario rispettare le seguenti regole:

1) deve sussistere un'improrogabile necessità di accedere ai dati per ragioni di servizio;

2) deve essere verificata l'impossibilità o la notevole difficoltà di raggiungere l'Incaricato;

3) il Responsabile (il DGSA) apre la busta chiusa riposta in luogo sicuro dov'è scritta la password. Poi la mette in una nuova busta chiusa.

4) chi ha aperto la busta, comunica l'accesso effettuato al dipendente assente al momento del suo rientro e lo invita a modificare immediatamente la password.

Questa procedura è descritta in via cautelativa. Tutti gli incaricati hanno pari accesso ai dati, pertanto non si dovrebbe rendere necessario usufruire dei codici di accesso degli assenti.

- Procedura di Protezione Dati **PP77**: **protezione dal furto di computers portatili contenenti dati personali**

Chi sottraesse un computer portatile avrebbe la possibilità di accedere ai dati personali eventualmente in esso contenuti. Considerata la facilità con cui possono essere sottratti, tali computers non devono essere utilizzati per dati sensibili o giudiziari. Vanno rigorosamente chiusi in armadio di sicurezza o cassaforte quando non utilizzati.

4 - Trattamenti da parte dei docenti

Queste Istruzioni vanno applicate dalla categoria: Docenti.

- Procedura di Protezione Dati **PP79: registri**

I registri personali devono essere sempre custoditi in modo sicuro.

I registri di classe possono essere consultabili solo dagli insegnanti e dagli alunni della classe interessata e si deve vigilare perché non vi siano accessi non autorizzati. Al termine delle lezioni i docenti ed i collaboratori scolastici sono Incaricati di riporli in luogo sicuro.

Il registro dei verbali del consiglio di classe e qualunque altro registro di verbali degli organi collegiali, affidato per la scrittura, la firma o la consultazione, dev'essere mantenuto protetto da accessi non autorizzati e riconsegnato quanto prima al Dirigente o alla segreteria perché lo riponga in luogo sicuro.

- Procedura di Protezione Dati **PP81: certificazioni mediche e informazioni sullo stato di salute degli alunni**

I dati personali in grado di rivelare lo stato di salute sono classificati "sensibili" e quindi protetti dalla visione di terzi quando non sia strettamente necessaria. Quindi eventuali certificati medici vanno visionati solo se necessario. Nel caso di certificati per la riammissione a scuola l'insegnante che li riceve deve inserirli in busta chiusa da conservare in luogo sicuro. Per i certificati di esonero o limitazione presentati per educazione fisica, gli insegnanti non prendono visione dei certificati medici, ma solamente della concessione predisposta dalla segreteria. In presenza di problemi di salute particolari, anche gravi, con rischio per la vita dell'alunno (allergie con pericolo di shock anafilattico, asma con pericolo di soffocamento, diabete, epilessia, cardiopatie gravi, ecc.) o imbarazzanti (disturbi di continenza, ecc.), comunicati dai genitori o dall'interessato ai docenti, verrà concordato formalmente con gli esercenti la patria potestà o il diretto interessato (nel caso di maggiorenne) quale comportamento tenere circa il riserbo sull'informazione.

In casi eccezionali si provvederà a stipulare un protocollo di intesa con l'autorità sanitaria territoriale.

Anche informazioni su particolari diete seguite dall'alunno o per motivi di salute o per motivi religiosi sono da considerare dati sensibili, pertanto vanno rivelati solo nei casi strettamente necessari.

La documentazione relativa ad alunni portatori di handicap è un dato di massima sensibilità in quanto idoneo a rivelare lo stato di salute. Pertanto i documenti potranno essere visti soltanto dai docenti della classe e personale strettamente necessario, ed al termine riconsegnati immediatamente in segreteria.

- Procedura di Protezione Dati **PP83: elaborati contenenti notizie particolari o sensibili**

Il docente che rilevi in un elaborato dati personali o familiari particolarmente sensibili, dovrà verificare col dirigente Scolastico la "sensibilità" dei dati per decidere la modalità di trattamento e conservazione

- Procedura di Protezione Dati **PP85: gestione degli elenchi degli alunni**

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte del D.Lgs 196/2003. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola. Va comunque previamente chiesta l'autorizzazione al Dirigente perché potrebbe costituire atto illegittimo.

- Procedura di Protezione Dati **PP87: gestione di documenti scolastici**

In generale qualunque documento scolastico che contenga dati personali di qualcuno è sottoposto dal D.Lgs 196/2003 a una qualche forma di protezione, quindi va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va riconsegnato in segreteria per l'archiviazione.

5 - Trattamenti da parte dei membri di organi collegiali (anche esterni alla scuola)

Queste Istruzioni vanno applicate dalla categoria: membri di organi collegiali.

- Procedura di Protezione Dati **PP89: gestione di documenti scolastici**

In generale qualunque documento scolastico che contenga dati personali di qualcuno è sottoposto dal D.Lgs 196/2003 a una qualche forma di protezione, quindi va custodito in modo che altri possano visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va consegnato in segreteria per l'archiviazione.

L'obbligo è ancora più stringente se il dato è di tipo particolare, sensibile o giudiziario.

Chi avesse originale o copia di un tale documento deve custodirlo con cura dalla visione di terzi e riconsegnarlo alla segreteria appena non serve più. E' vietato conservarlo quando è cessato il motivo istituzionale per cui il dato è stato acquisito.

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte del D.Lgs 196/2003. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola. Va comunque previamente chiesta l'autorizzazione al Dirigente perché potrebbe costituire atto illegittimo.

6 - Trattamenti da parte dei Collaboratori Scolastici

Queste Istruzioni vanno applicate dalla categoria: Collaboratori Scolastici.

- Procedura di Protezione Dati **PP91: gestione di documenti scolastici.**

In generale qualunque documento scolastico che contenga dati personali di qualcuno è sottoposto dal D.Lgs 196/2003 a una qualche forma di protezione, quindi va custodito in modo che altri non possano visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va consegnato in segreteria per l'archiviazione.

L'obbligo è ancora più stringente se il dato è di tipo particolare, sensibile o giudiziario.

Chi avesse originale o copia di un tale documento deve custodirlo con elevatissima cura e cautela dalla visione di terzi e riconsegnarlo alla segreteria appena non serve più.

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte del D.Lgs 196/2003. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola. Va comunque previamente chiesta l'autorizzazione al Dirigente perché potrebbe costituire atto illegittimo.

Pertanto qualsiasi registro, elaborato, elenco, libretto personale, certificato, e in generale documento scolastico che contiene dati personali di qualcuno va custodito con cautela, impedendo che altri ne prendano visione, lo copino o se ne impadroniscano.

- Procedura di Protezione Dati **PP93: trasporto di documenti scolastici**

I documenti ricevuti aperti vanno immediatamente consegnati alla segreteria, senza prenderne visione. Se c'è il sospetto che si tratti di certificati medici, certificazioni relativi ai redditi, ecc. si deve offrire all'interessato una busta chiusa affinché ve li inseriscano.

Nel caso di trasporto di documenti alla posta o ad altri destinatari o di ricezione di documenti destinati alla scuola, vanno trattati con cura, protetti da accesso di terzi, mai lasciati incustoditi, consegnati appena possibile alla segreteria o al legittimo destinatario.

Nel caso di documenti da consegnare internamente alla scuola vanno adottate analoghe cautele.

Per i registri di classe i collaboratori scolastici assieme ai docenti sono Incaricati di riporli in luogo sicuro quando terminano le lezioni.

- Procedura di Protezione Dati **PP95: custodia**

Le stanze contenenti archivi e non presenziate devono essere mantenute chiuse e si deve intervenire immediatamente se un non-Incaricato vi accede.

Stanze contenenti archivi non posti in contenitori chiusi a chiave e in cui si conservano anche documenti sensibili o giudiziari sono ad accesso controllato, il che significa che la chiave è gestita dal DGSA o da un suo delegato "Custode delle chiavi". Chi dovesse accedere per manutenzioni o pulizie, deve farlo chiedendone il permesso, limitando, al massimo il tempo di permanenza ed evitando di lasciare la stanza incustodita o di farvi accedere altri; inoltre, se ritenuto necessario dal DGSA deve presenziare un addetto alla segreteria.

L'ufficio del Dirigente , la segreteria e gli uffici in genere vanno chiusi a chiave quando non presenziati dal relativo personale.

E' fatto divieto assoluto a chiunque non ne abbia ricevuto esplicita autorizzazione di accendere o utilizzare i computers della segreteria o della presidenza o che comunque contengano dati personali. Si deve intervenire immediatamente se una persona non autorizzata tenta di farlo.

Se esterni per motivi di manutenzione devono entrare nelle stanze citate o negli archivi per i quali è prevista la chiusura a chiave, vanno seguiti a vista; se questo è impossibile, vanno invitati a tornare in altro momento, a meno che non sia in atto un'emergenza urgente che richiede il loro intervento.

Fuori dall'orario di apertura della scuola non si deve far entrare nei locali citati alcun estraneo.

- Procedura di Protezione Dati **PP97: partecipazione alle procedure della segreteria**

Questa procedura è costituita dalla partecipazione alle procedure già indicate per la segreteria, che richiedono il supporto consapevole e attento dei Collaboratori Scolastici.

ALLEGATO 6 – elenco delle comunicazioni cartacee o telematiche di dati sensibili o giudiziari

COMUNICAZIONE DI DATI COMUNI

Dati comuni: COMUNICAZIONE AD ALTRI ENTI PUBBLICI

E' consentita solo se tale comunicazione è contemporaneamente:

- **necessaria** per lo svolgimento delle funzioni **istituzionali**
- **prevista da norma di legge o regolamento legislativo**, entro i limiti da questi stabiliti (però l'Informativa deve averlo indicato, altrimenti chi riceve i dati può usarli solo dopo aver dato una nuova informativa all'Interessato)

OPPURE

- necessaria per le funzioni istituzionali più silenzio-assenso dopo 45 gg su richiesta del Garante (art.39). Notare che c'è l'obbligo di comunicazione al Garante.

In assenza di una norma di legge o di regolamento generale questo tipo di comunicazione è proibita.

Il realizzarsi delle condizioni sopra elencate è un tassativo presupposto di legittimità della comunicazione. Significa che al di fuori di questi criteri, la comunicazione diviene illegittima, può comportare nullità degli atti e , in certi casi, reato penale punito con l'arresto.

Dati comuni: COMUNICAZIONE A PRIVATI

E' consentita solo se tale comunicazione è contemporaneamente:

- **necessaria per lo svolgimento delle funzioni istituzionali**
- **prevista da norma di legge o regolamento legislativo, entro i limiti da questi stabiliti (però l'Informativa deve averlo indicato, altrimenti chi riceve i dati può usarli solo dopo aver dato una nuova informativa all'Interessato)**

In assenza di una norma di legge o di regolamento generale questo tipo di comunicazione è proibita.

Il realizzarsi delle condizioni sopra elencate è un tassativo presupposto di legittimità della comunicazione. Significa che al di fuori di questi criteri, la comunicazione diviene illegittima, può comportare nullità degli atti e , in certi casi, reato penale punito con l'arresto.

Dati comuni: DIFFUSIONE

E' consentita solo se tale comunicazione è contemporaneamente:

- **necessaria per lo svolgimento delle funzioni istituzionali**
- **esplicitamente prevista da norma di legge o regolamento legislativo, entro i limiti da questi stabiliti (però l'Informativa deve averlo indicato, altrimenti chi riceve i dati può usarli solo dopo aver dato una nuova informativa all'Interessato)**

Naturalmente l'ente pubblico ha spesso addirittura l'obbligo di legge di diffondere dati, nel caso di graduatorie di concorsi, esiti di esami e scrutini, appalti di opere pubbliche, ecc. In questi casi lo spirito della legge è che determinate informazioni devono essere conoscibili da tutti affinché l'opinione pubblica eserciti un controllo sull'operato dell'ente.

Il realizzarsi delle condizioni sopra elencate è un tassativo presupposto di legittimità della diffusione. Significa che al di fuori di questi criteri, la diffusione diviene illegittima, può comportare nullità degli atti, obbligo di risarcimento in sede civile e , in certi casi, reato penale punito con l'arresto.

In assenza di una norma di legge o di regolamento generale che esplicitamente preveda la diffusione, essa è proibita.

Va sottolineato la diffusione deve essere esplicitamente prevista da norma di legge o regolamento legislativo, ma va effettuata entro i limiti da questi stabiliti.

COMUNICAZIONE DI DATI SENSIBILI O GIUDIZIARI : gli unici casi leciti perché autorizzati espressamente dal "Regolamento dati sensibili e giudiziari".

Trattamento N. 1 -Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente, dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato (Il trattamento concerne tutti i dati, anche sensibili e giudiziari, in alcuni casi anche di familiari o terzi, relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro) (vedi Scheda 1 del "Regolamento" di cui al Decreto n. 305/2006 approvato dal M.P.I.)

Dati Sensibili o Giudiziari : DIFFUSIONE: IN NESSUN CASO

Dati Sensibili o Giudiziari : INTERCONNESSIONI E RAFFRONTI CON ALTRO TITOLARE:

- Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;

Dati Sensibili o Giudiziari : COMUNICAZIONE
Solo ai seguenti soggetti per le seguenti finalità:

- **Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;**
- Organi preposti al riconoscimento della **causa di servizio/equo indennizzo**, ai sensi del D.P.R, n. 29 ottobre 2001, n. 461.(Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermità da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonché per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie)
- Organi preposti alla **vigilanza in materia di igiene e sicurezza sui luoghi di lavoro** (d.lg. n. 626/1994 norme in materia di prevenzione e sicurezza nei luoghi di lavoro).
- **Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza** a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o **infortuni sul lavoro a**i sensi del D.P.R. n. 1124/1965 (testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali).
- Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della Legge 12 marzo 1999, n. 68 (Norme per il diritto al lavoro dei disabili) Norme per il diritto al lavoro dei disabili
- **Organizzazioni sindacali** per gli adempimenti connessi al **versamento delle quote di iscrizione e per la gestione dei permessi sindacali;**
- Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- **Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica** ai sensi della Legge 18 luglio 2003, n. 186 (Norme sullo stato giuridico degli insegnanti di religione cattolica degli istituti e delle scuole di ogni ordine e grado).
- **Organi di contro**llo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa **dei provvedimenti di stato giuridico ed economico del personale** ex Legge 14 gennaio 1994, n. 20 (Disposizioni in materia di giurisdizione e controllo della Corte dei Conti.) e D.P.R. 20 febbraio 1998, n. 38 (Regolamento recante le attribuzioni dei dipartimenti del ministero del tesoro, del bilancio e della programmazione economica, nonché disposizioni in materia di organizzazione e di personale, a norma dell'articolo 7, comma 3, della legge 3 aprile 1997, n. 94)
- **Agenzia delle Entrate: ai fini degli obblighi fiscali del personale** ex:

  - Legge 30 dicembre 1991, n. 413 (disposizioni per ampliare le basi imponibili, per razionalizzare, facilitare e potenziare l'attività di accertamento; disposizioni per la valutazione obbligatoria dei beni immobili delle imprese, nonché per riformare il contenzioso e per la definizione agevolata dei rapporti tributari pendenti; delega al Presidente della Repubblica per la concessione di amnistia per reati tributari; istituzioni dei centri di assistenza fiscale e del conto fiscale);

- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335 (Riforma del sistema pensionistico obbligatorio e complementare).

- **Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive** (art. 50, comma 3, D.Lgs.30 marzo 2001, n. 165 - Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche. Il comma 3 recita: " 3 . Le amministrazioni pubbliche sono tenute a fornire alla Presidenza del Consiglio dei ministri - Dipartimento della funzione pubblica - il numero complessivo ed i nominativi dei beneficiari dei permessi sindacali.").

Trattamento N. 2- Gestione del contenzioso e procedimenti disciplinari (Il trattamento concerne tutti i dati, anche sensibili e giudiziari, necessari o indispensabili alle attività relative alla difesa in giudizio nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili) (vedi Scheda 2 del "Regolamento" di cui al Decreto n. 305/2006 approvato dal M.P.I.)

Dati Sensibili o Giudiziari : DIFFUSIONE: IN NESSUN CASO

Dati Sensibili o Giudiziari : INTERCONNESSIONI E RAFFRONTI CON ALTRO TITOLARE: IN NESSUN CASO

Dati Sensibili o Giudiziari : COMUNICAZIONE ad altri soggetti pubblici o privati
Solo ai seguenti soggetti per le seguenti finalità:

- Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento **dei tentativi obbligatori di conciliazione** dinanzi a Collegi di conciliazione ex D.Lgs.30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.);
- **Organi arbitrali:** per le svolgimento delle procedure arbitrali ai sensi dei CCNL dì settore;
- **Avvocature dello Stato**: per la difesa erariale e consulenza presso gli organi di giustizia;
- **Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria:** per l'esercizio dell'azione di giustizia;
- **Liberi professionisti, ai fini di patrocinio o di consulenza**, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Trattamento N. 3 - Organismi collegiali e commissioni istituzionali (Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali. Il trattamento concerne tutti i dati, anche sensibili, in alcuni casi anche di familiari o terzi, necessari o indispensabili per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme dell'ordinamento scolastico, nonché i dati comuni necessari alla gestione di tali organismi.) (vedi Scheda 3 del "Regolamento" di cui al Decreto n. 305/2006 approvato dal M.P.I., relativa alla sola attivazione di tali organismi)

Dati Sensibili o Giudiziari : DIFFUSIONE: IN NESSUN CASO

Dati Sensibili o Giudiziari : INTERCONNESSIONI E RAFFRONTI CON ALTRO TITOLARE: IN NESSUN CASO

Dati Sensibili o Giudiziari : COMUNICAZIONE ad altri soggetti pubblici o privati: **IN NESSUN CASO**

Trattamento N. 4 - Attività propedeutiche all' avvio dell'anno scolastico (Il trattamento concerne tutti i dati, necessari o indispensabili, in alcuni casi anche di familiari o terzi, forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio oppure forniti ad altre istituzioni scolastiche per le stesse finalità)

Dati Sensibili o Giudiziari : DIFFUSIONE: IN NESSUN CASO

Dati Sensibili o Giudiziari : INTERCONNESSIONI E RAFFRONTI CON ALTRO TITOLARE: IN NESSUN CASO

Dati Sensibili o Giudiziari : COMUNICAZIONE ad altri soggetti pubblici o privati. Solo ai seguenti soggetti per le seguenti finalità:

a) agli Enti Locali per la fornitura dei servizi ai sensi del D.Lgs. 32 marzo 1998, n. 112 , limitatamente ai dati indispensabili all'erogazione del servizio (Il D.Lgs tratta: Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59)

b) ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;

c) **alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap** di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n.104 (Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate pubblicato sulla GU 17.02.1992 N. 39 SO; Materia: handicap -anche di familiari-, pubblico impiego e servizi pubblici, Assistenza, previdenza e assicurazioni).

Trattamento N. 5 - Attività educativa, didattica e formativa, di valutazione (Il trattamento concerne tutti i dati, anche sensibili e giudiziari, necessari o indispensabili all'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami) (vedi Scheda 4 del "Regolamento" di cui al Decreto n. 305/2006 approvato dal M.P.I.)

Dati Sensibili o Giudiziari : DIFFUSIONE: IN NESSUN CASO

Dati Sensibili o Giudiziari : INTERCONNESSIONI E RAFFRONTI CON ALTRO TITOLARE: IN NESSUN CASO

Dati Sensibili o Giudiziari : COMUNICAZIONE ad altri soggetti pubblici o privati
Solo ai seguenti soggetti per le seguenti finalità:

- **Alle altre istituzioni scolastiche, statali e non statali, per** la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
- agli **Enti Locali per** la fornitura dei servizi ai sensi del D.Lgs. 32 marzo 1998, n. 112 , limitatamente ai dati indispensabili all'erogazione del servizio (Il D.Lgs tratta: Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59)
- ai **gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica**, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
- **agli Istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;**
- **all'INAIL per la denuncia di infortuni** ai sensi del D.P.R. n. 1124/1965 (testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali).
- **alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione** e la verifica del Piano Educativo Individuale, ai sensi della Legge 5 febbraio 1992,

n.104 (Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate pubblicata sulla GU 17.02.1992 N. 39 SO; Materia: handicap -anche di familiari-, pubblico impiego e servizi pubblici, Assistenza, previdenza e assicurazioni).

- **ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro,** ai sensi della Legge 24 giugno 1997, n. 196 (1) e del D. Lgsl. 21 aprile 2005, n. 77 (2) e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio.
(1) Tratta di: Norme in materia di promozione dell'occupazione.
(2) Tratta di: Definizione delle norme generali relative all'alternanza scuola-lavoro, a norma dell'articolo 4 della legge 28 marzo 2003, n. 53. (GU n. 103 del 05/05/2005)

Trattamento N. 6 – Rapporti scuola – famiglie : gestione del contenzioso (Il trattamento concerne tutti i dati, anche sensibili e giudiziari, in alcuni casi anche di familiari o terzi, necessari o indispensabili, alle attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni denunce all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, nonché tutte le attività relative alla difesa in giudizio) (vedi Scheda 7del "Regolamento" di cui al Decreto n. 305/2006 approvato dal M.P.I.)

Dati Sensibili o Giudiziari : DIFFUSIONE: IN NESSUN CASO

Dati Sensibili o Giudiziari : INTERCONNESSIONI E RAFFRONTI CON ALTRO TITOLARE: IN NESSUN CASO

Dati Sensibili o Giudiziari : COMUNICAZIONE ad altri soggetti pubblici o privati : IN NESSUN CASO

Trattamento N. 7 – Fornitori e clienti (Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, necessari alle attività di vendita, acquisto o fornitura di beni, servizi o consulenze).

Trattamento N. 8 – Gestione finanziaria e contabile (Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, necessari alle attività di gestione finanziaria e contabile e all'amministrazione del bilancio)

Trattamento N. 9 – Gestione Istituzionale (Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, non compresi nei precedenti trattamenti e necessari per la gestione dell'attività istituzionale)

Tr.10 - Gestione sito web dell'istituto

Gestione sito web dell'istituto (Il trattamento concerne solo dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, per le quali apposita disposizione di legge prevede la possibilità di diffusione**)**

Dati Sensibili o Giudiziari : DIFFUSIONE: IN NESSUN CASO

Dati Sensibili o Giudiziari : INTERCONNESSIONI E RAFFRONTI CON ALTRO TITOLARE: IN NESSUN CASO

Dati Sensibili o Giudiziari : COMUNICAZIONE ad altri soggetti pubblici o privati: IN NESSUN CASO

Alcuni esempi

Questi esempi servono per comprendere meglio nel concreto come si applicano le regole e quali comunicazioni sono lecite.

Alunni: comunicazioni

a) Consegna di elenchi diplomati alle aziende che lo richiedono, contenente dati comuni e particolari: mai con votazione: gli alunni sono inseriti in questi elenchi solo su richiesta. Solo dati comuni, autorizzato dall'art. 96 del Codice privacy

b) Comunicazione di dati comuni degli alunni per stage o altre attività di orientamento-formazione professionale: Solo dati comuni, autorizzato dall'art. 96 del Codice privacy, ma l'alunno deve richiederlo espressamente o almeno autorizzarlo.

c) Nel caso di scuole con mensa, comunicazione e di particolari prescrizioni dietetiche che siano idonee a rivelare la religione professata o lo stato di salute (dati sensibili). Autorizzato dal Regolamento, scheda 5

d) Gestione di pratiche per la partecipazione di alunni a tirocini formativi/stages: implica solo dati comuni, autorizzato dall'art. 96 del Codice privacy

Dati neutri

e) Gestione delle pratiche relative alla determinazione del numero delle classi e del relativo organico (dati anonimi); in alcuni casi la presenza di alunni con handicap implica uno specifico riferimento e la possibilità di risalire in forma indiretta all'interessato (dato potenzialmente sensibile)

f) Gestione di statistiche in genere sugli alunni (dati anonimi) e invio delle stesse ad enti pubblici. Redazione di statistiche per l'analisi della dispersione scolastica e rispetto dell'obbligo scolastico (dato anonimo)

g) Gestione dell'iter per l'adozione dei testi scolastici (dati comuni o neutri)

h) Trattamento della determinazione del Calendario scolastico

i) Gestione del POF (Piano Offerta Formativa (dati neutri)

Atti rari o straordinari

j) Partecipazione alla gestione delle pratiche relative ad eventuali denunce per violazioni penali (dato giudiziario). Comunicazione di eventuali atti giudiziari per casi particolari (e rarissimi): dato giudiziario da trattare con estrema cautela. Autorizzato da schede 2 e 7 del Regolamento, ma con limiti.

k) Partecipazione agli atti relativi all'applicazione dell'obbligo scolastico a casi particolari (dati anche particolari o sensibili). Eventuali atti riferiti a interventi dell'autorità per inosservanza dell'obbligo scolastico (dato particolare e in alcuni casi sensibile). Autorizzato da scheda 7 del Regolamento.

l) Per chi è trasferito ad altra scuola pubblica, a quest'ultima viene trasmesso un foglio notizie e la parte rilevante del Fascicolo Personale (documenti anagrafici, documenti scolastici eventuale certificato di vaccinazione*),* mentre non vengono allegati eventuali certificati medici*.* Supporto: documenti cartacei. Se sono semplici dati comuni la comunicazione è autorizzata da norma di legge. Se sono dati sensibili indispensabili, è autorizzata dal Regolamento, scheda 4.

m) Ad altra scuola di grado superiore per prescrizioni. Supporto: documenti cartacei . Solo dati comuni, previsto da norma di legge.

n) Elenchi anagrafici contenenti dati comuni, ad ASL (se richiesti per controlli o per organizzazione di attività mediche a favore degli alunni), altre istanze organizzative dell'organizzazione dell'istruzione pubblica per graduatorie o simili, ad enti pubblici e a privati in occasione di visite guidate, viaggi e simili. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax. Solo se tali comunicazioni sono previste da norma di legge. Per dati sensibili, solo se autorizzate dalla scheda 4 o 5 del Regolamento.

o) A Inail e Questura per denuncia infortuni . Supporto: documenti cartacei . Eventualmente anche a Società assicuratrice privata. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax. Se trattasi di dati sensibili, comunicazione autorizzata dal Regolamento, schede 1, 4, 5.

p) Trasmissione ad enti pubblici di particolari pratiche, su richiesta dell'interessato, per ottenere determinati benefici. Supporto: documenti cartacei. Solo se tali comunicazioni sono autorizzate da norma di legge. Per dati sensibili, solo se autorizzate dalla scheda 4 o 5 del Regolamento.

q) Statistiche (dati anonimi) a enti locali e ad altre istanze organizzative dell'organizzazione dell'istruzione pubblica. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax. Essendo dati neutri, non serve alcuna autorizzazione di legge.

r) Corrispondenza con enti pubblici di supporto alla didattica, alla ricerca didattica, ai sistemi di valutazione,ecc. Non richiedono dati sensibili oppure solo dati identificativi. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax. Non serve alcuna autorizzazione di legge.

s) Corrispondenza con organismi pubblici italiani e dell'U.E. e altre scuole straniere per la gestione di progetti speciali. Non richiedono dati sensibili oppure solo dati identificativi. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax.. Non serve alcuna autorizzazione di legge.

t) Comunicazione dati anonimi per adozione libri di testo, anche a privati. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax. Essendo dati neutri, non serve alcuna autorizzazione di legge.

u) Pubblicazione all'albo di prospetti con esiti scolastici intermedi, finali, di ammissione a esami, di risultato degli esami, nonché di elenchi di ammessi all'Istituto o ad altre iniziative. Supporto: documenti cartacei.

Non è una comunicazione, bensì una diffusione. Il garante ha chiarito che è dovuta per legge. Però vanno osservate determinate cautele ben note.

v) Ad altri enti pubblici per conferma del titolo di studio conseguito presso la scuola. E' un dato comune, la richiesta può essere esaudita solo se motivata da una norma di legge.

Personale : comunicazioni

a) Gestione della dichiarazione di iscrizione a un sindacato con delega al versamento mensile dei contributi (dato sensibile), gestione diretta delle ritenute sindacali o trasmissione al Tesoro per via cartacea. Previsto dal Regolamento, scheda 1.

b) Trasmissioni dati per ritenute per sciopero al Ministero del Tesoro (dato sensibile) per via cartacea o telematica. Previsto dal Regolamento, scheda 1.

c) Gestione materiali sindacali, circolari, proclamazioni di sciopero, gestione contratto integrativo della scuola, rapporti con RSU e sindacati

d) Gestione richieste, certificazioni, dichiarazioni e concessioni in relazione a permessi e distacchi per attività sindacali (dato sensibile). Autorizzato dal regolamento scheda 1.

e) Eventuale cartella sanitaria ai sensi del D.lgs 626 (custodita in busta chiusa): dato sensibile ed eventuale giudizio di idoneità o inidoneità al lavoro (dato sensibile). corrispondenza con dipendenti su particolari situazioni personali o professionali (dati particolari o sensibili). Per consegnarla al medico competente o al RSPP esterno bisogna nominarli Incaricati esterni.

f) Comunicazioni per controversie di lavoro. Autorizzato dal regolamento, scheda 2.

g) Eventuali denunce per violazioni penali (dato giudiziario). Autorizzato dal Regolamento, scheda 2.

h) Comunicazioni relative a dipendenti che usufruiscano di permessi o aspettative perché ricoprono cariche pubbliche: dato potenzialmente sensibile. Autorizzato dal Regolamento, scheda 1, ma entro limiti.

i) Trasmissione per via telematica al MIUR di dati anonimi per statistiche e gestione organico (dati anonimi), ivi compresi dati anonimi sulle statistiche di partecipazione a scioperi. Non serve autorizzazione, essendo dati anonimi.

j) Per chi è trasferito ad altra scuola pubblica, a quest'ultima viene trasmesso un foglio notizie e la parte rilevante del Fascicolo Personale (documenti anagrafici, documenti scolastici di attualità, mentre eventuali certificati medici sono esclusi). Supporto: documenti cartacei. Comunicazione autorizzata da legge, se dato sensibile è autorizzato dal Regolamento, scheda 1.

k) Comunicazione ad altre scuole o da altre scuole di assunzione in servizio, di assenze , di particolari concessioni e di altri atti nel caso di docenti utilizzati a scavalco da più scuole; di orario scolastico, di impegni per riunioni, ecc., di partecipazione ad esami ed altri attività. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax. Comunicazione autorizzata da legge, se dato sensibile è autorizzato dal Regolamento, scheda 1.

l) Comunicazione ad altra scuola o al MPI di dati per graduatorie. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax. . Comunicazione di dati comuni autorizzata da legge, se dato sensibile, è autorizzato dal Regolamento, scheda 1.

m) Documentazione da trasmettere al CAF per il mod. 730, contenente notizie sul reddito annuo e sul patrimonio (dati particolari) e sul conferimento dell'8 per mille a chiese od organizzazioni religiose (dato sensibile): ricevuta in busta chiusa per la trasmissione al CAF. Supporto: documenti cartacei in busta chiusa. Comunicazione di dati comuni autorizzata da legge, se dato sensibile, è autorizzato dal Regolamento, scheda 1..

n) Trasmissione a enti pubblici di domande di prestiti, cessione del quinto ecc., a volte motivate con ragioni personali o familiari particolari o sensibili. Supporto: documenti cartacei. Comunicazione di dati comuni autorizzata da legge, se dato sensibile, è autorizzato dal Regolamento, scheda 1.

o) Trasmissione ad enti pubblici di particolari pratiche, su richiesta del dipendente, per ottenere determinati benefici. Supporto: documenti cartacei. Comunicazione di dati comuni autorizzata da legge, se dato sensibile. Bisogna controllare se è autorizzato dal Regolamento, scheda 1.

p) Trasmissione al Tesoro per via cartacea dei compensi accessori a fine del conguaglio fiscale. Supporto: documenti cartacei. Comunicazione di dati comuni, autorizzata da legge.

q) A Inail e Questura per denuncia infortuni . Supporto: documenti cartacei . Eventualmente anche a Società assicuratrice privata, previo consenso se trattasi di dati sensibili. Supporto: documenti cartacei **o messaggi di posta elettronica** o fax. Comunicazione prevista dal regolamento, scheda 1 (per gli alunni, scheda 5)

Altre comunicazioni:

a) Corrispondenza con gli interessati. Supporto: documenti cartacei o messaggi di posta elettronica o fax. Non è una comunicazione, perché il destinatario unico è l'Interessato.

b) Trasmissione cartacea o telematica al Dipartimento della Funzione Pubblica dei dati personali , retributivi e fiscali di collaboratori esterni relativamente alle prestazioni economiche per anagrafe delle prestazioni.

Supporto: documenti cartacei o messaggi di posta elettronica o fax o utilizzo di comunicazioni con emulatore di terminale sulla base di programmi gestiti da tale ente e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali.

c) Comunicazione e ricezione di dati anonimi e neutri al MPI e altri enti pubblici. Supporto: documenti cartacei o messaggi di posta elettronica o fax o utilizzo di comunicazioni con emulatore di terminale sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali.

All.7 - Mansionario D.Lgs 196/2003 e Piano di formazione degli Incaricati

19.2) Distribuzione dei compiti e delle responsabilità (regola 19.2)

Tabella 2.1. Strutture preposte ai trattamenti.

1	2	3	4
Struttura:	**Responsabile:**	**Trattamenti operati dalla struttura:**	**Compiti della struttura:**
Dirigente Scolastico	Dirigente Scolastico	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate
INCARICATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE:			
Collaboratori del DS	Dirigente Scolastico	Tutti (potenzialmente)	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Segreteria	D.G.S.A.	Tutti Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Corpo Docente	Dirigente Scolastico	Tr.3, Tr.4, Tr.5, Tr.7, Tr.8, Tr.9, Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc,)
Collaboratori scolastici	D.G.S.A.	Tutti, ma con attività di supporto. Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni, docenti e familiari
Membri ESTERNI di Organi Collegiali	Dirigente Scolastico	Tr.3 e tutti gli altri (tranne Tr.6) limitatamente alle strette esigenze della funzione	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché il CDI e la GE decisioni di tipo amministrativo, finanziario, regolamentare
INCARICATI INTERNI CON COMPITI SPECIFICI O ULTERIORI:			
Incaricato del Backup periodico	Responsabile dei trattamenti in questione	Tutti, ma limitatamente alla funzione	Esegue il backup almeno settimanale degli archivi informatici contenenti dati personali. .
Custode delle chiavi degli archivi ad accesso controllato. E vice-custode delle chiavi.	Responsabile dei trattamenti in questione	Tutti i trattamenti non informatici, ma limitatamente alla funzione	E' l'unico detentore delle chiavi degli archivi ad accesso controllato e consegna all'Incaricato autorizzato all'accesso a un certo archivio la relativa chiave; la riceve di ritorno non appena cessata l'attività. Il vice lo sostituisce in caso di assenza.
Custode delle passwords	Responsabile dei trattamenti in questione	Tutti i trattamenti informatici , ma limitatamente alla funzione	Da ogni Incaricato munito di accesso al computer mediante password, ad ogni scadenza della password (3 mesi) riceve una busta chiusa contenente la password, da tenere a disposizione in caso di necessità di accesso agli archivi elettronici di quell'Incaricato quando è assente

Addetti al S.P.P.,	Dirigente Scolastico	I trattamenti relativi all'applicazione della normativa 81 o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e commissioni istituzionali Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	Applicazione normativa Dlgs 81/2007 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale
RLS – rappresentante dei lavoratori per la sicurezza	Nessuno in questa funzione	Diritto di consultazione di tutti i documenti e materiali informatici strettamente inerenti alla funzione e risultanti come diritto di conoscenza	Contributo all'applicazione normativa Dlgs 81/ e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale; verifica ecc.
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap	Dirigente Scolastico	tutti i trattamenti informatizzati e non relativi all'attività Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	Gestione di alunni con handicap didattico grave
AMMINISTRATORE DI SISTEMA	Dirigente Scolastico	I trattamenti informatici rigorosamente nei limiti relativi alle funzioni	Creazione degli account utente con consegna delle credenziali delle credenziali, eliminazione di account non più in uso, impostazione e supervisione del backup ed esecuzione delle prove e verifiche nonché delle procedure di "disaster recovery"
RESPONSABILI INTERNI DI TRATTAMENTO:			
RESPONSABILE DI TRATTAMENTO: Direttore Servizi Generali Amm.vi	Dirigente Scolastico	Tutti i trattamenti, limitatamente alla gestione amministrativo-contabile e alla gestione delle attività dei Collaboratori Scolastici.	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
INCARICATI ESTERNI:			
RSPP	Dirigente Scolastico	I trattamenti relativi all'applicazione della normativa 626 o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e	Applicazione normativa Dlgs 626/1994 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale

		commissioni istituzionali Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	
Incaricato Tecnico Esterno della Manutenzione del software e dell'Hardware e coordinatore del "Disaster recovery" e delle prove di ripristino	Dirigente Scolastico	tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni	Manutenzione dell'hardware dei computers. Coordina l'impostazione del piano di recupero in caso di disastro informatico che comporti l'inagibilità del sistema o la perdita di dati personali. Coordina le prove obbligatorie di efficienza del backup e di ripristino dei dati dalla copia di salvataggio
Educatore esterno – Tirocinante	Dirigente Scolastico	i seguenti trattamenti non informatici: Tr.4 - Attività propedeutiche all' avvio dell'anno scolastico Tr.5 - Attività educativa e formativa, , rigorosamente nei limiti relativi alle funzioni	Attività di animazione ed educazione a favore degli alunni della scuola; sostegno a favore degli alunni portatori H

2) Formazione

19.6 Pianificazione degli interventi formativi previsti (regola 19.6)

Tab. 6.1

INCARICATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE:	**Formazione prevista tra il 31.03.2011 e il 31.3.2012**
Tutta la segreteria	**Studio delle nuove informative** Studio delle problematiche di migrazione dall'albo cartaceo a quello on-line ***Per la formazione sarà utilizzato il manuale sulle <NUOVE INFORMATIVE> .*** Numero persone da formare: 7 Periodo previsto: Luglio 2011
Tutti gli Incaricati e i responsabili che utilizzano computers	**1)** ***Le problematiche relative al REGOLAMENTO SULL'USO DEI COMPUTERS E DI INTERNET Per la formazione sarà utilizzato il manuale <GESTIONE COMPUTER-INTERNET (AGGTO 2011)>*** **2) Applicazione del Provvedimento del Garante in materia di *amministratori di sistema o assimilatI. Cod. 270*** **3)** ***E' prevista per luglio 2011 anche una formazione sull'argomento per i nostri Incaricati o responsabili che risulteranno definibili "amministratorl di sistema o assimilatI" e per tutti gli Incaricati e Responsabili che utilizzano computers.*** ***Per la formazione sarà utilizzato il manuale già acquisito.*** Numero persone da formare: 7 ***2) Formazione su le nuove misure minime di sicurezza nella gestione e cancellazione dei supporti informatici (Provvedimento a carattere generale del garante, ottobre 2008): è stato acquisito il kit Cod. 185 comprendente un corso di formazione illustrato.*** Numero persone da formare: 7

	Periodo previsto: Luglio 2011
Collaboratori del DS	Numero persone da formare: 0 Numero di persone già formate: 2 E già stato fornito il <Kit formazione privacy>, manuale completo divulgativo sulla privacy, consultabile a video, anche navigando tra files, e stampabile. ***Sarà comunque effettuata una formazione su le nuove misure minime di sicurezza nella gestione e cancellazione dei supporti informatici (Provvedimento a carattere generale del garante, ottobre 2008): è stato acquisito il kit Cod. 185 comprendente un corso di formazione illustrato.***
Corpo Docente	Numero persone da formare: 37 Numero di persone già formate: 82 Nel corso delle periodiche riunioni degli Organi Collegiali il Titolare illustrerà l'argomento e se ne potrà discutere. Si inviterà anche un esperto per una breve relazione. Il tema principale sarà le novità e soprattutto le nuove chiarezze introdotte dal <Regolamento dati sensibili> in vigore dal 2007. Si approfondirà in particolare il tema: "Dati sensibili: è vietato chiedere agli alunni dati sensibili che non siano strettamente indispensabili per l'attività formativa." **Periodo:** maggio 2011 e novembre 2011 Si prenderà in esame anche IL VADEMECUM DEL GARANTE PRIVACY SULLA SCUOLA. E' prevista la distribuzione all'inizio del prossimo anno scolastico (settembre-ottobre) di unl facsimile del VADEMECUM
Collaboratori sc. e personale ausiliario	Numero persone da formare: 3 Numero di persone già formate: 16 Viene fornito il <Compendio di livello base > della normativa privacy. Ma soprattutto si farà affidamento su alcune riunioni con illustrazione del tema fatta in modo semplice ed elementare da parte del Titolare o del DGSA.. **Periodo:** maggio 2011 e novembre 2011
Membri ESTERNI di Organi Collegiali	Numero persone da formare: 88 Numero di persone già formate: 0 Viene fornito il <Compendio di livello base > della normativa privacy (uno dei files del <Kit formazione privacy>) Nel corso delle periodiche riunioni degli Organi Collegiali il Dirigente illustrerà brevemente l'argomento e se ne potrà discutere. Si inviterà anche un esperto per una breve relazione. **Periodo:** maggio 2011 e novembre 2011
INCARICATI INTERNI CON COMPITI SPECIFICI O ULTERIORI:	
Incaricato del Backup periodico	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Custode delle chiavi degli archivi ad accesso controllato. E vice-custode delle chiavi.	[x] Già formato [ ] Da formare Viene fornito - MANUALE 'GESTIONE DEGLI ARCHIVI' NELLA PRIVACY , una **Guida per una miglior gestione degli archivi** E' previsto un breve colloquio con il DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Custode delle passwords	[x] Già formato [ ] Da formare Viene fornito - GUIDA COMPLETA ALLA GESTIONE DELLE PASSWORD, **una guida per una miglior organizzazione della gestione delle passwords.** E' previsto un breve colloquio con il DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Addetti al S.P.P.	[x] Già formato [ ] Da formare Viene fornito E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap	Numero persone da formare: 6 Numero di persone già formate: 6 E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e settembre 2011
Personale incaricato della creazione e gestione del sito web [	Numero persone da formare: 1 Numero di persone già formate: 0 Vengono forniti: 1) Manuale < NUOVE INFORMATIVE (AGGIORNATO 2011)>, da leggere per la parte che riguarda il sito 2) il <Compendio di livello avanzato > della normativa privacy E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011

AMMINISTRATORI DI SISTEMA ED ASSIMILATI	
[VEDI ELENCO AMMINISTRATORI, compila una riga per ciascuno)	[x] Già formato [ ] Da formare Viene fornito il manuale sul tema specifico del Provvedimento riguardante gli AdS e Assimilati
RESPONSABILI INTERNI DI TRATTAMENTO:	
RESPONSABILE DI TRATTAMENTI: Direttore Servizi Generali Amm.vi	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
INCARICATI ESTERNI:	
RSPP . ai sensi del Dlgs 626/1994.	[x] Già formato [ ] Da formare E' previsto un breve colloquio con il Dirigente per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Incaricato Tecnico Esterno della Manutenzione del Software	[x] Già formato [ ] Da formare Viene fornito: 1) il Manuale <Amministratore di sistema e assimilati> (2) il Manuale sulla cancellazione definitiva dei supporti di memoria **Periodo:** maggio 2011 e novembre 2011
Incaricato Tecnico Esterno della Manutenzione del dell'Hardware	[x] Già formato [ ] Da formare Viene fornito il <Compendio di livello base > E' previsto un breve colloquio con il Dirigente o del DSGA per verifica e approfondimento. **Periodo:** maggio 2011 e novembre 2011
Docente o animatore Esterno	[ ] Già formato [x] Da formare Viene fornito il <Compendio di livello base > della normativa privacy (uno dei files del <Kit formazione privacy>) E' previsto un breve colloquio con il Dirigente o del DSGA per verifica e approfondimento. **Periodo:** al momento dell'incarico
RESPONSABILI ESTERNI:	

Allegato 8 - Piano di back-up, disaster-recovery, di continuità, nonché misure per garantire l'integrità e la disponibilità dei dati

Analisi delle conseguenze dell'eventuale perdita di dati

Va premesso che i dati trattati dalla scuola in forma elettronica sono moderatamente importanti in se stessi; non è un Ospedale o un centro paghe o un ufficio anagrafe. Anche il grado di urgenza con cui all'Interessato possono servire i documenti necessariamente prodotti tramite computer è decisamente molto più basso rispetto a questi esempi.
Infine va osservato che i dati trattati dalla scuola in forma elettronica non sono, per ora, mai degli originali, bensì servono:

- per produrre documenti cartacei che sono conservati e che sono gli unici documenti ad avere valore legale
- per elaborare dati provenienti da documenti cartacei che sono conservati e che sono gli unici documenti ad avere valore legale
- per produrre comunicazioni ad altri Enti (Tesoro, Ministero della Funzione Pubblica, MPI, ecc.) e cessa la necessità di conservarli in forma elettronica non appena la comunicazione ha avuto effetto.
- per ricevere comunicazioni provenienti dall'esterno, delle quali di norma si fa immediatamente la copia cartacea, che viene poi conservata e che è l'unica ad avere valore legale. L'unica eccezione sono determinati allegati che non si ritiene utile stampare e determinati programmi che non è, ovviamente, possibile stampare. In entrambi i casi non si tratta mai di dati personali, né di software che tratti dati personali.

Quando si arriverà a implementare la firma elettronica e l'esistenza di documenti elettronici che di per sé costituiscano "originali" la situazione potrà cambiare.

Il programma per il protocollo

Poiché esiste un periodico back-up, le analisi che seguono riguardano la perdita di dati non ancora salvati (quindi una settimana al massimo, circa).
Il dato elettronico la cui perdita che creerebbe più problemi è il protocollo informatizzato, in quanto viene stampato con un certo ritardo rispetto alle registrazioni, quindi la perdita delle predette registrazioni creerebbe una seria difficoltà, in gran parte, però, rimediabile perché esistono comunque sempre i documenti cartacei con il timbro di protocollo e il relativo numero attribuito. Tuttavia sarebbe estremamente laborioso ritrovare tutti i documenti cartacei necessari a ricostruire la numerazione perduta, considerato che nel frattempo tali documenti possono essere stati archiviati in mezzo a centinaia di fascicoli e a migliaia di carte.
Da un altro punto di vista, la registrazione dell'avvenuto ingresso di un documento, con relativo numero attribuito, data e oggetto, costituisce sicuramente il dato personale che più frequentemente un Interessato potrebbe chiedere se esiste e di conoscerlo. Ciò perché in molti casi può essere per lui di vitale importanza provare di aver consegnato un certo documento o addirittura provare di averlo prodotto entro una certa scadenza temporale. In tali casi, però, è possibile trovare nel fascicolo personale o in un numero limitato di fascicoli il documento in oggetto, con relativo timbro datario e numero progressivo.
In tutti gli altri casi l'eventuale perdita di dati creerebbe un po' di lavoro in più per reinserirli copiandoli dai rispettivi originali cartacei, ma niente più..
La situazione cambierà quando eventualmente si passerà ad un protocollo esclusivamente elettronico, senza copia cartacea.

Altri dati la cui perdita creerebbe problemi

Il programma gestione finanziaria, che consente di emettere mandati e reversali è sicuramente quello che potrebbe soffrire non tanto della perdita dei dati quanto del breve blocco operativo conseguente alla necessità di reinserire i dati perduti, dei quali comunque esistono i documenti cartacei facilmente rintracciabili.
Anche il programma stipendi, il programma assenze e il programma alunni creerebbero notevoli perdite di tempo per reintegrare i dati, tuttavia la perdita non sarebbe irreversibile né di per sé grave.

Conseguenze di un blocco di computer di breve durata (1 giorno circa)

Nel caso di blocco :
- di un solo computer isolato (=non in rete) che fosse l'unico ad aver memorizzati certi dati e certi programmi,
- del server di rete in cui siano memorizzati tutti i dati e i programmi

si ritiene che il danno sarebbe minimo perché rarissimamente la scuola opera con scadenze in tempo reale, quindi l'attesa di un giorno non creerebbe problemi a meno che non si fosse atteso l'ultimissimo momento per un adempimento con scadenza tassativa.
Nel caso del protocollo, per un giorno si potrebbe procedere con annotazione manuale e successiva copiatura delle registrazioni quando il computer riprendesse a funzionare.
Nel caso che tale guasto riguardasse un terminale di rete (client), se i dati e i programmi di lavorazione dei dati sono memorizzati nel server, passando a un altro terminale si risolve il problema senza inconvenienti.

Conseguenze di un blocco di computer di media-lunga durata (oltre 1 giorno)

Nel caso di blocco prolungato :
a) di un solo computer isolato (=non in rete) che fosse l'unico ad aver memorizzati certi dati e certi programmi,
b) del server di rete in cui siano memorizzati tutti i dati e i programmi
c) dell'intero sistema

si ritiene che il danno diventerebbe serio, grave dopo circa 3-4 giorni, gravissimo dopo una settimana.
Invece, nel caso che tale guasto riguardasse un terminale di rete (client), se i dati e i programmi di lavorazione dei dati sono memorizzati nel server, passando a un altro terminale si risolve il problema senza inconvenienti.
Per intervenire nei casi a), b), c) è normalmente sufficiente una procedura di "Disaster Recovery" (= Recupero di un disastro, che ha provocato la messa fuori uso completa e prolungata, a volte irreversibile, del sistema informatico o di sue parti vitali a causa di un evento). Se essa si conclude in uno, massimo due giorni, è accettabile, mentre non sembra indispensabile un piano di continuità operativa che riduca necessariamente i tempi di sosta sotto uno-due giorni. I costi economici sarebbero infinitamente superiori ai costi dovuti al blocco temporaneo.

Procedure di Back-up. Analisi della situazione.

Attualmente il back-up viene eseguito con dischi rigidi, considerata la relativamente modesta quantità di dati da salvare. Nel tempo di vigenza del presente DPSS la scuola approfondirà il problema per pervenire ad eventuali soluzioni migliorative. E' stato nominato un incaricato responsabile delle operazioni di back-up

Procedure di Back-up.

1) In applicazione del principio che le copie di back-up non devono essere esposte al rischio di essere rovinate da un evento che contemporaneamente distrugga i computers, custodiamo le copie di back-up dei dati nonché i dischi originali dei programmi in un "armadio di sicurezza", resistente all'effrazione.
2) Contro il rischio di back-up malriuscito, abbiamo allo studio l'acquisto di un programma in grado di testare la qualità della copia di back-up eseguita e di gestirla in modo efficiente (compatibilmente con le disponibilità finanziarie..
Inoltre, come seconda misura, vengono effettuati due back-up dei dati:
- il primo direttamente sulle cartelle del server che viene poi replicato su una seconda macchina client in fase di back-up collocata in altra stanza;
- il secondo dell'intero contenuto del disco fisso viene effettuato su un HD rimovibile ogni qualvolta vengono installate patch di aggiornamento al sistema operativo o ai programmi installati.

Vengono create due immagini alternate, tramite questo è possibile ripristinare il server in breve tempo (tale "immagine" viene protetta con password per aumentarne la sicurezza).
Sullo stesso disco vengono nell'occasione salvati, inoltre tutti i dati aggiornati al momento disponibili.
3) Per evitare errori umani, procedurali, organizzativi o delle macchine, verranno periodicamente eseguiti test di ripristino (ovviamente dopo aver salvato i dati correnti oppure , preferibilmente, su un computer diverso da quello dove sono i dati correnti).
4) Periodicità: si ritiene che la periodicità di 7 giorni per il back-up sia al momento adeguata. Se e quando si arrivasse a veri e propri "documenti originali elettronici", andrebbe portata a frequenza di 2 giorni o 1 giorno per tali documenti.

5) Quali dati salvare? E' stato organizzato un censimento dei dati da salvare, che corrisponde alla specifica **tabella 5.1** inserita nel DPSS, Per quanto riguarda i files di testo o prodotti con altri programmi standard (esempio: excell, access, ecc.) non contenenti dati sensibili, ogni utilizzatore ha avuto l'istruzione di salvare tali elaborati personali in un'unica cartella (directory) in modo da poter salvare in blocco tutti i suoi files. Sono state anche individuate con chiarezza le directory di uso comune o riservate, in modo da avere una lista sempre aggiornata delle directory di cui fare il back-up.
6) Anche sulla base del predetto censimento, che corrisponde alla specifica **tabella 5.1** inserita nel DPSS, viene istituito un "registro dei back-up" in cui sono elencate le directory da salvare, le periodicità, il responsabile di ciascuna operazione. Ad ogni back-up il responsabile dovrà indicare la data e controfirmare.
Tutto il sistema di back-up viene gestito in maniera automatica tramite un programma su un client che gestisce la copia (con cadenza settimanale) di tutti i dati alternando due files. Il sistema, inoltre, una volta effettuato il back-up, replica lo stesso su una terza macchina. E' allo studio la possibilità di salvare i dati con un sistema ddi criptazione a 128 bit.
7) Sono state impartite precise disposizioni riguardo a tutte le procedure di back-up. Ogni mese il Titolare o suo delegato monitorerà le operazioni di back-up per verificare l'effettiva applicazione delle istruzioni date.

Procedure di "Disaster Recovery"

Nell'ipotesi che un evento distrugga o renda indisponibili tutti i computers, si possono utilizzare alcuni PC in uso agli alunni, per il tempo in cui ci si organizzerà per l'acquisizione di altri computers.
Tale computer sarà fornito con un sistema operativo compatibile con il software in uso alla scuola.
Nell'armadio di sicurezza sono conservati i dischi di back-up e di tutti i programmi necessari al funzionamento, in modo da poterli reinstallare. Un assistente amministrativo scriverà in un registro da custodire nell'armadio di sicurezza, l'elenco dei programmi da caricare, l'ordine di caricamento, i particolari settaggi necessari per implementare il software (parametri e altro da configurare, ecc.), l'elenco e l'ordine di caricamento dei files di back-up.

Piano di continuità

Esiste un computer in tutto compatibile con il software di elaborazione dei dati usato dalla segreteria collocato in altra area della scuola, tale che sia estremamente improbabile che il medesimo evento possa rendere indisponibili contemporaneamente sia i computers della presidenza e segreteria, sia questo computer di riserva. Nel frattempo sarebbe utilizzato per attività didattiche o personali dei docenti. In tale computer sarebbero già pre-caricati i programmi e le directory utilizzate in segreteria , ma naturalmente senza i dati. In tal caso, nel tempo tecnico del ripristino dati dai dischi di back-up il sistema informativo potrebbe riprendere a funzionare dopo una o due ore, il che sarebbe in pratica un piano di continuità operativa , data l'esiguità dell'interruzione.
E' altresì in uso sul server un sistema raid (= doppia registrazione contemporanea su due dischi fissi, in modo che alla rottura di uno resti disponibile l'altro) consentendo così l'erogazione dei servizi.
I programmi originali di tutto il software necessario saranno collocati nell'armadio di sicurezza di cui si è accennato, in modo che siano sempre disponibili e che l'evento disastroso abbia minime possibilità di distruggerli.

Prove di ripristino dei dati

Per evitare errori umani, procedurali, organizzativi o delle macchine, verranno periodicamente eseguiti test di ripristino (ovviamente dopo aver salvato i dati correnti oppure , preferibilmente, su un computer diverso da quello dove sono i dati correnti).
Per non avere problemi, anche in vista dell'implementazione di misure di disaster recovery e di un piano di continuità, il test verrà eseguito su un computer diverso da quelli dove risiedono gli archivi elettronici da ripristinare. Nell'occasione si farà quindi anche una prova di disaster recovery, caricando prima i programmi che servono per gestire i dati e successivamente facendo il test di ripristino.
Alla fine della prova i dati verranno cancellati, ma non i programmi (sempre che le licenze d'uso lo consentano) in modo che quel computer sia già predisposto per il disaster recovery.
Alle prove sarà presente un tecnico informatico per dare utili consigli e sovrintendere all'esecuzione. Saranno presenti tutti gli Incaricati che hanno avuto l'istruzione di realizzare il back-up periodico di un archivio elettronico, allo scopo anche che comprendano meglio a cosa serve e siano più motivati psicologicamente.

Allegato 9 - Misure per incrementare la sicurezza e misure di monitoraggio del livello di sicurezza

Premesso che le "misure minime" sono state implementate interamente fin dall'inizio, l'obiettivo è di inserire opportuni miglioramenti, tecnici e/o organizzativi per conseguire quel continuo miglioramento delle misure di sicurezza che è richiesto.

Misure già poste in essere

Negli ultimi 2 anni sono stati eseguiti i seguenti investimenti, finalizzati anche a migliorare la sicurezza dei dati personali:

Categorie:

- Acquisto di nuovi antivirus.
- Acquisto di nuovi computer

La scuola è già dotata di misure e sistemi antifurto nelle sedi n. 1 e n. 2 e antincendio nelle altre sedi. La scuola si è già dotata di computer tecnicamente sufficienti.

RESPONSABILI DELLE DECISIONI in merito all'implementazione delle misure di sicurezza

Va premesso che le decisioni in materia di acquisti di beni e servizi competono al Dirigente Scolastico e al Consiglio d'Istituto. Invece le decisioni in materia di lavori competono all'Ente Locale Comune di Ancona proprietario dell'immobile, benché piccoli interventi possano essere compiuti direttamente dalla Scuola.
Considerato che il nostro Istituto non dispone di significative risorse economiche, mentre abbiamo comunque cercato di investire le somme possibili per migliorare tutte le misure di sicurezza, in particolare abbiamo espresso il massimo impegno per migliorare le **misure organizzative, che hanno un costo estremamente basso ma hanno influenza decisiva sulla sicurezza dei dati. E' pertanto in tale categoria di misure che potranno essere apprezzati i più numerosi interventi.**

Miglioramento sicurezza anti-intrusione e antincendio

Descrizione dei rischi: furto, intrusione, incendio che comporterebbero perdita di dati
Trattamenti interessati: tutti, in particolare le operazioni informatizzate
*Struttura o persone addette all'adozione:*Dirigente, Consiglio d'istituto

L'Istituto dispone di un sistema di rilevamento automatico incendi

Installazione Impianto spegnimento automatico incendi
Non possedendo la scuola delle necessarie risorse finanziarie per l'acquisto dei suddetti sistemi, si può far riferimento al solo Comune di Ancona per l'eventuale installazione.

Analogo discorso può essere fatto per l'acquisto di estintori ad anidride carbonica per dotarne le stanze in cui c'è la massima concentrazione di computers , da utilizzare sui computers stessi e altri dispositivi elettrici in caso di incendio, in quanto non li rovinano, diversamente dagli estintori a polvere.

Miglioramento sicurezza fisica dei supporti magnetici (fisici, ecc.) e cartacei

Descrizione dei rischi: minacce all'integrità dei supporti magnetici e cartacei (incendio, ma anche furto)
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente, Consiglio d'istituto

a) CASSAFORTE IGNIFUGA per supporti magnetici e documenti
(può anche essere messa entro una cassaforte tradizionale o un armadio blindato per costituire una sezione di sicurezza antifuoco)
Cassetta ignifuga trasportabile per la protezione di supporti magnetici con guarnizione isolante da fumo gas e acqua. Costo presumibile € 540,00

Miglioramento hardware sistema informatico e sistemi di supporto e buona manutenzione nel tempo

Descrizione dei rischi: malfunzionamenti che potrebbero creare perdita di dati o blocco del sistema
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente, Consiglio d'istituto

a) Acquisto/sostituzione di gruppo di continuità con filtro antifulmine e antisbalzo di corrente , per impedire la perdita di dati conseguente a improvviso blackout o sbalzo di corrente e a fulmine . Spesa prevista, iva compresa: € 300,00. E' stato comunque sottoposto a manutenzione il gruppo continuità esistente.

b) stipula con un fornitore di un contratto per la manutenzione periodica dell'hardware,
E' noto che la polvere si deposita rapidamente sulle ventole e all'interno del case del computer, impedendo una dissipazione adeguata del calore prodotto dalla CPU e dai dischi di memorizzazione. I sistemi di dissipazione dell'elevato calore prodotto dalla CPU si basano spesso su particolari paste termiche e su una speciale ventola a contatto con la CPU stessa: una verifica se la pasta termica è ancora presente in modo compatto e sufficiente è importante.. Se la polvere non viene rimossa periodicamente e le ventole non vengono pulite e lubrificate, la dissipazione diventa inadeguata, il sistema rallenta le sue prestazioni per autoproteggersi e possono avvenire guasti.
Tutto ciò è particolarmente più significativo per i server di sistema, che sono sottoposti a un lavoro più continuo.
Per lo stesso motivo è necessario mantenere una buona circolazione dell'aria attorno al computer.
Anche le prese e le spine devono essere adeguate e sicure, disposte in modo ordinato e prive di polvere (quest'ultima è spesso la causa di surriscaldamento molto grave che può dare innesco a incendi). In generale un'inadeguata organizzazione del sistema di alimentazione e dei numerosi fili e prese può essere una probabile causa d'incendio.
Pertanto sarà instaurato un contratto di manutenzione periodica che tenga conto anche di questi obiettivi.

c)acquisto di un nuovo server
Si reputa necessario provvedere alla sostituzione di quello esistente. Spesa prevista € 1500,00

Miglioramento del software e della sicurezza dei dati gestiti con sistemi informatici

Descrizione dei rischi: maggiore vulnerabilità del sistema informatico, rischio di intrusioni o perdita di dati
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente, Consiglio d'istituto

a) Antivirus: rinnovo biennale dell'antivirus professionale esistente

b) Posta Elettronica Certificata rinnovo annuale dell'assistenza per la casella di posta elettronica certificata che la scuola possiede

c) Acquisto del programma con manuale per la gestione automatica del Backup generale e in particolare anche dell'archivio di Outlook Express (compresa una guida completa al backup, al ripristino e al Disaster recovery)

Spesa prevista, iva compresa, con i manuali d'uso: € 23,40

d) Applicazione del Provvedimento del Garante in materia di *amministratori di sistema o assimilati. Poiché entrerà in vigore al 1.07.2009, abbiamo già acquisito un manuale per applicarlo puntualmente per tale data. Poiché è possibile che fino a luglio il Garante emetta chiarimenti e indicazioni pratiche, riteniamo preferibile avvalerci della possibilità di non inserire le necessarie modifiche già nel DPS , 2009. A giugno sarà redatto l'elenco degli amministratori di sistema o assimilati e nel 2010 sarà allegato al DPS; nell'occasione sarà adattato a tale novità anche il "mansionario privacy" per ora lasciato con la precedente impostazione. E' prevista per luglio 2009 anche una formazione sull'argomento per i nostri amministratori di sistema o assimilati e per tutti gli Incaricati e Responsabili che utilizzano computers.*

e) **Applicazione del Provvedimento del Garante (dell'ottobre 2008, già in vigore) in materia di gestione di supporti informatici o computers rottamati o ceduti ad altri. Trattasi del Provvedimento a carattere generale [integrazione delle misure minime di sicurezza obbligatorie] "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali " del 13 ottobre 2008 in G.U. n. 287 del 9 dicembre 2008. LE INTEGRAZIONI ALLE MISURE DI SICUREZZA OBBLIGATORIE SONO GIA' APPLICATE. A*bbiamo già acquisito un manuale per applicarlo operativamente. L'argomento sarà anche oggetto di formazione per Incaricati e Responsabili che utilizzano computers.***

Miglioramento della protezione dei dati sensibili e giudiziari, affinché non siano visti quando non è necessario o da chi non ne ha diritto

Descrizione dei rischi: i dati sensibili o giudiziari possono essere visti inutilmente o da chi non ne ha diritto
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente, Consiglio d'istituto

Le regole del Codice Privacy prescrivono, in sostanza, che , **anche chi è autorizzato** a trattare dati sensibili o giudiziari:

a) non li veda associati a uno specifico interessato in quelle operazioni in cui non è necessario e che, pertanto, possono essere eseguite in forma anonima (esempio: analisi statistiche, raffronti, ecc.)

b) nelle operazioni svolgibili con soli dati comuni, in cui non serve visualizzare i dati sensibili o giudiziari, non li veda inutilmente ma siano oscurati temporaneamente.

Queste situazioni si realizzano, per esempio, quando si svolgono analisi statistiche su un data-base oppure quando si lavora soltanto su certi dati e non su tutti (questo avviene quasi sempre in fase di consultazione).

Possono sembrare misure eccessive, però - come abbiamo premesso - è obbligatorio possedere un programma di questo tipo PRIMA di detenere dati sensibili come condizione per essere autorizzati a ciò. Inoltre è obbligatorio utilizzare un programma informatico che abbia questo tipo di funzioni in tutti i casi in cui si trattino dati personali.

a) E' già stato acquisito di un software per la cifratura obbligatoria dei dati sensibili o giudiziari
Questo programma consente di lavorare a 3 livelli :

1) c**on la funzione <FiltroZero>** (cioè con nessun filtro) lavora **come in un normale foglio Excel**: si usa per il caricamento dei dati e per le operazioni in cui sia indispensabile vedere contestualmente sia tutti i dati sensibili/giudiziari sia l'identità dell'Interessato. Con <FiltriPrivacy> si lavora normalmente come in un qualsiasi foglio di Excel (comprese operazioni matematiche, ecc.), però il programma è in grado di presentare lo stesso foglio con mascherati tutti gli elementi non necessari (ed eventualmente sostituendoli con un codice identificativo segreto ma verificabile in caso di bisogno) proprio come è prescritto.

2) quando l'operazione da eseguire può essere svolta senza visualizzare certi dati, in particolare sensibili o giudiziari, **con la funzione <FiltroDati>** oscura i dati collocati nelle colonne che scegli di oscurare.

3) quando l'operazione da eseguire può essere svolta utilizzando dati anonimi, **con la funzione <FiltroIdentità>** sostituisce il nome delle persone con un codice, oscura gli altri dati identificativi, nonché cambia l'ordine di successione delle registrazioni in modo da rendere provvisoriamente impossibile identificare l'Interessato cui si riferiscono i dati. Possono essere contemporaneamente oscurati anche dati sensibili o giudiziari non necessari all'operazione da svolgere. In caso di bisogno, **una tabella a parte consente, di risalire all'identità dell'interessato** cui si riferisce una certa registrazione.

Miglioramenti organizzativi

a) Istituzione di un "REGISTRO DEI CONTROLLI PERIODICI" ,

che mediante delle liste di controllo semestrali o mensili, consente di monitorare l'applicazione della normativa privacy e delle misure di sicurezza, ottenendo nel contempo di far sì che il personale mantenga elevato il livello di attenzione e di diligenza. Il facsimile con le relative istruzioni operative è già stato acquisito insieme al "Manuale per il DPS 2009"

.

b) revisione della gestione dei dipendenti con verifica della piena applicazione delle Linee Guida sulla gestione dei dipendenti in ambito pubblico emesse dal Garante Privacy

Descrizione dei rischi: la gestione dei dipendenti potrebbe avere dei difetti
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente

La Dirigenza e la Segreteria studieranno le predette Linee Guida, mediante un manuale ad hoc già acquisito.
Le procedure in essere utilizzate per la gestione dei dipendenti verranno passate al vaglio in ogni fase del ciclo e sarà verificata la piena corrispondenza alle prescrizioni contenute nelle Linee Guida.
Questa azione sarà sinergica con le altre di seguito illustrate e pertinenti in particolare o anche alla gestione dei dipendenti.

c) miglior pubblicizzazione dell'informativa e del <Regolamento Dati Sensibili …>

Descrizione dei rischi: la comunicazione dell'informativa alle varie categorie di Interessati potrebbe essere dimenticata o saltata per fretta, potrebbe essere insufficientemente conosciuto dagli Interessati il <Regolamento dati sensibili>, se un Interessato che ha un rapporto diretto con l'Istituto deve utilizzare dati di tersi (familiari), costoro potrebbero non ricevere l'informativa.
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente

Si è provveduto già a:

1) Inserire nella bacheca vicino all'ufficio di segreteria o all'interno dello stesso , un volume in cui inserire tutte le diverse informative, il "Regolamento Dati sensibili", tutte le diverse designazioni degli incaricati, ed il DPS
2) Identica pubblicazione anche nel sito web dell'Istituto.
3) L'informativa a terzi con i quali non esiste un rapporto diretto:

Ci sono istanze, di solito per richiedere benefici (dagli assegni familiari ai permessi Legge 104), nelle quali è indispensabile chiedere dati personali di un altro familiare adulto, per il quale il dipendente non può firmare in qualità di genitore o tutore. Solitamente si tratta del coniuge.
La normativa è chiarissima: anche a questo terzo Interessato va data informativa al più presto e comunque prima di iniziare il trattamento conseguente all'istanza.
Considerato che è poco probabile che questo Interessato, estraneo all'istituto scolastico, venga allo sportello di persona e possa così ricevere l'informativa o possa vederla pubblicata nell'apposita bacheca, si pone il problema di implementare una procedura "a prova di dimenticanza dell'Incaricato".
Pertanto, si ritiene che le soluzioni possano essere diverse e saranno valutate per la scelta. Intanto le elenchiamo:
a) in ogni modulo che deve essere firmato anche dal coniuge o altro familiare del dipendente, inserire l'intera informativa chiedendo che la firma attesti anche l'avvenuta presa visione di essa.

b) se la precedente soluzione appare troppo dispendiosa come volume di carta, se il modulo che deve essere firmato anche dal coniuge o altro familiare del dipendente, inserire un'ampia postilla in cui si comunica a tale persona che nel sito web dell'Istituto sono pubblicati l'informatica e il Regolamento Dati sensibili, chiedendo che la firma attesti l'avvenuta presa visione.

c) se il modulo fa riferimento a dati personali del coniuge o di altro familiare del dipendente, **ma non è richiesta la sua firma** (ad esempio, nelle richieste di permesso per handicap di un familiare), il caso è particolarmente complesso da gestire. D'altra parte è il tipico caso in cui è strutturalmente più probabile che sia dimenticata l'informativa a questo terzo Interessato.

Sicuramente la pubblicazione nel sito web dell'informativa , che per i dati sensibili rinvia al Regolamento, anch'esso pubblicato, è una prima soluzione.

La seconda soluzione è inserire in tutta la modulistica che può avere quest'uso una formula del tipo: "Se per questa pratica vengono conferiti dati personali di familiari o di terzi, far apporre la loro firma in calce a queste righe, come attestazione che hanno preso visione dell'informativa privacy consultandola nel sito web o ricevendone una copia cartacea tramite la persona che ha attivato la presente pratica." .

La terza soluzione è , ovviamente, che la segreteria si ricordi di consegnare un'informativa completa, verificando che ritorni firmata per attestazione di presa visone del terzo Interessato; nelle pratiche ricorrenti (come nel caso dei permessi per legge 104 o per congedi parentali) sarà sufficiente che l'operazione sia svolta solo per la prima volta che viene presentata un'istanza di questo tipo.

d) revisione modulistica per le istanze, per verificare che siano pienamente corrispondenti alle regole Privacy e implementando anche un'attestazione di presa visione dell'informativa in base all'art. 13 e del <Regolamento Dati Sensibili …>

Descrizione dei rischi: la comunicazione dell'informativa alle varie categorie di Interessati potrebbe essere inadeguata, potrebbero essere involontariamente chiesti dati eccedenti o privi dei presupposti di legittimità
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente

Si tratta sia della modulistica per i dipendenti (che è al più numerosa), ma anche di quella utilizzata da Alunni e Famiglie e da fornitori e Collaboratori dell'Istituto

L'obiettivo è di verificare che non siano richiesti dati personali eccedenti o che non sia legittimo trattare.

Questa complessa e impegnativa attività viene svolta cogliendo l'occasione di dare concreta attuazione all'obbligo imposto dal Dlgs 82/2005 <Codice dell'Amministrazione Digitale> che all'Art. 57 - Moduli e formulari impone dal 1.1.2008 la pubblicazione nel sito web della scuola di TUTTI i moduli utilizzati.

Per quanto riguarda i dati comuni la verifica sarà eseguita in modo che non siano richiesti dati non necessari o estranei alle finalità istituzionali proprie della scuola pubblica.

Per quanto riguarda i dati sensibili o giudiziari la verifica sarà mirata a controllare per ogni modulo o pratica o istanza**:**

1) **che siano richiesti esclusivamente dati strettamente indispensabili** a raggiungere la finalità prevista dall'istanza o dalla pratica in questione e che essa non sia estranea alle finalità istituzionali proprie della scuola pubblica.
2) **che esista piena corrispondenza ai presupposti di legittimità stabiliti dal Regolamento** adottato con Decreto del Ministero dell'Istruzione n. 305 del 7 dicembre 2006, entrato in vigore il 30 gennaio 2007. Tale regolamento si intitola esattamente: <<Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazione effettuate dal Ministero della Pubblica Istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003 n. 196, recante "Codice in materia di protezione dei dati personali">>. Per brevità lo chiameremo <<Regolamento dati sensibili>>. Pertanto per ciascun modulo o pratica che utilizzi dati sensibili o giudiziari si individuerà quale sia la scheda pertinente del Regolamento. Tramite essa si verificherà che **i tipi di dati** siano tra quelli autorizzati, che le **operazioni che s'intende eseguire** (in particolare se prevista la COMUNICAZIONE o DIFFUSIONE) siano tra quelli autorizzate e che la **finalità del trattamento** sia tra quelle dichiarate nella scheda come "di rilevante interesse pubblico".
3) Che **l'informativa generale** data all'Interessato sia adeguata a ricomprendere le finalità, i tipi di dati e di operazioni da eseguire , oppure se talune istanze o pratiche **richiedano un'ulteriore specifica informativa.**

Sia per i dati comuni che in particolare per quelli sensibili:

creare presupposti organizzativi tali da prevenire qualsiasi dimenticanza nel fornire completa informativa di cui all'art. 13 o la possibilità che qualunque Interessato possa per qualche ragione non aver contezza dell'informativa stessa.
Va premesso che non è materialmente possibile inserire in ciascun modulo l'intera informativa che lo riguarda, perché ciò appesantirebbe troppo la gestione della modulistica stessa.
Tuttavia le pratiche più delicate dal punto di vista dei dati sensibili o giudiziari o che prevedano la diffusione degli stessi, saranno comunque dotate in calce di adeguata informativa.

La restante modulistica, cioè la quasi totalità, sarà dotata di un breve richiamo all'informativa già comunicata oppure disponibile nel sito web dell'Istituto e pubblicata permanentemente all'Albo della scuola su apposita bacheca, nonché - di un breve richiamo del al <Regolamento dati sensibili ecc.> anch'esso pubblicato permanentemente all'Albo e nel sito web dell'Istituto.

_e)_ revisione gestione dei Internet e Posta Elettronica alla luce delle prescrizioni contenute nelle relative Linee Guida emanate dal Garante Privacy

Descrizione dei rischi: a causa di cattiva organizzazione la gestione di Internet e della Posta elettronica potrebbe non essere conforme alle prescrizioni del Garante
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
_Struttura o persone addette all'adozione:_Dirigente, Consiglio d'istituto

Verrà utilizzata come base di lavoro l'Illustrazione delle Linee Guida. Verranno eseguite in particolari queste verifiche:

1) che non sia effettuata alcuna forma di controllo indiretto o disegno del profilo del dipendente, così come prescritto dal Garante, e che non sia possibile che ciò avvenga in futuro. Dopo la verifica della situazione attuale, sarà emanata una circolare che confermi i diritti dei dipendenti.

2) che sia garantita la riservatezza e la sicurezza delle comunicazioni ricevute tramite internet
che nessun dato personale relativo ai dipendenti o terzi sia mantenuto in memoria oltre il tempo strettamente necessario (regole sulla conservazione dei dati). Verrà messa a punto una procedura per cui in tutti i casi in cui sia possibile il messaggi e il file contenete dati personali (in particolare del dipendente, ma non solo) , sia cancellato definitivamente (anche dal backup !). In molti acsi converrà stampare il messaggio e subito cancellarlo. Il documento stampato seguirà il suo iter e poi dovrà essere distrutto o trasferito in uno speciale archivio di documenti in stato di "blocco", in attesa di distruzione.

3) che sia data specifica informativa ai dipendenti, come espressamente previsto dal D.Lgs 82 "Codice dell'Amministrazione Digitale" all'art. 47, nel rispetto del comma 3, punto b, di cui si parla nel prossimo punto.

f) Dare applicazione al D.Lgs 82 "Codice dell'Amministrazione Digitale" all'art. 47, nel rispetto del comma 3, punto b,

Descrizione dei rischi: l'informativa ai dipendenti potrebbe essere incompleta
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
_Struttura o persone addette all'adozione:_Dirigente, Consiglio d'istituto

Il predetto Art. 47. Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni, recita:

<<3. Entro il 31.12.2007 le pubbliche amministrazioni centrali [compresa ogni scuola statale] provvedono a: a) istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ciascun registro di protocollo; **b) utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati. >>**

In applicazione di quanto sopra, verranno compiute le seguenti operazioni:

1) Verrà inserita nel modulo <Assunzione di servizio> la richiesta dell'email del dipendente, con l'avvertenza di comunicarne eventuali variazioni.

2) Per i dipendenti già in servizio verrà emanata una circolare in cui verrà richiesto a ciascuno il suo indirizzo email. Inoltre i dipendenti saranno avvertiti che in ossequio alla legge:

- 2.1) dovranno preferibilmente e progressivamente utilizzare la modulistica pubblicata sul sito web e spedirla alla scuola tramite email.

- 2.2) Riceveranno eventuali comunicazioni personali dall'Istituto **TRAMITE EMAIL**.

- 2.3) Progressivamente **tutte le circolari destinate ai dipendenti saranno a loro trasmesse prevalentemente tramite email, riducendo al minimo la circolazione residuale di copie cartacee.**

La circolare che darà queste istruzioni iniziali dovrà contenere anche una specifica informativa sui trattamenti conseguenti, come esplicitamente impone il citato art. 47. Così come tale elemento dovrà essere aggiunto all'informativa già utilizzata per i dipendenti.

Va premesso che lo spirito della norma è anche di risparmiare denaro in spese di francobolli e di riproduzione su carta. Il Ministro della Funzione Pubblica al momento dell'uscita della norma sottolineò che ogni comunicazione cartacea ha un costo medio, comprensivo dei costi di spedizione e del costo del lavoro necessario per la spedizione o la consegna e per al riproduzione, per cui la Corte dei Conti un giorno dovrà chiedere ai dirigenti le maggiori spese sopportate per non aver attuato norme di questo tipo.

Dal punto vista organizzativo, per l'applicazione del punto 2.3 potranno essere seguiti questi accorgimenti:

1) istituite anche caselle di posta elettronica collegate al sito della scuola per i dipendenti che ne siano privi
2) per i dipendenti (come alcuni operatori scolastici) che non siano familiarizzati con l'uso del computer, indicare un tutor che li aiuti per una prima fase (preferibilmente un loro collega, altrimenti qualcuno della segreteria)
3) Predisporre in Outlook Express (o software simile) simile i cosiddetti <Gruppi di destinatari>: per esempio il gruppo <Personale ATA>, il Gruppo <Docenti> , il Gruppo <Coordinatori di classe> e così via, in modo che sia automatico spedire la circolare esclusivamente alle categorie di destinatari che interessano.
4) Nei casi in cui sia possibile, non distribuire la circolare cartacea (che resterà solo agli atti), ma limitarsi a mettere un cartello che informi che sono state spedite nuove circolari, invitando ciascuno a controllare nella sua casella di posta elettronica.

Poiché il progetto è ambizioso e molto complesso, ne verrà comunque almeno avviato lo studio preliminare, tenendo ben presenti tutte le implicazioni per la Privacy dei dipendenti e per la sicurezza dei computers.

g) Implementazione di procedure per il controllo dell'osservanza delle regole nella gestione delle password

Descrizione dei rischi: le password potrebbero non essere gestite correttamente
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente, Consiglio d'istituto

a) E' stato acquisito un software che organizza meglio il lavoro del <Custode delle passwords>

Pertanto il <Custode delle password> potrà registrare ogni volta che riceve da un Incaricato la busta con la password segreta modificata trimestralmente o semestralmente a seconda dei casi. Tale software evidenzia immediatamente se qualcuno è in ritardo nella consegna della busta e stampa una lettera per invitarlo a provvedere. Inoltre, stampa dei report per il Titolare, affinché sia informato dell'attività svolta dal <Custode delle Password>. Infatti il Dirigente ha l'obbligo di verificare in modo adeguato e ripetuto nel tempo che le misure di sicurezza siano regolarmente applicate.

Sicurezza dei documenti cartacei contenenti dati sensibili

L'obiettivo è di dare piena attuazione all'art. 35 del Dlgs 196/2003, che recita:
<<Art. 35. Trattamenti senza l'ausilio di strumenti elettronici
1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

a**) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati**.>>

Descrizione dei rischi: l'organizzazione degli archivi ad accesso controllato o selezionato potrebbe non essere adeguata
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente, Consiglio d'istituto

a) Acquisto di una guida per una miglior gestione degli archivi
Spesa prevista, iva compresa, con i manuali d'uso: € 9,00

b) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.>>

Descrizione dei rischi: l'organizzazione degli archivi ad accesso controllato o selezionato potrebbe non essere adeguata
Trattamenti interessati: tutti quelli svolti in particolare nella Segreteria e Dirigenza
*Struttura o persone addette all'adozione:*Dirigente, Consiglio d'istituto

A seguito dello studio del manuale di cui al precedente punto a) , verranno applicati ad ogni armadio o schedario o stanza o archivio dei cartelli che indicano:

1) tipo di dati contenuti
2) natura dell'archivio: ad accesso selezionato o ad accesso controllato (in quest'ultimo caso indicare il nome del custode delle chiavi)

I facsimili dei cartelli sono contenuti nel predetto manuale.

Conclusione:

In base alle soluzioni scelte, va compilata la colonna n. 7 della tabella che segue, indicando anche in linea di massima il periodo in cui si presume che le misure siano effettivamente adottate.
Si noti che anche le date della colonna 6 vanno verificate e riportate all'effettiva situazione (noi abbiamo messo la data in cui erano diventate sostanzialmente obbligatorie).

19.4 Misure in essere e da adottare (regola 19.4).

Tab. 4.1. Le misure di sicurezza adottate o da adottare

1	2	3	4	5	6	7	8
Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Rif. scheda analitica	Misura già in essere (con data di effettività)	Misura da adottare (con data di effettività prevista)	Periodicità e responsabilità dei controlli
Istruzioni agli Incaricati (all.5)	Comportamenti inadeguati o errati degli operatori, incuria, ecc. : Furto delle credenziali di autenticazione ; carenza di consapevolezza, disattenzione o incuria; comportamenti sleali o fraudolenti; azione di *virus* informatico o di codici malefici *spamming (posta indesiderata e disturbante)* o altre tecniche di sabotaggio malfunzionamento, indisponibilità o degrado degli strumenti accessi esterni telematici non autorizzati intercettazione di informazioni in rete errore materiale	Tutti	Tutte	Allegato 5	Ottobre-Nov2004 Marzo 2008 Gennaio 2010		mensile Titolare/ Responsabile,
formazione		idem	idem	All. 6	Nov-Dic 2004 marzo 2008 giugno 2010 settembre 2010	Maggio 2011	annuale Titolare/ Responsabile,
azione del “Custode delle Parole-chiave”,		Trattamenti con dati sensibili o giudiziari (da Tr1 a Tr6).	idem				mensile Titolare/ Responsabile,
controllo dell’accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate		Idem	idem	All.2	Ottobre 2004 marzo 2008 gennaio 2010		mensile Titolare/ Responsabile,
eventuale creazione di profili di autorizzazione diversificati		Non adottato	idem				
Utilizzo di files cifrati per i rari files contenenti dati sensibili, giudiziari o particolari importanti.		Non adottato					
profilo di autorizzazione che non consenta la formattazione dei dischi fissi o la cancellazione di files importanti.		Non adottato	Idem				
Regolare aggiornamento dell’antivirus e del software (patches) : istruzioni agli incaricati	Eventi relativi agli strumenti: azione di *virus* informatici o di codici malefici; *spamming (posta indesiderata e*	Tutti	tutte	All. 5	Ottobre 2004	Aprile 2011	mensile Titolare/ Responsabile,
istruzioni a individuare e prevenire le situazioni a rischio (vedi allegato 5)		Idem	idem	All. 5	Dic 2004 Gennaio 2010		semestrale Titolare/Responsabile,
Eventuale implementazione di un filtro antispamming		idem	idem				semestrale Titolare/Respon

	disturbante) o						sabile,
formazione degli Incaricati a riconoscere i messaggi di disturbo e a gestire le regole di assegnazione dei messaggi di posta elettronica alle varie cartelle	altre tecniche di sabotaggio; malfunzionamento, indisponibilità o degrado degli strumenti; accessi esterni telematici non autorizzati; intercettazione di informazioni in rete	idem	idem	All. 5	Gennaio 2005 Gennaio 2010		semestrale Titolare/Responsabile,
Manutenzione programmata		idem	idem				semestrale Titolare/Responsabile,
Formazione ad individuare i sintomi di malfunzionamento per un rapido intervento		idem	idem		Gennaio 2005 Gennaio 2010		annuale Titolare/Responsabile,
piano di backup - Distaster Recovery e di continuità operativa		idem	idem	All. 8	Maggio 2005 Gennaio 2010	Maggio 2011	semestrale Titolare/Responsabile,
Installazione di Firewall, con regolare aggiornamento		idem	idem		Settembre 2004		semestrale Titolare/ Responsabile,
Eventuale adozione di cifratura o firma elettronica per proteggere i dati più gravi (allo studio)		Non adottato	Non adottato		Non dovuto	Non dovuto	
Verifica ed eventuale miglioramento della solidità degli infissi dei locali	Eventi relativi al contesto: accessi non autorizzati a locali/reparti ad accesso ristretto; asportazione e furto di strumenti contenenti dati; eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria; guasto ai sistemi complementari (impianto elettrico); guasto ai sistemi complementari (climatizzazione); errori umani nella gestione della sicurezza fisica	Tutti	Tutti	All. 1	Settembre 2004		semestrale Titolare/ Responsabile
Chiusura a chiave dei locali quando non presidiati : istruzioni a tutti gli operatori		idem	idem	All. 5	Gennaio 2004 Gennaio 2010		mensile Titolare/ Responsabile,
installazione di allarme antifurto		idem	idem		2000		annuale Titolare /Responsabile,
disponibilità di estintori ad anidride carbonica per non danneggiare i computers		idem	idem			Secondo disponibilità del Comune	annuale Titolare/ Responsabile,
Regolare back-up dei dati, piano di back-up - Distaster Recovery e di continuità operativa		idem	idem		Luglio 2007		mensile Titolare/ Responsabile,
Custodia dei dischi di back-up in armadio chiuso.		idem	idem		Gennaio 2004		semestrale Titolare/ Responsabile,
Sensibilizzazione e formazione degli Assistenti Amministrativi e dei Collaboratori Scolastici		idem	idem	All. 5	Nov-dic 2005 Marzo 2008 Settembre 2009		mensile Titolare/ Responsabile,
Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti		idem	idem		Settembre 2004		annuale Titolare/ Responsabile,
Uso di protezioni antifulmine e contro sovratensioni elettriche		idem	idem			Secondo disponibilità del Comune	annuale Titolare,/ responsabile,
Verifica della logistica degli apparecchi e del loro corretto posizionamento.		idem	idem		Gennaio 2005 Gennaio 2010		semestrale Titolare/ Responsabile,
Gruppo di continuità		idem	idem		2000		annuale Titolare/ responsabile,
Studio una miglior ventilazione dei computers (revisione regolare delle ventole interne e loro potenziamento).		idem	idem				annuale Titolare/ Responsabile,
Formazione e sensibilizzazione di tutti gli Incaricati, compresi Operatori delle pulizie e Collaboratori .Scolastici per il controllo.		idem	idem		Dicembre 2005 Marzo2008 Settembre 2009		mensile Titolare/ Responsabile,

Nuove misure incrementative della sicurezza:							
Soluzioni incrementative della sicurezza (vedi allegato 9)	Rischi fisici	idem	idem			Secondo disponibilità finanziaria	Mensile Titolare Responsabile
Soluzioni incrementative della sicurezza (vedi allegato 9)	Rischi sicurezza dati	idem	idem			Idem	mensile Titolare Responsabile,
Soluzioni incrementative della sicurezza (vedi allegato 9)	Rischi sistemi di supporto.	idem	idem			idem	mensile Titolare/ Responsabile,

Commento finale

Con il presente allegato si è ritenuto di approfondire il problema della sicurezza dal punto di vista organizzativo. La ragione dipende dal fatto che in generale nella scuola il rischio maggiore per i dati personali è legato principalmente a carenze organizzative, incuria di addetti, ecc.
Per ovviare a questi rischi, sono previsti questi rimedi:

1) monitoraggi periodici da parte del Dirigente Scolastico [e del Responsabile] con eventuale verifica a campione di fascicoli e di archivi, della realizzazione regolare degli aggiornamenti dei programmi e del back-up, ecc.

2) Riunioni con gli addetti per verificare collegialmente in modo costruttivo il progressivo affinamento nell'applicazione delle procedure previste e del D.Lgs 196/2003 in generale.

3) messa a disposizione degli Incaricati in un certo numero di copie (con disposizione che ne prendano visione e lo applichino) di un manuale di procedure da seguire per la sicurezza, che corrisponde all'allegato 5 del DPSS, in modo che tutti gli Incaricati conoscano le regole proprie e delle altre categorie di Incaricati con cui collaborano. E' prevista la manutenzione di questo manuale, aggiornando le misure in base all'esperienza e alle modifiche della situazione.

4) Istituzione delle seguenti figure, eseguita allo scopo di responsabilizzare altri soggetti e creare un monitoraggio amichevole ma continuo:

"Custode delle parole chiave"

La nomina del "Custode delle parole chiave" è sostanzialmente obbligatoria (sia pure non necessariamente in questa forma) perché prevista una forma di nomina scritta di un incaricato che svolga funzioni di tal genere (vedi la norma citata nel facsimile di nomina). Dev'essere qualcuno già incaricato dei trattamenti dei dati cui le parole chiave si riferiscono. Se fosse una figura diversa dal DGSA o dagli assistenti amministrativi, bisognerebbe designarlo Incaricato per i loro trattamenti.

Ha i seguenti compiti :

La funzione di "Custode delle parole-chiave" prevede i seguenti compiti:
1) Ricevere da ciascun Incaricato utilizzatore di computer una busta già chiusa e controfirmata, contenente una sola credenziale (= coppia di parola-chiave e username o nomeutente o user-id). Dall'utente che disponga di più credenziali, dovrà ricevere altrettante buste chiuse.
Ogni busta, naturalmente, dovrà riportare gli estremi identificativi dell'utente della credenziale e il riferimento alla funzione che essa svolge.
La busta chiusa sarà controfirmata anche dal Custode e quindi custodita in luogo sicuro di cui il Custode sia l'unico detentore della chiave.
2) Come previsto dal punto 10 dell'Allegato B, in caso di assenza prolungata dell'Incaricato (o suo impedimento) che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Custode aprirà la busta e ne consegnerà il contenuto al Titolare o al Responsabile o all'Incaricato da loro delegato, facendosi rilasciare ricevuta. Avvertirà tempestivamente dell'intervento il detentore originario della parole-chiave, invitandolo anche a sostituirla immediatamente.
3) In caso di smarrimento della parola-chiave da parte del legittimo detentore della stessa, provvederà a restituirgli la sua busta e a ricevere subito dopo copia della nuova parola chiave in busta chiusa controfirmata.

4) Registrare in un quaderno la data in cui ogni utente cambia la parole-chiave e verificare se ha provveduto alla modifica dopo 6 mesi (3 nel caso che i computer o gli archivi elettronici a cui la parole-chiave dà accesso contengano anche dati sensibili o giudiziari). Eventualmente sollecitarlo al rinnovo. In caso di assegnazione di nuova parole-chiave dal tecnico informatico, verificare che l'Incaricato abbia immediatamente provveduto a inserirne una nuova.
5) Ricordare a ogni utente che le parole-chiave devono avere le caratteristiche di cui al punto 5 dell'Allegato B (minimo 8 caratteri, evitare nomi, date o altri elementi riferibili all'Incaricato, ecc.)
6) Intervenire nel caso che riscontri anomalie o negligenze nella riservatezza della gestione chiavi da parte dei colleghi, richiamandoli cortesemente al corretto comportamento e invitandoli a sostituire immediatamente la parole-chiave che abbia perduto, anche solo potenzialmente, i requisiti di sicurezza.
7) Segnalare al Titolare [o al Responsabile, se esiste]eventuali problematiche riferibili alla gestione delle parole-chiave.
8) Gestire gli eventuali codici di cifratura (se e quando utilizzati) in modo identico a quello descritto per le parole chiave, in modo da assicurarne la disponibilità come previsto nei casi 2) e 3).

Al "Custode delle parole-chiave" la scuola metterà a disposizione un cassetta chiudibile a chiave da conservare o in cassaforte o in armadio a sicura chiusura, o altra soluzione equivalente che garantisca un'adeguata condizione di sicurezza. Del contenitore esisteranno soltanto 2 chiavi, date rispettivamente al "Custode" e al suo sostituto.

"Custode delle chiavi" degli archivi ad accesso controllato

E' facoltativa la nomina del "Custode delle chiavi" degli archivi ad accesso controllato perché contenenti dati sensibili/giudiziari (punto 29 dell'allegato B), però la consigliamo vivamente, perché altrimenti ricade tutto sulle spalle del DGSA. Inoltre è molto utile responsabilizzare le persone.

Ha i seguenti compiti :

Gestione degli archivi ad Accesso controllato. Si precisa che viene definito archivio ad accesso controllato quell'archivio al quale possono accedere solamente le persone previamente incaricate per iscritto dei trattamenti di dati personali conservati in tale archivio, le quali – inoltre – devono ciascuna volta chiedere la chiave per accedervi e restituirla im mediatamente dopo l'uso consegnandola direttamente nelle sue mani del Custode (è vietato appoggiarla o lasciarla in giro).
Pertanto l'Incaricato dovrà rivolgersi di norma al "Custode delle chiavi" per ricevere la chiave dell'archivio ad accesso controllato. In caso di sua assenza potrà rivolgersi al suo sostituto.
Per le emergenze, copia delle chiavi saranno a disposizione anche del Titolare o di altri da lui delegati, però con le seguenti modalità che assicurino dell'uso esclusivamente per situazioni d'emergenza e della custodia con modalità di elevata sicurezza: le chiavi saranno collocate in busta chiusa controfirmata dal Custode, munita di opportuna dicitura esterna, e consegnate al DGSA, al Titolare, al sostituto, i quali avranno cura di conservarle in luogo sicuro e le utilizzeranno esclusivamente in caso di assenza del Custode. Nel caso una busta sia aperta, dovrà essere stilato in un apposito quaderno-registro un breve verbale indicante ora, motivo e autore dell'accesso all'archivio controllato. Il Custode provvederà a rimettere la chiave in busta chiusa, mentre il verbale sarà da lui conservato per almeno un anno.

Il Custode terrà la chiave con sé o in luogo sicuro e la consegnerà temporaneamente solamente quando la scuola è aperta ed esclusivamente alle persone autorizzate secondo le indicazioni ricevute dal Titotare/Responsabile del trattamento e le regole descritte nell'allegato 5 del DPSS.
Dovrà altresì verificare che le chiavi siano a lui restituite dopo il tempo tecnico strettamente necessario all'accesso all'archivio.

"Coordinatore / Supervisore del Back-up, del ripristino e dell'aggiornamento del software"

Stesse considerazioni per il "Coordinatore / Supervisore del Back-up, del ripristino e dell'aggiornamento del software". Qui va anche tenuto conto del fatto che il Titolare e il responsabile hanno l'obbligo del monitoraggio periodico delle misure di sicurezza, anche organizzative, quindi introdurre queste figure significa dare prova di aver attuato la norma.

Ha i seguenti compiti :

1) Verificare che siano fedelmente applicati i punti dell'Allegato B sopra citati

2) Verificare che siano fedelmente eseguite alle scadenze previste **Custode delle parole-chiave** le copie di salvataggio e le altre attività descritte nel DPSS e nell'allegato 9, comprese le istruzioni relative al piano di Disaster Recovery e di continuità operativa.
3) Verificare che siano eseguiti alla giusta cadenza gli aggiornamenti del sistema operativo, dell'antivirus, del firewall, del software in generale.
4) Gestire l'armadio di sicurezza descritto nell'allegato 9, monitorandone la buona tenuta secondo le regole descritte
5) Verificare che i dischi originali del sistema operativo e di tutti i programmi utilizzati siano presenti e mantenuti nel predetto armadio, in vista delle procedure di Disaster Recovery e di continuità operativa
6) Ricevere per la distruzione o formattazione i floppy disk utilizzati, in particolare se contenenti dati sensibili
7) In generale monitorare l'evoluzione della situazione e mensilmente riferirne al Titolare al Responsabile].

ALLEGATO 9 Parte 2^ - Ulteriori misure per migliorare la sicurezza Verifica applicazione degli ultimi provvedimenti a carattere generale emessi dal Garante Privacy

Il Garante ha emesso negli ultimi anni vari Provvedimenti a carattere generale, cioè valevoli per tutti i Titolari, che hanno effetti simili alla normativa di legge.

Questa parte dell'allegato viene dedicata all'applicazione dei due principali Provvedimenti che sono all'ordine del giorno.

1) GARANTE PRIVACY: PROVVEDIMENTO A CARATTERE GENERALE in materia di *Amministratori di sistema e assimilati.*

E' entrato in vigore il 1.07.2009 per la parte documentale, il 16 dicembre 2009 per la parte che concerne la registrazione degli accessi logici degli AdS e Assimilati.

Lo scrivente istituto ha dato piena applicazione e quanto segue costituisce dimostrazione di ciò.

E' stato già acquisito un manuale per conoscerlo a fondo e applicarlo correttamente.

E' stato anche acquisito e implementato il software <E20AdS> che per ogni computer contenente dati personali eseguirà quotidianamente il backup di 3 Registri Eventi (Protezione/Sicurezza, Applicazione e Sistema) in una cartella locale e in una centralizzata. Va sottolineato che la copia di backup non sarà eseguita con la normale funzionalità di copia, bensì con la funzionalità speciale interna che mantiene la copia identica al Registro originale (file binario non modificabile, solo cancellabile).

Una volta alla settimana il software comprimerà i files dei Registri in pacchetti unici: ognuno conterrà tutti i Registri eventi di tutti i computers di un certo giorno. Poi realizzerà un'esportazione dei files con modalità che consentano di dimostrarne l'integrità, come richiesto dal Garante.

In ciascun computer il software genererà un file di log, in cui ci sarà il diario delle operazioni riuscite e di quelle eventualmente fallite. In quest'ultimo caso dei messaggi informeranno della necessitò di risolvere l'eventuale problema. Il log servirà anche per validare il software, com'è richiesto dai sistemi di qualità.

Anche in sede centrale il software genererà automaticamente un file di log e avvertirà in caso di problemi.

Per la parte documentale, riportiamo come allegati a questo DPS i 4 documenti principali, a partire da un atto ricognitivo dei rischi.

2) GARANTE PRIVACY: PROVVEDIMENTO A CARATTERE GENERALE (dell'ottobre 2008) in materia di gestione di supporti informatici o computers rottamati o ceduti ad altri.

Trattasi del Provvedimento a carattere generale [integrazione delle misure minime di sicurezza obbligatorie] "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali " del 13 ottobre 2008 in G.U. n. 287 del 9 dicembre 2008.

In sostanza si tratta di INTEGRAZIONI ALLE MISURE DI SICUREZZA OBBLIGATORIE GIA' IN VIGORE.

Il Garante Privacy, valendosi dei poteri a lui conferiti dalla legge, ha emesso il 13 ottobre 2008 un Provvedimento a carattere generale, che integra le misure di sicurezza obbligatorie in caso:

a) un Incaricato ceda ad un collega avente diverso profilo di autorizzazione un qualsiasi supporto informatico (CD, DVD, Floppy Disk, pennette USB, Hard Disk) contenente dati

personali : i files vanno cancellati con appositi software che rendono impossibile a chiunque recuperare i dati

b) un Incaricato dismetta un supporto informatico (CD, DVD, Floppy Disk, pennette USB): prima di gettarlo nei rifiuti deve distruggerlo fisicamente (ad esempio col tritarifiuti, se è in grado di farlo) oppure cancellando l'intero supporto con con appositi software che rendono impossibile a chiunque recuperare i dati
c) venga dimesso o ceduto a terzi o rottamato un computers contenente dati personali: i dischi fissi vanno distrutti con le modalità indicate dal Garante oppure cancellati con appositi software che rendono impossibile a chiunque recuperare i dati

Pertanto, le "misure minime di sicurezza" obbligatorie elencate nell'Allegato B del DLgs 196/2003 – Disciplinare Tecnico , s'intendono ampliate e ricomprendenti quindi anche le nuove regole.

Pertanto, allo scopo di dare dimostrazione di aver predisposto l'applicazione diligente della nuova misura di sicurezza, si riporta quanto eseguito:

1) Abbiamo acquisito un Kit specifico sull'argomento, comprendente Manuale esplicativo, Software speciale in grado di cancellare definitivamente files e interi supporti di memoria, Corso illustrato di formazione per gli Incaricati

2) Abbiamo messo concretamente a disposizione di ciascun Incaricato della Segreteria (o che comunque tratta dati personali con il computer):

    a) il software speciale che esegue la cancellazione definitiva/sicura + un manuale in Italiano di guida all'uso

    b) un file contenente il corso di formazione illustrato, di facile e gradevole lettura. In tal modo si persegue l'obiettivo di formare tali Incaricati, affinché conoscano adeguatamente le nuove prescrizioni

3) E' stata diramata una circolare permanente che spiega a ogni Incaricato la problematica e dà precise, vincolanti istruzioni per accedere al software speciale e al Corso di formazione, dando poi ricevuta di conferma di aver eseguito tutto.

ALLEGATO 10 – VERIFICA ALMENO ANNUALE DEL SISTEMA DI AUTORIZZAZIONE

La normativa:

ALLEGATO B -DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)

A - Trattamenti con strumenti elettronici

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

B - Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. (…)**.** Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Commento

In informatica <**profilo di autorizzazione**> significa che ad ogni <account + password> è associato il diritto e il potere di:

- accedere solo a certe cartelle e programmi (o a tutti)
- compiere solo determinate operazioni (ad esempio: cancellazione di files, formattazione di dischi, aggiornamento dei programmi, creazione o modifica di account e di profili di autorizzazione, backup, ecc..) o di compierle tutte.

Si noti che nelle situazioni più delicate, a volte uno stesso Incaricato può disporre di più account con profili differenziati.

Se gli Incaricati nell'ambito di una rete informatica non hanno profili differenziati, significa che hanno TUTTI il potere di leggere e modificare qualsiasi file, usare qualsiasi programma e compiere qualsiasi operazione. Normalmente, però, nelle reti esiste almeno una differenza di profilo tra l'Amministratore di sistema (a volte chiamato anche Manutentore del Sistema o Manutentore del Software), che ha diritto di compiere QUALSIASI OPERAZIONE, e gli utenti (che non possono compiere alcune operazioni più delicate, quali – per esempio – la creazione o cancellazione di account e la determinazione dei profili di autorizzazione ad essi associati)..

Nel mondo della gestione cartacea, invece, <**profilo di autorizzazione**> significa abilitazione a :

- trattare determinate (o tutte le) categorie di documenti (contenenti dati personali ordinari o sensibili o giudiziari)
- accedere a certi (o a tutti gli) <**archivi ad accesso controllato**>, cioè contenenti dati sensibili o giudiziari,
- accedere a certi (o a tutti gli) archivi , contenenti solo dati personali ordinari non sensibili e non giudiziari (<**archivi ad accesso selezionato>**).

Analisi per categorie di incaricati:

Premessa generale:

Nel corso del 2007 le nomine sono state rifatte perché la ripartizione dei trattamenti e la loro nomenclatura è radicalmente cambiata, a seguito dell'approvazione del REGOLAMENTO DATI SENSIBILI E GIUDIZIARI in attuazione degli articoli 20 e 21 del Dlgs 196/2003, che ha adottato una classificazione definitiva.

Pertanto, il rifacimento delle nomine sostituisce la verifica annuale della sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Classi omogenee di funzioni applicative del D.Lgs 196/2003 - INCARICATI INTERNI PER CLASSI OMOGENEE

1) Unità organizzativa omogenea:
Incaricati Collaboratori del Dirigente Scolastico:

Trattamenti autorizzati (*): **tutti i trattamenti, cartacei e informatici, autorizzati e legittimi per il Titolare**
Categorie di dati autorizzate (*):**tutte quelle autorizzate e legittime per il titolare (per comunicazione e diffusione vedi di seguito)**
Operazioni eseguibili (*): **tutte quelle autorizzate e legittime per il titolare TRATTAMENTI AUTORIZZATI (*): tutti i trattamenti, informatici e non, autorizzati e legittimi per il Titolare, ma solo in caso di assenza del DS o di specifica sua delega**
Operazioni di comunicazione di dati personali: **Tutte, ma solo in caso di assenza del DS o di specifica sua delega**
Operazioni di diffusione di dati personali: **Tutte, ma solo in caso di assenza del DS o di specifica sua delega**
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO"(non contengono dati sensibili e giudiziari): **SI, tutti**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO"(contengono dati sensibili e giudiziari): **SI, tutti**
PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti membri dell'unità organizzativa, salvo ulteriore nomina individuale per compiti specifici ed ulteriori.**
I membri di questa unità organizzativa svolgono necessariamente anche tutte le funzioni tipiche dell'unità organizzativa "docenti", di cui costituiscono un sottogruppo. Quando agiscono esclusivamente come docenti, sono soggetti alle seguenti regole:

Trattamenti informatici autorizzati (*): **solo su PC non contenenti dati personali:**
Tr.5 - Attività educativa, didattica e formativa, di valutazione, limitatamente alla gestione della didattica e della valutazione del docente
Operazioni eseguibili (*): **tutte (per comunicazione e diffusione vedi di seguito)**
Operazioni di comunicazione di dati personali autorizzate: **solo agli alunni e loro familiari o su delega esplicita del Dirigente o del Responsabile**
Operazioni di diffusione di dati personali autorizzate: **nessuna**
(*):Nell'uso della rete informatica, non hanno accesso a files della scuola contenenti dati personali e non possono compiere le operazioni tipiche dell'Amministratore di sistema. Possono accedere solo agli archivi selezionati o controllati specifici della funzione docente. Sono autorizzati a trattare dati di salute nelle funzioni di relative all'attività educativa (aiuto ecc. ad alunni con problemi di handicap o di salute) e all'applicazione delle norme sulla sicurezza ed emergenza (evacuazione di persone con handicap o problemi di salute), di cui al trattamento Tr.1-Gestione del personale
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **SI, quelli pertinenti i trattamenti attribuiti**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **NO, tranne i registri, verbali ecc. che contengano dati sensibili o giudiziari**
PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti membri dell'unità organizzativa, salvo ulteriore nomina individuale per compiti specifici ed ulteriori, come la partecipazione a commissioni disciplinari e al Consiglio d'Istituto.**

2) Unità organizzativa omogenea:
Incaricati Docenti e Assimilati (compresi T.P. e assistenti vari alla didattica, figure di sostegno, ecc.):

Trattamenti non informatici autorizzati: **(*):**

Tr.2 - DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari (solo se membri di commissioni disciplinari; in tal caso sono autorizzati ai trattamenti Tr.1 – Gestione del Personale, senza autorizzazione alla comunicazione o diffusione di dati personali a persone diverse dall'interessato)

Tr.3 - Organismi collegiali e commissioni istituzionali

Tr.4 - Attività propedeutiche all' avvio dell'anno scolastico

Tr.5 - Attività educativa, didattica e formativa, di valutazione

Tr.6 - Rapporti scuola – famiglie : gestione del contenzioso

Nell'attività di docenza e vigilanza in casi eccezionali, in emergenza o in caso di necessità di soccorso immediato, sono autorizzati a trattare dati sensibili di salute relativi agli alunni (Tr.5) o ad altri dipendenti (Tr.1- Gestione del personale), senza autorizzazione alla comunicazione o diffusione di dati personali a persone diverse dall'interessato (o – in caso di minori – da chi esercita la patria potestà); possono informare, però, gli organi addetti al soccorso.

Se partecipano ad attività di addetti all'emergenza, all'evacuazione o al primo soccorso, possono trattare dati sensibili relativi al personale (Tr.1) e agli alunni (Tr.5), senza autorizzazione a comunicare o diffondere tali dati personali; possono , però, informare organi preposti al soccorso.

I membri di questa unità organizzativa partecipano necessariamente all'attività dei Consigli di classe e interclasse, delle commissioni di lavoro e del Collegio Docenti.

Partecipano anche alle attività di organizzazione delle elezioni agli organi collegiali (Tr.3- Attivazione e gestione organi collegiali e commissioni istituzionali; nell'ambito di tale attività possono trattare dati sensibili relativi ad appartenenze sindacali).

Trattamenti informatici autorizzati (*): **solo su PC non contenenti dati personali:**

Tr.5 - Attività educativa, didattica e formativa, di valutazione, limitatamente alla gestione della didattica e della valutazione del docente

Operazioni eseguibili (*): **tutte (per comunicazione e diffusione vedi di seguito)**

Operazioni di comunicazione di dati personali autorizzate: **solo agli alunni e loro familiari o su delega esplicita del Dirigente o del Responsabile**

Operazioni di diffusione di dati personali autorizzate: **nessuna**

(*):Nell'uso della rete informatica, non hanno accesso a files della scuola contenenti dati personali e non possono compiere le operazioni tipiche dell'Amministratore di sistema. Possono accedere solo agli archivi selezionati o controllati specifici della funzione docente. Sono autorizzati a trattare dati di salute nelle funzioni di relative all'attività educativa (aiuto ecc. ad alunni con problemi di handicap o di salute) e all'applicazione delle norme sulla sicurezza ed emergenza (evacuazione di persone con handicap o problemi di salute), di cui al trattamento Tr.1-Gestione del personale

Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **SI, quelli pertinenti i trattamenti attribuiti**

Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **NO, tranne i registri, verbali ecc. che contengano dati sensibili o giudiziari**

PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti membri dell'unità organizzativa, salvo ulteriore nomina individuale per compiti specifici ed ulteriori, come la partecipazione a commissioni disciplinari e al Consiglio d'Istituto.**

3) Unità organizzativa omogenea:
Incaricati Assistenti Amministrativi della Segreteria e eventuali figure assimilabili

Trattamenti autorizzati (*): **tutti i trattamenti, cartacei e informatici, autorizzati e legittimi per il Titolare**
In emergenza o in caso di necessità di soccorso immediato, sono autorizzati a trattare dati sensibili di salute relativi agli alunni (Tr.5 – Gestione degli alunni) o ad altri dipendenti (Tr.1- Gestione del personale), senza autorizzazione alla comunicazione o diffusione di dati personali a persone diverse dall'interessato (o – in caso di minori – da chi esercita la patria potestà); possono informare, però, gli organi addetti al soccorso.
Se partecipano ad attività di addetti all'emergenza, all'evacuazione o al primo soccorso, possono trattare dati sensibili relativi al personale (Tr.1) e agli alunni (Tr.5), senza autorizzazione a comunicare o diffondere tali dati personali; possono , però, informare organi preposti al soccorso.
Partecipano anche alle attività di organizzazione delle elezioni agli organi collegiali (Tr.3- Attivazione e gestione organi collegiali e commissioni istituzionali; nell'ambito di tale attività possono trattare dati sensibili relativi ad appartenenze sindacali).
Categorie di dati autorizzate (*): **tutte quelle autorizzate e legittime per il titolare**
Operazioni eseguibili (*): **tutte quelle autorizzate e legittime per il titolare (per comunicazione e diffusione vedi di seguito)**
Operazioni di comunicazione e diffusione autorizzate: **tutte quelle legittime, ma in ogni caso devono essere previamente autorizzate dal Dirigente o dal Responsabile e devono rientrare nelle seguenti regole:**
Comunicazione di dati comuni a Enti Pubblici: solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela (il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati comuni a Privati: solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).

Comunicazione di dati sensibili o giudiziari: solo nei casi e per i destinatari i previsti dal Regolamento MPI per il trattamento in questione (vedi allegato 1 del Documento Programmatico Sulla Sicurezza)

Diffusione di dati comuni: solo se previsti da specifica norma di legge

Diffusione di dati particolari: solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione di dati di salute: MAI , tranne i casi obbligatori per legge, ma con particolari accorgimenti (esempio graduatorie, ma sostituendo la notazione "portatore di handicap" con un codice; il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Diffusione degli altri dati sensibili e dei dati giudiziari: solo se previsto espressamente da norme di legge o regolamento e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)

Interconnessioni e raffronti di dati con altro titolare: solo nei casi previsti dal Regolamento MPI per il trattamento in questione (vedi allegato 1 del Documento Programmatico Sulla Sicurezza).

(*) Sono autorizzati a tuttI i trattamenti cartacei o informatici in quanto gestiscono attività in stretta collaborazione con il Dirigente e devono assicurare intercambiabilità all'interno dell'unità organizzativa. Nell'uso della rete informatica, hanno accesso a tutti i files della scuola contenenti dati personali e non possono compiere le operazioni tipiche dell'Amministratore di sistema. Possono accedere a tutti gli archivi selezionati o controllati, compreso l'archivio riservato del Dirigente e gli archivi dei docenti.
I membri di questa unità organizzativa partecipano necessariamente anche alle attività di organizzazione delle elezioni agli organi collegiali (Tr.3- Attivazione e gestione organi collegiali e commissioni istituzionali; nell'ambito di tale attività possono trattare dati sensibili relativi ad appartenenze sindacali).
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **SI, tutti (tranne archivi riservati del Dirigente)**
Autorizzazione ad accedere ad archivi ad 2ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **SI, tutti (tranne archivi riservati del Dirigente)**

PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti membri dell'unità organizzativa, salvo ulteriore nomina individuale per compiti specifici ed ulteriori, come la partecipazione a commissioni disciplinari e al Consiglio d'Istituto.**

4) Unità organizzativa omogenea: Incaricati Collaboratori Scolastici-

Trattamenti autorizzati (*): **tutti i trattamenti, con operazioni non informatiche, relativamente a funzioni elementari di supporto. Nell'ambito dei trattamenti informatici, possono solo consultare a video elenchi con dati comuni.**
Categorie di dati autorizzate (*): **solo dati comuni, tranne le seguenti eccezioni (*):**
(*)
Nell'attività di vigilanza e collaborazione, in casi eccezionali, in emergenza o necessità di soccorso immediato sono autorizzati a trattare dati sensibili di salute relativi al personale (Tr.1) e agli alunni (Tr.5), senza autorizzazione alla

comunicazione o diffusione di dati personali a persone diverse dall'interessato (o – in caso di minori – da chi esercita la patria potestà) possono informare, però, gli organi interni addetti al soccorso.
I membri di questa unità organizzativa partecipano necessariamente anche alle attività di organizzazione delle elezioni agli organi collegiali (Tr.3- Attivazione e gestione organi collegiali e commissioni istituzionali; nell'ambito di tale attività possono trattare dati sensibili relativi ad appartenenze sindacali).
Se partecipano a commissioni disciplinari, nell'ambito di "Tr.2 - DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari" sono autorizzati ai trattamenti "Tr.1 – Gestione del Personale" anche dati sensibili e giudiziari, senza autorizzazione alla comunicazione o diffusione di dati personali a persone diverse dall'interessato).
Se partecipano ad attività di addetti all'emergenza, all'evacuazione o al primo soccorso, sono autorizzati a trattare dati sensibili di salute relativi al personale (Tr.1) e agli alunni (Tr.5), senza autorizzazione alla comunicazione o diffusione di dati personali a persone diverse dall'interessato; possono , però, informare organi preposti al soccorso.
Operazioni eseguibili (**): **solo funzioni di supporto**
(**) **Possono accedere ad elenchi cartacei o informatici con dati comuni relativi alle attività scolastiche. Sono autorizzati a trattare dati di salute limitatamente a funzioni di supporto all'attività di cui al trattamento Tr.5-Attività educativa (aiuto ad alunni con problemi di handicap o di salute) e all'applicazione delle norme sulla sicurezza ed emergenza (evacuazione di persone con handicap o problemi di salute), di cui al trattamento Tr.1-Gestione del personale.**
Possono prendere in consegna, trasportare, custodire materiali contenenti dati sensibili, senza autorizzazione a consultarli o a mostrali a chicchessia.
Operazioni di comunicazione di dati personali autorizzate: **nessuna autonomamente, però possono fungere da supporto fisico alla consegna e ricezione di documenti a a mano, tramite posta o spedizioniere, tramite fax, tramite telefono e fonogrammi.**
Operazioni di diffusione di dati personali autorizzate: **nessuna autonomamente, però possono fungere da supporto alle operazioni di diffusione.**

Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **SI, limitatamente ad elenchi, dati anagrafici, classe frequentata e altre attività di supporto**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): NESSUNO

PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti membri dell'unità organizzativa, salvo ulteriore nomina individuale per compiti specifici ed ulteriori, come la partecipazione a commissioni disciplinari e al Consiglio d'Istituto.**

5) Unità organizzativa omogenea:
Incaricati Membri degli Organi Collegiali (persone esterne alla scuola nei Consigli di classe; tutti i membri del Consiglio d'Istituto e della Giunta esecutiva)

Trattamenti autorizzati (*):
Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.
Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari
Tr.3 Organismi collegiali e commissioni istituzionali
Tr.4 Attività propedeutiche all' avvio dell'anno scolastico
Tr.5 Attività educativa, didattica e formativa, di valutazione
Tr.6 Rapporti scuola – famiglie : gestione del contenzioso
Tr.7 Fornitori e clienti
Tr.8 Gestione finanziaria e contabile
Tr.9 Gestione Istituzionale
tutti i trattamenti non informatici, relativamente alle funzioni strettamente connesse all'organo di cui fanno parte. Nell'ambito dei trattamenti informatici, possono solo consultare a video dati comuni.
Categorie di dati autorizzate (*): **solo dati comuni, tranne i rarissimi dati sensibili o giudiziari strettamente indispensabili per l'attività dell'organo di cui fanno parte.**
Operazioni eseguibili (*): **tutte, fuorché diffusione e comunicazione**

(*)Possono accedere ad elenchi cartacei o informatici con dati comuni relativi alle attività scolastiche.

Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): NO, tranne verbali, registri, atti dell'organo partecipato
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): NO, tranne verbali, registri, atti dell'organo partecipato
Operazioni di comunicazione di dati personali autorizzate: **nessuna autonomamente, però possono fungere da supporto alla comunicazione verso alunni e loro familiari**
Operazioni di diffusione di dati personali autorizzate: **nessuna**
PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti membri dell'unità organizzativa, salvo ulteriore nomina individuale per compiti specifici ed ulteriori.**

6) Altri Incaricati interni, con incarico aggiuntivo rispetto a quello dell'unità organizzativa di appartenenza

6.1) Addetto al backup periodico dei dati della Segreteria con funzioni di coordinatore per il "disaster recovery" e le prove di ripristino

Trattamenti autorizzati: **tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni**
Categorie di dati autorizzate: **tutti dati, purché sia indispensabile prenderne visione**
Operazioni eseguibili: **tutte, fuorché diffusione e comunicazione**
Operazioni di comunicazione di dati personali autorizzate: **nessuna**
Operazioni di diffusione di dati personali autorizzate: **nessuna**
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **solo archivi elettronici e rigorosamente nei limiti delle esigenze dell'attività**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **solo archivi elettronici e rigorosamente nei limiti delle esigenze dell'attività**
PROFILO DI AUTORIZZAZIONE: **individuale**

6.2) Custode delle chiavi e Vice- Custode delle chiavi degli archivi ad accesso controllato

Trattamenti autorizzati: **tutti, per la gestione degli archivi ad accesso controllato**
Categorie di dati autorizzate: **tutti dati, purché sia indispensabile prenderne visione**
Operazioni eseguibili: **tutte le operazioni su supporti non informatici, fuorché diffusione e comunicazione**
Operazioni di comunicazione di dati personali autorizzate: **nessuna**
Operazioni di diffusione di dati personali autorizzate: **nessuna**
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): si
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **si**
PROFILO DI AUTORIZZAZIONE: **identico per custode delle chiavi e vicecustode**

6.3) Incaricato Tecnico interno della Manutenzione del Software o dell'Hardware

Trattamenti autorizzati: **tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni**
Categorie di dati autorizzate: **tutti dati, purché sia indispensabile prenderne visione**
Operazioni eseguibili: **tutte, fuorché diffusione e comunicazione**
Operazioni di comunicazione di dati personali autorizzate: **nessuna**
Operazioni di diffusione di dati personali autorizzate: **nessuna**
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **solo archivi elettronici e rigorosamente nei limiti delle esigenze dell'attività**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **solo archivi elettronici e rigorosamente nei limiti delle esigenze dell'attività**
PROFILO DI AUTORIZZAZIONE: **individuale**

6.4) Custode delle passwords

Trattamenti autorizzati : **tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni**
Categorie di dati autorizzate : **nessuna**
Operazioni eseguibili: **solo la presa in carico delle buste delle password e il controllo che tutti abbiano provveduto alla scadenza.**
Operazioni di comunicazione di dati personali autorizzate: **nessuna**
Operazioni di diffusione di dati personali autorizzate: **nessuna**
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **no**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **no**
PROFILO DI AUTORIZZAZIONE: **individuale**

6.5) Personale incaricato della funzione di RLS (Rappresentante dei lavoratori per Sicurezza) ai sensi del Dlgs 626/1994.

Diritto di consultazione di tutti i documenti e materiali informatici strettamente inerenti alla funzione e risultanti come diritto di conoscenza
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **NO, i documenti saranno estratti da apposito incaricato e offerti per la consultazione**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **NO, i documenti saranno estratti da apposito incaricato e offerti per la consultazione**
PROFILO DI AUTORIZZAZIONE: **individuale**

6.6) Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap

Trattamenti autorizzati **: tutti i trattamenti informatizzati e non relativi all'attività**
Tr.4 Attività propedeutiche all' avvio dell'anno scolastico
Tr.5 Attività educativa, didattica e formativa, di valutazione
Categorie di dati autorizzate : **tutti dati di salute, purché sia indispensabile trattarli**
Operazioni eseguibili: **tutte, fuorché diffusione e comunicazione. La comunicazione può avvenire solo su accordo del Dirigente o del Responsabile e solo agli enti indicati nelle schede 4 e 5 allegate al REGOLAMENTO.**
Operazioni di comunicazione di dati personali autorizzate: solo nell'ambito dei trattamenti degli alunni (Tr.4 e Tr.5) e verso i destinatari tassativamente indicati per tali trattamenti (vedi allegato 1 del Documento Programmatico Sulla Sicurezza)

Operazioni di diffusione di dati personali autorizzate: **nessuna**
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **SI, nei limiti delle esigenze dell'attività**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **SI, ma rigorosamente nei limiti delle esigenze dell'attività**
PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti gli addetti a questa funzione.**

6.7) Incaricato interno per la creazione e gestione del sito web

Trattamenti autorizzati: **i trattamenti informatici, rigorosamente nei limiti relativi alle seguenti attività::**
Tr.10 Gestione sito web dell'istituto
Categorie di dati autorizzate: **solo dati comuni, purché sia indispensabile prenderne visione**
Operazioni eseguibili: **poiché ogni pubblicazione sul sito web equivale a una diffusione, dev'esser previamente autorizzata dal Titolare. Vietata ogni comunicazione di dati all'esterno.**
Operazioni di comunicazione di dati personali autorizzate: nessuna
Operazioni di diffusione di dati personali autorizzate: **pubblicazione nel sito web esclusivamente di quei dati comuni la cui possibilità di pubblicazione sia prevista da norme di legge**
Autorizzazione ad accedere ad archivi ad "ACCESSO SELEZIONATO" (non contengono dati sensibili e giudiziari): **SI, nei limiti delle esigenze dell'attività**
Autorizzazione ad accedere ad archivi ad "ACCESSO CONTROLLATO" (contengono dati sensibili e giudiziari): **NO**
PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti gli addetti a questa funzione.**

6.8) Amministratore di sistema e assimilato

NORMATIVA DA APPLICARE : ***quando agisce come nostro Incaricato è tenuto ad applicare le regole stabilite per gli Enti Pubblici (art. 18-22 del Codice Privacy) e non gli articoli destinati agli imprenditori ecc. Privati (art. 23-27), che deve invece applicare nella sua restante attività privata !***

Trattamenti autorizzati: **tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni**

Categorie di dati autorizzate: **tutti dati, purché sia indispensabile prenderne visione**

Operazioni eseguibili: **tutte, fuorché diffusione e comunicazione**

Operazioni di comunicazione di dati personali autorizzate: **nessuna**

Operazioni di diffusione di dati personali autorizzate: **nessuna**

PROFILO DI AUTORIZZAZIONE: **individuale**

7) Incaricati esterni (persone fisiche)

7.1) Incaricato esterno della funzione di RSPP

NORMATIVA DA APPLICARE : ***quando agisce come nostro Incaricato è tenuto ad applicare le regole stabilite per gli Enti Pubblici (art. 18-22 del Codice Privacy) e non gli articoli destinati agli imprenditori ecc. Privati (art. 23-27), che deve invece applicare nella sua restante attività privata !***

Trattamenti autorizzati: **tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare:**

Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.

Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari

Tr.3 Organismi collegiali e commissioni istituzionali

Tr.4 Attività propedeutiche all' avvio dell'anno scolastico

Tr.5 Attività educativa, didattica e formativa, di valutazione

Categorie di dati autorizzate: **tutti dati, purché sia indispensabile trattarli.**

Operazioni eseguibili: **tutte, fuorché diffusione e comunicazione.**

Operazioni di comunicazione di dati personali autorizzate: **solo quelle indispensabili alla funzione**

Operazioni di diffusione di dati personali autorizzate: **nessuna**

Autorizzazione ad accedere ad archivi ad <ACCESSO SELEZIONATO>(non contengono dati sensibili e giudiziari): SI, nei limiti delle esigenze dell'attività

Autorizzazione ad accedere ad archivi ad <ACCESSO CONTROLLATO>(contengono dati sensibili e giudiziari): SI, ma rigorosamente nei limiti delle esigenze dell'attività

PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti gli addetti a questa funzione.**

7.2) Incaricato Tecnico Esterno della Manutenzione del Software o dell'Hardware

l'incaricato sarà chiamato solo in caso di necessità dopo l'intervento dell'incaricato interno

NORMATIVA DA APPLICARE : ***quando agisce come nostro Incaricato è tenuto ad applicare le regole stabilite per gli Enti Pubblici (art. 18-22 del Codice Privacy) e non gli articoli destinati agli imprenditori ecc. Privati (art. 23-27), che deve invece applicare nella sua restante attività privata !***

Trattamenti autorizzati: **tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni**

Categorie di dati autorizzate: **tutti dati, purché sia indispensabile prenderne visione**

Operazioni eseguibili: **tutte, fuorché diffusione e comunicazione**

Operazioni di comunicazione di dati personali autorizzate: **nessuna**

Operazioni di diffusione di dati personali autorizzate: **nessuna**

PROFILO DI AUTORIZZAZIONE: **individuale**

7.3) Animatore Esterno

NORMATIVA DA APPLICARE : ***quando agisce come nostro Incaricato è tenuto ad applicare le regole stabilite per gli Enti Pubblici (art. 18-22 del Codice Privacy) e non gli articoli destinati agli imprenditori ecc. Privati (art. 23-27), che deve invece applicare nella sua restante attività privata !***

Trattamenti autorizzati: **i seguenti trattamenti non informatici:**

Tr.4 - Attività propedeutiche all' avvio dell'anno scolastico

Tr.5 - Attività educativa, didattica e formativa, di valutazione

, rigorosamente nei limiti relativi alle funzioni

Categorie di dati autorizzate: **tutti dati, purché sia indispensabile trattarli per al funzione svolta**

Operazioni eseguibili: **tutte, fuorché diffusione e comunicazione**

Operazioni di comunicazione di dati personali autorizzate: **nessuna (solo all'interessato ai suoi genitori se minorenne o incapace)**

Operazioni di diffusione di dati personali autorizzate: **nessuna**

Autorizzazione ad accedere ad archivi ad <ACCESSO SELEZIONATO>(non contengono dati sensibili e giudiziari): **solo archivi elettronici e rigorosamente nei limiti delle esigenze dell'attività**

Autorizzazione ad accedere ad archivi ad <ACCESSO CONTROLLATO>(contengono dati sensibili e giudiziari): **solo archivi elettronici e rigorosamente nei limiti delle esigenze dell'attività**

PROFILO DI AUTORIZZAZIONE: **per ragioni di funzionalità si ritiene necessario mantenerlo identico per tutti gli addetti a questa funzione.**

8) RESPONSABILI INTERNI DEL TRATTAMENTO

8.1) Responsabile del trattamento : il DGSA limitatamente ai trattamenti della segreteria e degli Operatori Scolastici-Personale ausiliario

Trattamenti autorizzati: **tutti i trattamenti, informatici e non, autorizzati e legittimi per il Titolare**
Categorie di dati autorizzate : **tutte quelle autorizzate e legittime per il titolare**
Operazioni eseguibili : **tutte quelle autorizzate e legittime per il titolare**

9) RESPONSABILI ESTERNI (titolari persone giuridiche o titolari con dipendenti)

ALLEGATO 11 Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Premessa

La logica di questa misura di sicurezza è di rendere edotti formalmente tutti gli organi che hanno poteri deliberativi di spesa o hanno poteri di controllo che :

1) esiste l' obbligo di azioni conseguenti al Codice Privacy e che esse hanno un costo, anche perché vengono richiesti ogni anno interventi incrementativi dei livelli di sicurezza in tutti i trattamenti dei dati personali, nonché – ovviamente – la rimozione di tutte le criticità cui i dati stessi sono esposti in modo abnorme.
2) gli organi che hanno gestito il bilancio hanno perciò tenuto nel debito conto le sopraindicate esigenze
3) l'Ente o Azienda è in regola e quindi al riparo dalle importanti sanzioni penali e dalle possibili richieste civilistiche di danni degli interessati a cui i dati personali detenuti dall'istituto si riferiscono.

Testo da inserire nella relazione accompagnatoria al bilancio

Ai sensi del punto 26 del Disciplinare Tecnico – Allegato B del Dlgs 196/2003 <Codice in materia di protezione dei dati personali>, esiste l'obbligo di riferire quanto segue:

In applicazione della normativa Privacy il Titolare dei trattamenti di dati personali svolti da questo Istituto è l'Istituto stesso, rappresentato pro tempore dal Dirigente Scolastico in carica.

Il Titolare ha provveduto a mettere a norma secondo le regole privacy tutti i trattamenti svolti, sia sotto il profilo dell'adozione delle misure minime obbligatorie, che sarebbe reato penale disattendere, sia per tutti gli altri adempimenti la cui inosservanza renderebbe illeciti i trattamenti di dati personali.

Il più rilevante degli adempimenti è la redazione annuale, entro il 31 marzo, del <Documento programmatico Sulla Sicurezza>, il quale è una puntuale, aggiornata ricognizione dei trattamenti in essere e della qualità stato delle misure di sicurezza che proteggono i dati personali a noi affidati dagli alunni e loro famiglie, dai dipendenti e assimilati, da altri che sono in rapporto con il nostro Istituto.

Il <Documento programmatico Sulla Sicurezza> contiene anche un progetto per incrementare nel tempo in modo progressivo i livelli di sicurezza, investendo sia nella formazione dei nostri dipendenti, sia nel miglioramento delle strutture e degli strumenti utilizzati.

In modo particolare il Dlgs 196/2003 <Codice in materia di protezione dei dati personali> prevede che sia posta particolare attenzione alla gestione informatica dei dati personali, in quanto il Legislatore ha ritenuto che potesse essere il massimo tallone d'Achille per la sicurezza dei dati personali stessi. Pertanto impone elevati standard dei sistemi informatici (hardware e software) e una certa ridondanza dell'hardware disponibile. Impone, inoltre, spese ricorrenti assai significative per software continuamente aggiornati, come i sistemi professionali antivirus.

Pertanto nel bilancio hanno trovato e troveranno necessariamente copertura una serie di spese e investimenti assai cospicui.

A parte il fatto che l'adozione di questi elevati standard di sicurezza è obbligatoria per legge e sanzionata penalmente, si deve osservare che talune misure hanno comunque ricadute generali benefiche. Ad esempio, l'obbligo di avere un backup, ovvero copia di salvataggio, almeno settimanale di tutti i nostri dati informatici fa sì che non veniamo colti impreparati da improvvise rotture dell'hardware o dall'azione distruttiva di virus informatici, subendo enormi perdite di tempo lavorativo, temporanea paralisi operativa, ecc.

ALLEGATO 12 - ATTO RICOGNITIVO dei rischi in materia di Amministratori di Sistema e Assimilati

Premessa:

Riportiamo qui di seguito, come allegato, l'ATTO RICOGNITIVO dei rischi in materia di Amministratori di Sistema e Assimilati, in quanto esso integra il presente Documento Programmatico sulla Sicurezza e in particolare l'analisi dei rischi e delle misure di sicurezza adottate.

ATTO RICOGNITIVO in materia di Amministratori di Sistema e Assimilati

Il sottoscritto Giulio Ottaviani Legale Rappresentante dell'Istituto Comprensivo Quartieri Nuovi – Via Lanzi -60131 Ancona, Titolare dei Trattamenti Personali :

In attuazione del provvedimento di carattere generale emesso dal Garante Privacy in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)"" e successive modifiche e integrazioni"

procede alla seguente ricognizione della situazione esistente riguardo all'esistenza:

- di sistemi informatici o base-dati ricadenti nel Provvedimento citato,
- di figure professionali rientranti nella definizione di Amministratore di Sistema o si Assimilabile ad esso
- di rischi per i dati personali contenuti nei sistemi informatici a seguito dell'intervento di figure che eseguono manutenzione o gestione del software o dell'hardware.

1) Dotazione di reti di computers e di singoli elaboratori non connessi in rete che trattano dati personali:

a) rete di 8 workstations della segreteria facenti capo a un server (numero suscettibile di piccole variazioni a seconda delle situazioni). Contengono grande quantità di dati personali, anche delicati, quasi sensibili e sensibili.

b) rete di 33 computer a disposizione dei dipendenti ed alunni (esclusa perché non tratta dati personali)

c) n. 1 computer non in rete a disposizione del personale (escluso perché non tratta dati personali)

d) n. 8 computer portatili per la sala proiezioni ed altro (escluso perché non tratta dati personali)

Responsabilità dal punto di vista Privacy

La gestione dei computer di cui al punto a) **dipende dal Responsabile del trattamento**, che pertanto può avere anche l'incarico da parte del Titolare di eseguire le verifiche annuali sull'attività degli Amministratore di Sistema o Assimilati che operano su tali macchine.

Il punto b) è gestito direttamente dal Titolare dei Trattamenti Personali.

2) Presenza di database contenenti dati personali

a) Si, la rete utilizza il software SISSI, funzionante mediante Database crittografato, contenente dati personali di alunni e loro familiari, dipendenti e loro familiari, cui si accede mediante password d'ingresso all'applicazione. Contiene grande quantità di dati personali, anche delicati, quasi sensibili e sensibili.

3) Presenza di reti e di apparati di sicurezza: NO

4) Presenza di sistemi software complessi : NO

Censimento degli interventi a livello software per la manutenzione/gestione del sistema:

Punto 1 (rete segreteria):

Manutenzione a livello software e di sistema:

a) un incaricato esterno, esperto in informatica, viene su chiamata o al bisogno per circa 2 ore alla settimana: poiché il suo intervento è sistematico è assimilabile a un AdS e pertanto si dà corso alla nomina di cui al Provvedimento in esame, alla registrazione degli accessi logici e alla verifica annuale. La nomina spetta al Responsabile del Trattamento.

Creazione-eliminazione di account, gestione delle credenziali e profili di autorizzazione, ecc. e altri punti dell'allegato B del DLgs 196:

a) il tecnico di cui al punto precedente crea ed elimina account gestendo le credenziali degli utenti, modifica al bisogno profili di autorizzazione, ecc. : poiché il suo intervento è sistematico anche su questo punto è assimilabile a un AdS e pertanto si dà corso alla nomina di cui al Provvedimento in esame, alla registrazione degli accessi logici e alla verifica annuale. La nomina spetta al Responsabile del Trattamento.

b) Il backup è impostato a livello generale dal tecnico di cui al punto precedente, che esegue anche le prescritte prove periodiche per verificarne il buon funzionamento: poiché il suo intervento è sistematico anche su questo punto è assimilabile a un AdS e questa funziona va richiamata nella nomina di cui al punto precedente.

c) Il backup periodico è eseguito settimanalmente a cura di un incaricato del trattamento, che deve solo inserire il disco e farlo partire: è un intervento sistematico ma di contenuto assai limitato; tuttavia – considerato che teoricamente potrebbe asportare la copia di tutti i dati - a causa di questo rischio si decide di considerarlo assimilabile a un AdS e pertanto si dà corso alla nomina di cui al Provvedimento in esame, alla registrazione degli accessi logici e alla verifica annuale. La nomina spetta al Responsabile del Trattamento.

d) Custode delle password *(persona che riceve da ogni utente di computer copia in busta chiusa della sua password, quando la rinnova; il custode mantiene in luogo sicuro le buste e le apre solo nei casi previsti e con le previste procedure)***:** è un incaricato che svolge sistematicamente tale funzione. Considerato il rischio che in teoria potrebbe accedere a qualunque computer del sistema, avvalendosi delle password a lui conferite, ancorché in busta chiusa, a causa di questo rischio si decide di considerarlo assimilabile a un AdS e pertanto si dà corso alla nomina di cui al Provvedimento in esame, alla registrazione degli accessi logici e alla verifica annuale. La nomina spetta al Responsabile del Trattamento.

e) Responsabile dell'impostazione e delle prove del Disaster Recovery: è il tecnico di cui al punto a). Considerato che si tratta di interventi episodici (massimo 2 volte all'anno) e che è già valutato come assimilato a un AdS, per questo punto non è valutato in tal modo.

Punto 2 (database):

a) un tecnico esterno viene solo in caso di malfunzionamenti o aggiornamenti: la sua presenza è assolutamente episodica e quindi non va considerato assimilabile a un AdS e pertanto non si dà corso alla nomina di cui al Provvedimento in esame, alla registrazione degli accessi logici e alla verifica annuale. La nomina spetta al Responsabile del Trattamento.

Censimento degli interventi a livello hardware per la manutenzione/riparazione/gestione del sistema:

Gli interventi di questo tipo sono compiuti sempre da altro tecnico esterno, peraltro nominato Incaricato esterno del trattamento.

I suoi interventi sono relativamente poco frequenti, a volte non toccano il computer vero e proprio (ad esempio, sostituzione dei monitor). Gli interventi che gli consentirebbero di accedere a dati personali contenuti nel sistema informatico sono episodici e avvengono sempre in orario lavorativo e in presenza di incaricati interni. Non dispone di un proprio account per entrare nel sistema informatico. Per tali motivi si ritiene che il rischio di visione di dati cui non ha diritto d'accesso sia inesistente, come anche non esista il rischio di asportazione di dati. Pertanto si valuta la sua figura come non assimilabile ad un AdS e pertanto non si dà corso alla nomina di cui al Provvedimento in esame, alla registrazione degli accessi logici e alla verifica annuale.

L'unico elemento di rischio è l'eventuale sostituzione di dischi fissi guasti con asportazione di quello guasto o asportazione di computer da portare all'esterno in quanto obsoleti. In entrambi i casi si applicherà il **Provvedimento a carattere generale [*integrazione delle misure minime di sicurezza obbligatorie*] del Garante Privacy del** 13 ottobre 2008 in materia di **"Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali ",** in particolare per quanto riguarda: dismissione o cessione ad altri incaricati di supporti informatici (CD, DVD, Floppy Disk, pennette USB, Hard Disk) contenenti dati personali : vanno distrutti con le modalità indicate oppure cancellati con appositi software che rendono impossibile a chiunque leggere i dati.

Esame della situazione sul punto specifico della conoscibilità ai dipendenti dell'identità degli AdS o Assimilati che intervengono nella gestione della loro posizione

[punto 2-c 2° e 3° e punto d) paragrafo delle prescrizioni del Provvedimento]

L'attività degli AdS o Assimilati riguarda anche indirettamente servizi o sistemi informatici che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori ?

Si. Pertanto il Titolare è tenuto a rendere nota o almeno conoscibile ai dipendenti l'identità degli AdS o Assimilati in relazione ai diversi servizi informatici cui questi sono preposti.

In pratica tutti gli AdS e Assimilati individuati in precedenza rientrano in questa fattispecie. Pertanto verrà emessa la seguente Circolare interna, di cui si indica il facsimile:

Facsimile

Ai sensi del Codice Privacy e del Provvedimento del Garante Privacy in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati **con strumenti elettronici"** relativamente alle attribuzioni delle funzioni di amministratore di sistema (27 novembre 2008) il Titolare informa tutti i dipendenti che i loro dati personali sono trattati, oltre che dagli Incaricati del trattamento, **anche dalle seguenti figure che svolgono funzioni assimilabili a quelle di un Amministratore di Sistema informatico o di base-dati:**

Prof. Saverio Rosati Addetto alla manutenzione e gestione del software, alla gestione delle credenziali si accesso al sistema, ai profili di autorizzazione degli utenti del sistema, all'organizzazione del backup periodico dei dati, dell'impostazione e delle prove del Disaster Recovery.

Sig.ra Loretta Lucconi Addetto al backup periodico dei dati

Sig.ra Loretta Lucconi Addetto alla custodia delle password

Sig. Filippo Rosignoli nato 21.01.1966 Ancona (incaricato esterno) addetto alla manutenzione e gestione del software.

Si chiarisce, inoltre, che non esistono servizi di amministrazione di sistema, sempre relativi a trattamenti di dati personali dei dipendenti, affidati in *outsourcing*. Naturalmente per legge il calcolo e l'emissione dei cedolini dello stipendio è affidato al Tesoro.

Data ……. *Firma del Titolare*

NOMINE

[punti a) e b) delle prescrizioni del Provvedimento]

a. Valutazione delle caratteristiche soggettive
L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29. *[requisiti di affidabilità, esperienza, condotta]*

b. Designazioni individuali
La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Tutte le persone individuate nel presente atto come ricadenti nella normativa relativa agli AdS e Assimilati saranno oggetto di nomina individuale specifica, come previsto. Per ragioni di chiarezza, si preferisce sommare la nuova nomina a quella ad Incaricato, quando già emessa.

ELENCO DEGLI AMMINISTRATORI DI SISTEMA ED ASSIMILATI

[punto 2-c 1° paragrafo delle prescrizioni del Provvedimento]

Si prende atto dell'obbligo che gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

Pertanto sarà immediatamente redatto tale documento interno, che riporterà i nominativi delle persone individuate in questo documento, con a fianco la data di nascita ed eventualmente il tipo di inquadramento come dipendenti, nonché tutte le funzioni a loro attribuite ricadenti nella normativa in esame e già individuate in altra parte del presente atto ricognitivo.

Naturalmente tale documento interno sarà aggiornato ad ogni cambiamento.

Registrazione degli accessi *logici ai sistemi di elaborazione e agli archivi elettronici da parte degli AdS e Assimilati*

[punto 2-f delle prescrizioni del Provvedimento]

E' stato acquisito e implementato in ogni computer un software in grado di gestire i Registri degli Eventi di Protezione-Sicurezza, Applicazione e Sistema. Anche sulla base dei riferimenti del Garante, si ritiene che tali registrazioni soddisfino in modo adeguato, rispetto alla situazione di questo Titolare, l'obbligo di contenere i riferimenti temporali e la descrizione dell'evento che le ha generate. Inoltre sono di per sé files crittografati non alterabili.

Tale software esegue quotidianamente copia di tali registri sia in una diversa cartella del computer di origine sia in un computer diverso, per assicurarne l'esistenza anche in caso di guasto o perdita del computer d'origine. Per non sovrapporsi avranno un nome che comprende anche la data. Questa soluzione garantisce le richieste **caratteristiche di completezza** alle registrazioni.

Quanto ai requisiti di **inalterabilità** e **possibilità di verifica della loro integrità essi saranno garantiti da una di queste due soluzioni:**

a) dalla periodica copia dei files dei Registri in CD o DVD NONRISCRIVIBILE, che sarà poi conservato in luogo sicuro, in modo che ogni file sia mantenuto per almeno 6 mesi.

oppure

b) mediante spedizione dei files dei Registri come **allegato di un messaggio di Posta Elettronica Certificata autospedito,** che – **una volta ricevuto** - sarà poi conservato con cura insieme all'impronta digitale che lo accompagna e **che ne garantisce piena possibilità di verifica della loro integrità. Queste email saranno conservate per almeno 6 mesi.**

Verifica delle attività degli AdS e Assimilati

[punto 2-e) delle prescrizioni del Provvedimento]

L'operato delle figure individuate come ricadenti nella normativa sugli AdS e Assimilati sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Sarà utilizzata un'apposita scaletta, comprendente tutti i fattori comportamentali da verificare, inoltre saranno esaminati a campione alcuni Registri degli Eventi per verificare la regolarità in particolare degli orari degli accessi.

Tale verifica, di norma, sarà eseguita in occasione della redazione annuale del Documento Programmatico sulla Sicurezza, di cui costituirà un allegato.

Ai sensi del punto 3 *bis*. , nel caso in cui il Titolare del trattamento attribuisca a un Responsabile del trattamento il compito di dare attuazione alle prescrizioni di cui al punto 2, lett. d) [Servizi in outsourcing] ed e) [Verifica annuale delle attività dell'AdS], avverrà mediante integrazione della designazione del Responsabile da parte del titolare del trattamento, ai sensi dell'art. 29 del Codice, o anche tramite opportune clausole contrattuali;

ALLEGATO 13 - Nomina di Amministratori di Sistema o assimilati

Premessa:

Riportiamo qui di seguito, come allegato, ***le nomine degli Amministratori di Sistema e Assimilati***, in quanto esse integrano il presente Documento Programmatico sulla Sicurezza e in particolare l'analisi delle misure di sicurezza adottate.

Nomina di Amministratori di Sistema o assimilati

Protocollo n. 1875/C1 Data, 31 marzo 2011

Oggetto: **designazione di Amministratori di Sistema e Assimilati**

IL DIRIGENTE SCOLASTICO

Visto il D.Lgs 196/2003 "Codice in materia di protezione dei dati personali", che d'ora in poi nel presente documento sarà richiamato semplicemente come "Codice";

Visti gli articoli 29 e 30 del Codice in materia di designazioni di Incaricati e Responsabili;

Visto l'art. 33 del Codice , che impone di adottare le misure di sicurezza disposte dal Codice stesso e almeno le misure minime individuate dall'allegato B del Codice stesso;

Visto il Provvedimento di carattere generale (di seguito chiamato semplicemente <Provvedimento>) emesso dal Garante Privacy in materia di <<Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)"> (e sue successive integrazioni, modifiche e chiarificazioni);

Visto in particolare il comma 2 dell'art. 29 del Codice **che il Provvedimento appena citato indica come riferimento per la selezione degli Amministratori di sistema e assimilati: "**Se designato, il responsabile è individuato tra soggetti che per esperienza**, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni** in materia di trattamento, ivi compreso il profilo relativo alla sicurezza."

determina

di assegnare alla propria persona le attività e funzioni assimilabili a quello di Amministratore di

in considerazione dell'esperienza maturata.

Pertanto, il sottoscritto , nel senso e per i fini previsti dal citato Provvedimento, assume la qualifica di "Amministratore di Sistema informatico" relativamente al trattamento di dati svolto nell'ambito della finalità esclusiva di gestione/manutenzione del software dei computer e della rete di computer della segreteria.

Ai sensi del citato Provvedimento i compiti sono qui esplicitati nel dettaglio:

a) **gestione e manutenzione della rete informatica**
b) **caricamento, gestione e manutenzione del software nei computers della rete. compresi antivirus e firewall; risoluzione di eventuali malfunzionamenti riscontrati**
c) **creazione degli account utente, con consegna delle credenziali iniziali, e associazione di eventuali specifici profili di autorizzazione all'utente**
d) **eliminazione di account non più in uso**
e) **impostazione e supervisione del backup ed esecuzione delle relative prove e verifiche previste dal Codice**
f) **impostazione e supervisione delle procedure di "Disasyer Recovery" ed esecuzione delle relative prove e verifiche previste dal Codice**

La presente designazione è altresì accompagnata dalle seguenti disposizioni:

1) **Nell'attività si deve dare piena e rigorosa applicazione alle regole del Codice Privacy, in particolare alle misure di sicurezza, e ai provvedimenti di carattere generale del Garante.**

In applicazione delle prescrizioni contenute nel citato Provvedimento del Garante Privacy:

- **L'Istituto provvederà alla registrazione continua degli eventi informatici che riguardano tutti gli accessi logici nonché degli eventi di sistema e di applicazioni. Tali Registri eventi saranno conservati per almeno 6 mesi in modo inalterabile e che consenta la verifica dell'integrità.**
- **Almeno una volta all'anno l'attività sarà oggetto di verifica complessiva, utilizzando anche l'analisi a campione dei Registri Eventi**

2° Facsimile di Nomina di Amministratori di Sistema o assimilati

Protocollo n. 1881/C1 Ancona 30 marzo 2010

Sig.ra Loretta Lucconi.
C.F. LCCLTT58C48A271M
Via Ginelli 15
60131 ANCONA

Oggetto: **designazione di Amministratori di Sistema e Assimilati**

Visto il D.Lgs 196/2003 "Codice in materia di protezione dei dati personali", che d'ora in poi nel presente documento sarà richiamato semplicemente come "Codice";

Visti gli articoli 29 e 30 del Codice in materia di designazioni di Incaricati e Responsabili;

Visto l'art. 33 del Codice , che impone di adottare le misure di sicurezza disposte dal Codice stesso e almeno le misure minime individuate dall'allegato B del Codice stesso;

Visto il Provvedimento di carattere generale (di seguito chiamato semplicemente <Provvedimento>) emesso dal Garante Privacy in materia di <<Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)"> (e sue successive integrazioni, modifiche e chiarificazioni);

Visto in particolare il comma 2 dell'art. 29 del Codice **che il Provvedimento appena citato indica come riferimento per la selezione degli Amministratori di sistema e assimilati: "**Se designato, il responsabile è individuato tra soggetti che per esperienza**, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni** in materia di trattamento, ivi compreso il profilo relativo alla sicurezza."

Vista la designazione già effettuata della S.V. a **INCARICATO interno del trattamento;**

Premesso che ai sensi del D.Lgs . 196/2003 Titolare dei dati personali trattati da parte di questo istituto è l'Istituto stesso e il Legale Rappresentante pro-tempore ha nominato lo scrivente quale Responsabile del trattamento per le attività della segreteria (ivi compresa la rete di computer della segreteria stessa);

Il sottoscritto Responsabile intende dare applicazione al citato Provvedimento del Garante Privacy del 27 novembre 2008, ad integrazione della designazione ad Incaricato di trattamento già effettuata e che rimane valida

determina

di individuare nelle attività e funzioni a Lei assegnate un ruolo assimilabile a quello di Amministratore di Sistema informatico.

Il sottoscritto ha pertanto proceduto, ai sensi del citato Provvedimento e in base ai tassativi criteri previsti dall'art. 30 del Codice, ad una nuova, più approfondita valutazione sulle Sue caratteristiche di capacità,

esperienza, affidabilità , anche in relazione alla scrupolosa applicazione delle misure di sicurezza previste dal Codice. Tale valutazione si è conclusa positivamente. **Infatti avendo già svolto negli ultimi anni questo compito in questo Istituto, ci risulta che:**

- **Lei è sicuramente dotata di adeguata esperienza.**
- **mai si sono registrati episodi negativi, anzi ha dato ripetute prove di serietà, riservatezza, affidabilità, capacità professionale, scrupolo e massima correttezza nell'applicazione delle misure di sicurezza.**

Pertanto, il sottoscritto , nel senso e per i fini previsti dal citato Provvedimento, La designa quale "Amministratore di Sistema informatico" relativamente al trattamento di dati svolto nell'ambito della finalità esclusiva di gestione del backup della rete di computers della segreteria.

Ai sensi del citato Provvedimento i Suoi compiti sono qui esplicitati nel dettaglio:

eseguire secondo la programmazione stabilita il backup, con il seguente protocollo:

Effettuare due back-up dei dati:
- il primo direttamente sulle cartelle del server che viene poi replicato su una seconda macchina client in fase di back-up collocata in altra stanza;
- il secondo dell'intero contenuto del disco fisso viene effettuato su un HD rimovibile ogni qualvolta vengono installate patch di aggiornamento al sistema operativo o ai programmi installati.

Vengono, in questo modo, create due immagini alternate, tramite questo è possibile ripristinare il server in breve tempo (tale "immagine" viene protetta con password per aumentarne la sicurezza). Sullo stesso disco vengono nell'occasione salvati, inoltre tutti i dati aggiornati al momento disponibili.

La presente designazione è altresì accompagnata dalle seguenti disposizioni:

- **in questa sua funzione, che svolgerà in concorso con il Prof. Saverio Rosati, Lei è tenuta a limitare gli accessi al sistema e gli interventi a quanto strettamente pertinente alle sue funzioni e alle operazioni analiticamente descritte.**
- **Nella sua attività deve dare piena e rigorosa applicazione alle regole del Codice Privacy, in particolare alle misure di sicurezza, e ai provvedimenti di carattere generale del Garante.**

Nell'occasione si comunica che in applicazione delle prescrizioni contenute nel citato

Provvedimento del Garante Privacy:

- **L'Istituto provvederà alla registrazione continua degli eventi informatici che riguardano tutti i Suoi accessi logici nonché degli eventi di sistema e di applicazioni. Tali Registri eventi saranno conservati per almeno 6 mesi in modo inalterabile e che consenta la verifica dell'integrità.**
- **Almeno una volta all'anno la Sua attività sarà oggetto di verifica complessiva, utilizzando anche l'analisi a campione dei Registri Eventi**
- **Il suo nominativo sarà dal Titolare reso conoscibile ai Dipendenti, in quanto il sistema informatico di cui Lei si occupa tratta loro dati personali.**

Il Responsabile del Trattamento

Sig. Stefano Giorgini

3° Facsimile di Nomina di Amministratori di Sistema o assimilati

Protocollo n. 1883/C1 Ancona 30 marzo 2010

Sig.ra Loretta Lucconi.
C.F. LCCLTT58C48A271M
Via Ginelli 15
60131 ANCONA

Oggetto: **designazione di Amministratori di Sistema e Assimilati**

Visto il D.Lgs 196/2003 "Codice in materia di protezione dei dati personali", che d'ora in poi nel presente documento sarà richiamato semplicemente come "Codice";

Visti gli articoli 29 e 30 del Codice in materia di designazioni di Incaricati e Responsabili;

Visto l'art. 33 del Codice , che impone di adottare le misure di sicurezza disposte dal Codice stesso e almeno le misure minime individuate dall'allegato B del Codice stesso;

Visto il Provvedimento di carattere generale (di seguito chiamato semplicemente "Provvedimento") emesso dal Garante Privacy in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)"" (e sue successive integrazioni, modifiche e chiarificazioni);

Visto in particolare il comma 2 dell'art. 29 del Codice **che il Provvedimento appena citato indica come riferimento per la selezione degli Amministratori di sistema e assimilati: "**Se designato, il responsabile è individuato tra soggetti che per esperienza**, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni** in materia di trattamento, ivi compreso il profilo relativo alla sicurezza."

Vista la designazione già effettuata della S.V. a **INCARICATO INTERNO del trattamento;**

Premesso che ai sensi del D.Lgs . 196/2003 Titolare dei dati personali trattati da parte di questo istituto è l'Istituto stesso e il Legale Rappresentante pro-tempore ha nominato lo scrivente quale Responsabile del trattamento per le attività della segreteria (ivi compresa la rete di computer della segreteria stessa);

Il sottoscritto Responsabile intende dare applicazione al citato Provvedimento del Garante Privacy del 27 novembre 2008, ad integrazione della designazione ad Incaricato di trattamento già effettuata e che rimane valida

determina

di individuare nelle attività e funzioni a Lei assegnate un ruolo assimilabile a quello di Amministratore di Sistema informatico:

Il sottoscritto ha pertanto proceduto, ai sensi del citato Provvedimento e in base ai tassativi criteri previsti dall'art. 30 del Codice, ad una nuova, più approfondita valutazione sulle Sue caratteristiche di capacità, esperienza, affidabilità , anche in relazione alla scrupolosa applicazione delle misure di sicurezza previste dal Codice. Tale valutazione si è conclusa positivamente. **Infatti avendo già SVOLTO questo compito per anni in questo Istituto ed essendo quindi ben conosciuta, ci risulta che:**

- **Lei è sicuramente dotato di adeguata esperienza.**
- **mai si sono registrati episodi negativi, anzi ha dato ripetute prove di serietà, riservatezza, affidabilità, capacità professionale, scrupolo e massima correttezza nell'applicazione delle misure di sicurezza.**

Pertanto, il sottoscritto , nel senso e per i fini previsti dal citato Provvedimento, La designa quale "Amministratore di Sistema informatico" relativamente al trattamento di dati svolto nell'ambito della finalità esclusiva di esecuzione della funzione di "Custode delle password" della rete di computers della segreteria.

Ai sensi del citato Provvedimento i Suoi compiti sono qui esplicitati nel dettaglio:

- **custodire in modo sicuro le password, subordinando l'eventuale presa di visione della password contenuta nelle buste alle circostanze previste dal Codice e seguendo le procedure previste (verbalizzazione con testimone)**

La presente designazione è altresì accompagnata dalle seguenti disposizioni:

- **in questa sua funzione, Lei è tenuta** a non effettuare accessi al sistema**, in quanto non necessari, salvo nei casi e secondo e le procedure previste.**
- **Nella sua attività deve dare piena e rigorosa applicazione alle regole del Codice Privacy, in particolare alle misure di sicurezza, e ai provvedimenti di carattere generale del Garante.**

Nell'occasione si comunica che in applicazione delle prescrizioni contenute nel citato Provvedimento del Garante Privacy:

- **L'Istituto provvederà alla registrazione continua degli eventi informatici che riguardano tutti i Suoi accessi logici nonché degli eventi di sistema e di applicazioni. Tali Registri eventi saranno conservati per almeno 6 mesi in modo inalterabile e che consenta la verifica dell'integrità.**
- **Almeno una volta all'anno la Sua attività sarà oggetto di verifica complessiva, utilizzando anche l'analisi a campione dei Registri Eventi**
- **Il suo nominativo sarà dal Titolare reso conoscibile ai Dipendenti, in quanto il sistema informatico di cui Lei si occupa tratta loro dati personali.**

Il Responsabile del Trattamento

Sig Stefano Giorgini.

Protocollo n. 1884/C1 Ancona, 30 marzo 2010

Sig. Filippo Rosignoli
C.F. RSGFPP66A21A271W
Via LAMBRO 11
60020 ANCONA

Oggetto: **designazione di Amministratori di Sistema e Assimilati**

Visto il D.Lgs 196/2003 "Codice in materia di protezione dei dati personali", che d'ora in poi nel presente documento sarà richiamato semplicemente come "Codice";

Visti gli articoli 29 e 30 del Codice in materia di designazioni di Incaricati e Responsabili;

Visto l'art. 33 del Codice , che impone di adottare le misure di sicurezza disposte dal Codice stesso e almeno le misure minime individuate dall'allegato B del Codice stesso;

Visto il Provvedimento di carattere generale (di seguito chiamato semplicemente <Provvedimento>) emesso dal Garante Privacy in materia di <<Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)"> (e sue successive integrazioni, modifiche e chiarificazioni);

Visto in particolare il comma 2 dell'art. 29 del Codice **che il Provvedimento appena citato indica come riferimento per la selezione degli Amministratori di sistema e assimilati: "**Se designato, il responsabile è individuato tra soggetti che per esperienza**, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni** in materia di trattamento, ivi compreso il profilo relativo alla sicurezza."

Vista la designazione già effettuata della S.V. a **INCARICATO Esterno del trattamento;**

Premesso che ai sensi del D.Lgs . 196/2003 Titolare dei dati personali trattati da parte di questo istituto è l'Istituto stesso e il Legale Rappresentante pro-tempore ha nominato lo scrivente quale Responsabile del trattamento per le attività della segreteria (ivi compresa la rete di computer della segreteria stessa);

Il sottoscritto Responsabile intende dare applicazione al citato Provvedimento del Garante Privacy del 27 novembre 2008, ad integrazione della designazione ad Incaricato Esterno di trattamento già effettuata e che rimane valida

determina

di individuare nelle attività e funzioni a Lei assegnate un ruolo assimilabile a quello di

Amministratore di Sistema informatico:

Il sottoscritto ha pertanto proceduto, ai sensi del citato Provvedimento e in base ai tassativi criteri previsti dall'art. 30 del Codice, ad una nuova, più approfondita valutazione sulle Sue caratteristiche di capacità, esperienza, affidabilità , anche in relazione alla scrupolosa applicazione delle misure di sicurezza previste

dal Codice. Tale valutazione si è conclusa positivamente. **Infatti avendo già collaborato per anni con questo Istituto ed essendo quindi ben conosciuto, ci risulta che:**

- **Lei è sicuramente dotato di adeguata esperienza.**
- **mai si sono registrati episodi negativi, anzi ha dato ripetute prove di serietà, riservatezza, affidabilità, capacità professionale, scrupolo e massima correttezza nell'applicazione delle misure di sicurezza.**

Pertanto, il sottoscritto , nel senso e per i fini previsti dal citato Provvedimento, La designa quale "Amministratore di Sistema informatico" relativamente al trattamento di dati svolto nell'ambito della finalità esclusiva di gestione/manutenzione del software dei computer e della rete di computer della segreteria.

Ai sensi del citato Provvedimento i Suoi compiti sono qui esplicitati nel dettaglio:

A) gestione e manutenzione della rete informatica
B) caricamento, gestione e manutenzione del software nei computers della rete. compresi antivirus e firewall; risoluzione di eventuali malfunzionamenti riscontrati

La presente designazione è altresì accompagnata dalle seguenti disposizioni:

1) **Lei è tenuto a limitare gli accessi al sistema e gli interventi a quanto strettamente pertinente alle sue funzioni e alle operazioni analiticamente descritte.**
2) **Nella sua attività deve dare piena e rigorosa applicazione alle regole del Codice Privacy, in particolare alle misure di sicurezza, e ai provvedimenti di carattere generale del Garante.**

Nell'occasione si comunica che in applicazione delle prescrizioni contenute nel citato Provvedimento del Garante Privacy:

- **L'Istituto provvederà alla registrazione continua degli eventi informatici che riguardano tutti i Suoi accessi logici nonché degli eventi di sistema e di applicazioni. Tali Registri eventi saranno conservati per almeno 6 mesi in modo inalterabile e che consenta la verifica dell'integrità.**
- **Almeno una volta all'anno la Sua attività sarà oggetto di verifica complessiva, utilizzando anche l'analisi a campione dei Registri Eventi**
- **Il suo nominativo sarà dal Titolare reso conoscibile ai Dipendenti, in quanto il sistema informatico di cui Lei si occupa tratta loro dati personali.**

Il Responsabile del Trattamento

Sig. ……..

ALLEGATO 14 - ELENCO DEGLI AMMINISTRATORI DI SISTEMA ED ASSIMILATI (documento interno)

[punto 2-c 1° paragrafo delle prescrizioni del Provvedimento]

Premessa:

Riportiamo qui di seguito, come allegato, l' ELENCO degli Amministratori di Sistema e Assimilati, in quanto esso integra il presente Documento Programmatico sulla Sicurezza e in particolare l'analisi delle misure di sicurezza adottate. Inoltre, trattandosi di attività obbligatoria da aggiornare ad ogni modifica e da mantenere in evidenza a disposizione in caso di accessi ispettivi , risulta molto pratico agganciarlo DPS come suo allegato e operare una verifica dell'aggiornamento in occasione della scadenza annuale al 31 marzo, fermo restando l'impegno di aggiornarlo immediatamente nel caso intervengano delle modifiche in qualsiasi momento dell'anno.

ELENCO DEGLI AMMINISTRATORI DI SISTEMA ED ASSIMILATI (documento interno)

[punto 2-c 1° paragrafo delle prescrizioni del Provvedimento]

In attuazione del provvedimento di carattere generale emesso dal Garante Privacy in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)" e successive modifiche e integrazioni,

e in particolare in attuazione del punto 2c – 1° paragrafo di tale provvedimento, che prevede l'obbligo che gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite,

1) , Addetto alla manutenzione e gestione del software, alla gestione delle credenziali di accesso al sistema, ai profili di autorizzazione degli utenti del sistema, all'organizzazione del backup periodico dei dati.

2) Sig.ra Loretta Lucconi, nata il 08.03.1958 Ancona., Dipendente inquadrato come assistente amministrativo , Addetto al backup periodico dei dati (in concorso con il Prof. Saverio Rosati)

3) Sig.ra Loretta Lucconi, nata il 08.03.1958, Dipendente inquadrato come assistente amministrativo , Addetto alla funzione di <Custode delle password>

4) Sig. Filippo Rosignoli nato 21.01.1966 Ancona (incaricato esterno) addetto alla manutenzione e gestione del software.

Naturalmente il presente e documento interno sarà aggiornato ad ogni cambiamento.

Data 30 marzo 2011

Firma del Titolare

ALLEGATO 15 - VERIFICA ANNUALE DELL'OPERATO DEGLI AMMINISTRATORI DI SISTEMA E ASSIMILATI

Premessa:

Riportiamo qui di seguito, come allegato, la VERIFICA ANNUALE dell'operato degli Amministratori di Sistema e Assimilati, in quanto essa integra il presente Documento Programmatico sulla Sicurezza e in particolare l'analisi delle misure di sicurezza adottate. **Inoltre, trattandosi di attività obbligatoria con cadenza almeno annuale, risulta molto pratico agganciarla alla scadenza del DPS annuale, in modo da non dimenticare l'adempimento e anzi eseguirlo in modo contestuale con l'intera attività di revisione del sistema privacy dell'Istituto.**

FACSIMILE VERIFICA ANNUALE

Contenuti della verifica, ricavabili dalla normativa:

Provvedimento: punti 4.4 e 2.e Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Provvedimento: punti 4.1 e 2.a Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

Provvedimento: punti 4.5 ed f Registrazione degli accessi

*Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;*

Art. 29 Codice Privacy: Responsabile del trattamento

2. Se designato, il responsabile è individuato tra soggetti che per ***esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza****.*

Da tali indicazioni normative si ricava la seguente griglia di valutazione annuale:

1) La verifica deve essere piuttosto **un'attività di verifica** da parte dei titolari del trattamento o dei responsabili.

2) Per ogni AdS o Assimilato va controllato **se la sua condotta <u>negli ultimi 12 mesi</u>** è stata **rispondente:**

- alle misure organizzative,
- alle misure tecniche
- alle misure di sicurezza

riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

3) Per ogni AdS o Assimilato va controllato se **la sua condotta <u>negli ultimi 12 mesi</u>** ha confermato i requisiti di:

- esperienza,
- capacità
- affidabilità

che erano stati alla base della sua nomina e

- ha fornito idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza

4) Per ogni AdS o Assimilato va controllato **<u>almeno a campione</u> se nell'ultimo periodo ha effettuato accessi logici <u>anomali , strani o comunque ingiustificati</u> rispetto alle funzioni assegnate** e alle regole di sicurezza stabilite (valutando la congruità della frequenza, degli orari, dei computer utilizzati, del software o delle base-dati utilizzati, ecc.). Per questa valutazione va utilizzata **la registrazione degli accessi logici** (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema, comprendendo tali registrazioni i riferimenti temporali e la descrizione dell'evento che le ha generate. Naturalmente le registrazioni utilizzate devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate.