ISTITUTO COMPRENSIVO STATALE
SCUOLA INFANZIA – PRIMARIA – SECONDARIA DI I GRADO
" Rita Levi Montalcini "
Via G. Bocchini, 37 – 82018 San Giorgio del Sannio(BN)
Segreteria: 0824.49249 Dirigente:0824.49140

REGOLAMENTO PER LA PROTEZIONE DEI DATI

a.s. 2013-2014

Premessa

Lo scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dall' **Istituto Comprensivo Statale "Rita Levi Montalcini" con sede in San Giorgio del Sannio(BN) alla via G. Bocchini, 37,** il cui legale rappresentante p.t. è il Dirigente Scolastico **Dott.ssa Gabriella Cirocco.**

Nel seguito del documento tale Istituto Scolastico sarà indicato come Titolare ovvero come il soggetto cui competono le decisioni in ordine a: finalità, modalità del trattamento di dati personali, strumenti utilizzati, ivi compreso il profilo della sicurezza.

Nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali mediante:
   - la individuazione dei tipi di dati personali trattati;
   - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
   - la elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. l'analisi dei rischi che incombono sui dati;
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati;
5. i criteri e le modalità di ripristino dei dati in seguito a distruzione o danneggiamento;
6. previsione di interventi formativi degli incaricati del trattamento;
7. i criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno;
8. le procedure da seguire per il controllo sullo stato della sicurezza;
9. le dichiarazioni d'impegno e firma.

Allegati

All. 1	Elenco trattamenti
All. 2	Descrizione Aree, locali e strumenti
All. 3	Lista Incaricati
All. 4	Procedure di protezione dati personali - Mansionario
All. 5	Elenco Amministratori di Sistema ed Assimilati

1. L'elenco dei trattamenti dei dati personali

Al fine di elaborare l'elenco dei trattamenti dei dati posti in essere dal Titolare, si è proceduto come segue:

- sono stati individuati i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili), i soggetti cui essi si riferiscono (alunni, personale dipendente, collaboratori, fornitori, Organi Collegiali, Consulenti,…..) e l'identificazione delle funzioni interne che, a vario titolo, sono coinvolte dalla loro gestione;
- sono state descritte le aree, i locali e gli strumenti con i quali si effettuano i trattamenti;
- è stata elaborata la mappa dei trattamenti effettuati, ottenuta incrociando le coordinate informative dei due punti precedenti.

1.1. Tipologie di dati trattati

I dati oggetto di trattamento da parte del Titolare si individuano come segue:

Elenco dati oggetto di trattamento

Oggetto del trattamento	***Codifica Gruppo Trattamenti***
Alunni/ Famiglie	A
Personale dipendente	B
Gestione finanziaria	C
Gestione Istituzionale	D
Gestione Fornitori / Acquisti	E
Collaboratori scolastici	F
Organi collegiali	G
Consulenti / Collaboratori esterni	H
Sito WEB scolastico	I

Vengono inoltre individuate come Categorie Omogenee le Funzioni già esistenti all'interno dell'Istituzione Scolastica che per facilitare la schematizzazione saranno individuate come segue:

- DS Dirigente Scolastico (e Vicario)
- DOC Personale Docente
- DSGA Direttore Servizi Generali e Amministrativi
- AMM Assistenti Amministrativi
- CS Collaboratori Scolastici
- PA Personale Ausiliario

In relazione a ciascun gruppo sopra indicato e alle funzioni coinvolte, si sono individuati i seguenti trattamenti (analiticamente specificati nell'**allegato 1**):

Elenco dei trattamenti

A – Alunni

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Didattica e altre connesse	DS / DOC	S	C / WP	Possibile*
Integrative e complementari	DS / DOC/ DSGA / AMM	S	C / WP / Gest	Possibile*
Amministrative e altre connesse	DS / DSGA / AMM	S G	C / Gest	Possibile*
Supporto didattica	DS / DSGA / AMM	S	C / Gest	Possibile*
Organizzazione e operatività scolastica	DS / DSGA / AMM	S G	C / Gest	Possibile*
Infortuni / Assicurazioni / Prevenzione	DS / DSGA / AMM	S G	C / Gest	Possibile**

B – Personale Dipendente

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Amministrative e altre connesse	DS / DSGA / AMM	S	C / Gest / WP	Possibile**
Retribuzioni e previdenza	DS / DSGA / AMM	S	C / Gest / WP	Possibile**
Organizzazione e operatività scolastica	DS / DSGA / AMM	S	C / Gest / WP	Possibile*
Infortuni / Assicurazioni / Prevenzione	DS / DSGA / AMM	S	C / Gest / WP	Possibile**
Organizzazione e operatività scolastica	DS / DSGA / AMM	S	C / Gest / WP	Possibile*

C – Gestione Finanziaria

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Bilancio, Cassa e Banche	DS / DSGA / AMM	S	C / Gest / WP	Possibile**

D – Gestione Istituzionale

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Protocollo e archivio in/out	DS / DSGA / AMM	S G	C / Gest / WP	Possibile
Protocollo riservato	DS	S G	C / Gest / WP	Possibile
AA.GG.	DS / DSGA / AMM	S G	C / Gest / WP	Possibile

E – Gestione Fornitori / Acquisti

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Gest. offerte e preventivi, Gest. contab., ademp. fiscali, inventario e connessi	DS / DSGA / AMM	S G	C / Gest / WP	Possibile*

F – Collaboratori Scolastici / Pers. Ausiliario

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Ricezione, trasporto, consegna documenti	CS / PA / AMM	S G	C	NO
Supporto per custodia e gest. archivi	CS / PA	S	C	NO

G – Organi Collegiali

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Consigli con inform. verbali e su atti	DS/DSGA/Comp.OO.CC.	S G	C / Gest / WP	Possibile*

H – Consulenti / Collaboratori esterni

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Amministrativa, retributiva, fiscale, previdenziale e connesse	DS / DSGA / AMM	S	C / Gest / WP	Possibile*

I – Gestione del Sito WEB

Attività trattate	*Funzioni coinvolte*	*Tipo dato*	*Strumento utilizzato*	*Comunicazione Telematica*
Informative e divulgative	DS / DSGA / DOC	C	SW	Possibile

Legenda:

Tipo dato	C	Comune
	S	Sensibile
	G	Giudiziario
Strumento	C	Cartaceo
	Gest	SW gestionale su Server/PC
	WP	SW elaborazione testi su PC
Comunicazione Telematica		tutti
	*	solo dati comuni
	**	anche dati sensibili

1.2. Caratteristiche di aree, locali e strumenti

L'Istituto gestisce più plessi scolastici dislocati nel territorio comunale di San Giorgio del Sannio(BN).

Il trattamento dei dati viene eseguito presso la sede sita in via G. Bocchini, 37 ove sono anche allocati gli uffici amministrativi.

1.2.1 Descrizione aree e locali e relativa mappa dei trattamenti

La situazione generale dei plessi presenta alcuni caratteri comuni: ordinaria sicurezza delle vie di accesso.

In tutti i plessi sono presenti dispositivi antincendio (estintori).

In nessun plesso è presente un sistema di allarme e/o di sorveglianza anti intrusione.

I locali ove avviene il trattamento dei dati per la didattica, da parte del personale docente, coincidono con quelli adibiti ad attività didattica distribuiti nei diversi plessi costituenti l'Istituzione scolastica.

Il trattamento dei dati da parte dei docenti, avviene di norma con mezzi manuali su supporti cartacei (registri personali e di classe, elaborati, ..) contenenti documentazione didattica.

Le chiavi di accesso ai locali dove sono trattati i dati personali sono affidate ai Collaboratori Scolastici in servizio e custodite in appositi armadietti dotati di serratura.

La descrizione dettagliata dei locali è riportata nell'**allegato 2**.

1.2.2 Strumenti e relativa mappa dei trattamenti

Il trattamento dei dati personali avviene con i seguenti strumenti:

1.2.2.1 Schedari ed altri supporti cartacei

Nella seguente tabella sono riportati i legami tra i trattamenti prima individuati e i luoghi fisici (sede e locali) ove essi vengono eseguiti con l'utilizzo di supporti cartacei.

I documenti di natura cartacea vengono ordinatamente raccolti in schedari o nella pratica cui si riferiscono per essere archiviati, a ciclo lavorativo concluso.

Elenco dei dati trattati e luoghi fisici (locali) del trattamento con supporti cartacei

	Id. *Trattam.to*	*Tipologia dei dati*			*Stanza* *Trattamento*	*Archivio* *Cartaceo*	
		Com	*S*	*G*		corrente	storico
Alunni (Uffici)	A	X	X	X	Segreteria e D.S.	X	X
Alunni (Docenti)	A	X	X		Aule e Sala Doc.	X	X
Pers.le Dipendente	B	X	X		Segreteria e D.S.	X	X
Gest. Finanziaria	C	X	X		Segreteria e D.S.	X	X
Gest. Istituzionale	D	X	X	X	Segreteria e D.S.	X	X
Gest. Fornitori	E	X	X	X	Segreteria e D.S.	X	X
Collab. Scolastici	F	X	X	X	tutte	X	X
Organi Collegiali	G	X	X	X	Sala riunioni e D.S.	X	X
Consulenti esterni	H	X	X		Segreteria e D.S.	X	X
WEB	I	X			D.S.		

In allegato 2 – si riporta:

-il prospetto del censimento degli schedari fisici rilevati (armadio, cassettiera, cassaforte, …) e utilizzati per l'archiviazione di supporti cartacei, il luogo fisico di ubicazione e i relativi dati oggetto di trattamento in essi contenuti;

-il contenuto fisico delle pratiche presenti per ciascuno schedario fisico.

1.2.2.2 Elaboratori

Sono stati censiti tutti gli elaboratori presenti presso la struttura scolastica, suddivisi in relazione al loro utilizzo:

Elaboratori non in rete

Per elaboratori non in rete si intendono quelli non accessibili da altri elaboratori e, più in generale, da altri strumenti elettronici.

Elaboratori in rete

Per elaboratori in rete privata si intendono quelli accessibili, da altri elaboratori o più in generale da altri strumenti elettronici, solo attraverso reti proprietarie, sulle quali possono viaggiare unicamente i dati del titolare del sistema.

Elaboratori in rete pubblica

Per elaboratori in rete pubblica si intendono quelli che utilizzano, anche solo per alcuni tratti, reti di telecomunicazione disponibili al pubblico, ivi inclusa la rete Internet.

Elenco dei trattamenti con strumenti elettronici, DB e ubicazione fisica dei dati

Trattamento	Id. Tratt.to	Banca Dati	Ubicazione DB	Dispositivo di accesso	Rete / Internet
Alunni	A	AXSIOS di SISSI	Server	PC	LAN / SI
Personale Dipendente	B	AXSIOS di SISSI	Server	PC	LAN / SI
Gestione Finanziaria	C	AXSIOS di SISSI	Server	PC	LAN / SI
Gestione Istituzionale	D	NO	PC	PC	LAN / SI
Gestione Fornitori	E	AXSIOS di SISSI	Server	PC	LAN / SI
Collaboratori Scolastici	F	NO	NO	PC	NO
Organi Collegiali	G	NO	PC	PC	NO
Consulenti / Collab. esterni	H	NO	NO	NO	NO
Sito Web	I		Provider	PC	Internet

2. Compiti e responsabilità

Il D.Lgs.vo 196/03 sulla protezione dei dati personali individua all'art. 4 i seguenti soggetti coinvolti nel trattamento dei dati personali:

1) il **Titolare**, cioè la persona fisica o giuridica che ha la responsabilità finale ed assume le decisioni fondamentali riferite al trattamento dei dati personali;

2) il **Responsabile**, è la persona dotata di particolari caratteristiche di natura morale e di competenza tecnica, preposta dal Titolare al trattamento dei dati personali "ivi compreso il profilo della sicurezza";

3) l'**Incaricato** è la persona fisica che materialmente provvede al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile laddove nominato;

4) l'**Interessato**, soggetto cui i dati oggetto di trattamento si riferiscono.

Nella fattispecie in esame, il **Titolare** dei dati personali trattati da parte di questo istituto è l'Istituto stesso (art. 28 D.Lgs.vo 196/03), di cui **la Dott.ssa Gabriella Cirocco** è il Legale Rappresentante p.t.

Per il trattamento dei dati personali il Titolare, dopo aver definito la struttura organizzativa e funzionale, ha individuato attraverso nomina diretta riportata in allegato al presente documento, attribuendogli incarichi di ordine organizzativo e direttivo nonché di garanzia del soddisfacimento dei diritti esercitabili dagli stessi interessati, il **Responsabile** nella persona del **D.S.G.A. Aurelia Cerulo.**

In **allegato 3** sono riportati nominalmente i **Responsabili** e gli **Incaricati** suddivisi per categorie funzionali omogenee.

Il trattamento dei dati personali può essere effettuato solo da soggetti che hanno ricevuto un formale incarico, mediante preposizione di ogni soggetto ad una unità in cui risulta articolata l'istituzione scolastica, per la quale sia stato individuato per iscritto: l'ambito del trattamento consentito agli addetti componenti l'unità stessa, categorie dei dati cui può avere accesso, tipologia di trattamento e vincoli specifici applicabili alle vari tipologie di dati, istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati sono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, arrivando a distinguere quelli sensibili e giudiziari, per garantire maggiore sicurezza rispetto a quanto previsto per il trattamento dei dati di natura comune;
- modalità di reperimento dei documenti contenenti dati personali, modalità da osservare per la custodia e l'archiviazione degli stessi al termine dello svolgimento dell'attività lavorativa che ha determinato l'utilizzo dei documenti;
- modalità per definire e custodire le parole chiave (password) necessarie per l'accesso agli strumenti elettronici ed ai dati ivi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi e le banche dati ivi contenuti;
- procedure per il backup dei dati;
- modalità di custodia ed utilizzo dei supporti rimovibili contenenti dati personali;
- dovere di aggiornarsi, attraverso il materiale e gli strumenti messi a disposizione dal Titolare, in merito alle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni che esterni all'Istituzione Scolastica del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le nomine sono effettuate anche per il personale supplente temporaneo, docente e ATA. Qualora l'Istituzione Scolastica si dovesse avvalere di soggetti o società o imprese non appartenenti all'organizzazione ma che debbano trattare dati personali da questa detenuti o avere accesso ad aree contenenti archivi di dati personali, per effettuare prestazioni di servizi a favore della stessa Istituzione, gli stessi dovranno essere identificati dal responsabile del trattamento e richiamati al dovere di rispettare i principi della privacy per il trattamento dei dati personali.

Le lettere di nomina dei responsabili e di designazione degli incaricati vengono raccolte ed archiviate in modo ordinato, in base alla funzione organizzativa cui i soggetti sono preposti: in tal modo il Titolare

dispone di un quadro completo di ***chi fa - cosa*** nell'ambito del trattamento dei dati personali, determinandosi un vero e proprio "**mansionario della privacy**".

Con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti o società o imprese esterne.

Nel seguente prospetto si riassumono i tratti salienti **dell'attuale mansionario della privacy**:

Strutture e trattamenti

Struttura	***Responsabile***	***Trattamenti operati***	***Compiti della struttura***
Dirigente Scolastico	Dirigente Scolastico	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate
Collaboratori D.S.	Dirigente Scolastico	Tutti (potenzialmente)	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Segreteria	D.S.G.A.	A, B, C, D, E, F	Gestione amministrativa di tutte le pratiche e supporto al D.S. e al Corpo Docente
Corpo Docente	Dirigente Scolastico	A, G	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,)
Collab. Scolastici e pers. Ausiliario	D.S.G.A.	F	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività
Membri di Organi Collegiali	Dirigente Scolastico	G	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché il CDI e la GE decisioni di tipo amministrativo, finanziario, regolamentare
Consulenti esterni	Dirigente Scolastico	A, B, C	Consulenza professionale al D.S. e DSGA per la gestione contabile e fiscale o al D.S e Docenti relativamente ad attività operative connesse alla didattica

3. Analisi dei rischi derivanti dal trattamento dei dati

La stima del rischio che grava sul trattamento di dati è il risultato della combinazione di due parti:

- una parte che identifica, valuta e contrasta i rischi propri indicati dalla legge, e cioè "il rischio 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"
- una parte che identifica, valuta e contrasta i rischi legati alle caratteristiche degli strumenti (manuali ed elettronici) che sono propri dell'attività in esame utilizzati per il trattamento dei dati.

Si evidenzia che un grado di rischio alto, o addirittura elevatissimo, è attribuito al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- quelli idonei a rivelare informazioni di carattere sensibile o giudiziario dei soggetti interessati, che sono accomunati dall'aspetto critico di avere un elevato grado di pericolosità per la privacy dei soggetti interessati;
- quelli che costituiscono un'importante risorsa didattica e tecnologica per il Titolare, in relazione ai danni che conseguirebbero da una eventuale perdita o trafugamento dei dati.

Di seguito sono evidenziati i fattori di rischio cui sono soggetti gli strumenti con cui l'Istituzione Scolastica procede al trattamento dei dati personali.

In generale tali fattori possono riassumersi nelle tipologie elencate agli artt. 31 e 32 del D.Lgs. 196/03 così individuate:

- distruzione o perdita, anche accidentale, dei dati;
- accesso non autorizzato ai dati;
- trattamento non consentito o non conforme alle finalità della raccolta;
- connessi con l'uso di reti di telecomunicazione disponibili al pubblico;
- connessi al reimpiego di supporti di memorizzazione;
- connessi alla conservazione della documentazione relativa al trattamento;
- connessi all'uso di archivi e contenitori con serrature.

Nella fattispecie le componenti di rischio di natura fisico, logico ed organizzativo possono essere:

1) legate ad atti di sabotaggio e ad errori umani del personale interno o di soggetti a contatto con esso;
2) rischio di guasti tecnici delle apparecchiature, in particolare degli strumenti elettronici (hardware e supporti vari), del software e rischio di penetrazione logica nelle reti di comunicazione;
3) rischio di area, che dipende dal luogo dove gli strumenti sono ubicati ed è legato sostanzialmente:
    - al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti);
    - alla possibilità che persone malintenzionate accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici);

Procedendo per ciascuno di essi alla valutazione del grado di impatto sulla sicurezza dei dati trattati unitamente alla gravità di esposizione al rischio, si arriva a definire un quadro di riferimento della classificazione primaria delle misure disponibili di controllo del rischio, da adottare anche in fase di aggiornamento del presente documento a seguito di una variazione dei rischi o della sopravvenuta inidoneità delle misure in essere.

Nella seguente tabella si evidenziano i fattori di rischio possibili, il loro impatto sulla sicurezza dei dati personali e le misure necessarie, adottate / da adottare, per garantire la loro sicurezza.

Analisi dei rischi

ANALISI DEI RISCHI E DELLE POTENZIALI MISURE DI CONTROLLO				
Rischio legato a:		Impatto sulla sicurezza dei dati		Possibili Misure di controllo
		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 sopra
	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 sopra eventuale creazione di profili di autorizzazione diversificati
	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.
Eventi relativi a guasti tecnici e penetrazione logica	azione di *virus* informatici o di codici maliziosi	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) 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 al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	Sabotaggio delle macchine, con eventuale perdita di dati; accesso abusivo se le credenziali fossero lasciate disponibili	Sabotaggio: media Altro: bassa	Solidità degli infissi dei locali chiusura a chiave quando non presidiati[eventuale installazione di allarme antifurto] disponibilità di estintori ad anidride carbonica per non danneggiare i computers 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, 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 eventuale allarme antincendio sensibilizzazione e formazione degli Incaricati e dei Collaboratori Scolastici Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti Uso di protezioni contro sovratensioni elettriche Verifica della logistica degli apparecchi e del loro corretto posizionamento Custodia dei dischi di back-up in armadio ignifugo, chiusi, collocato in locale diverso dai computer.
	guasto ai sistemi complementari (impianto elettrico)	Perdita di dati e blocco del sistema	media	Gruppo di continuità
	guasto ai sistemi complementari (climatizzazione)	Surriscaldamento dei computers e in particolare della scheda madre o altre componenti, con possibilità di guasto	bassa	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 Collab.Scolastici per il controllo Verifica della logistica degli apparecchi e del loro corretto posizionamento.

Nell'elaborare la tabella si è tenuto conto anche di alcuni fattori legati alla struttura scolastica, nei seguenti termini:

- il rischio d'area, legato alla eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento, è giudicato maggiore per gli ambienti connessi alle attività amministrativa rispetto a quelli per l'attività didattica, con conseguente aumento del rischio:
  - per gli archivi esistenti;

- per gli elaboratori in rete privata o pubblica, in relazione al fatto che il server è ubicato in tale area;

- il rischio di guasti tecnici delle apparecchiature interessa esclusivamente gli strumenti elettronici: in tale contesto, è giudicata più rischiosa la situazione degli strumenti non in rete che, essendo affidati a singoli che non sempre possiedono un bagaglio tecnico adeguato, presentano un rischio di rottura maggiore, rispetto agli impianti che vengono gestiti da persone con specifiche competenze, quale quello in rete;
- il rischio di penetrazione logica nelle reti di comunicazione interessa, in buona sostanza, i soli strumenti che sono tra loro collegati tramite una rete di comunicazione accessibile al pubblico;
- il rischio legato ad atti di sabotaggio o ad errori umani delle persone, presente in tutte le tipologie di strumenti utilizzati, è maggiore per quelli che sono in rete.

4. Misure organizzative per incrementare la sicurezza

Nel presente capitolo si approfondisce la problematica della sicurezza dal punto di vista organizzativo in quanto tale aspetto assume maggiore delicatezza in una organizzazione come quella della Scuola Pubblica dove i rischi legati alla sicurezza dei dati personali diventano di gran lunga maggiori rispetto ad altre Istituzioni a causa dell'altissima mobilità del personale, di carenze organizzative, incuria di addetti, ecc.

Per contrastare questi rischi, sono previsti i seguenti interventi di natura organizzativa:

- **Monitoraggi periodici da parte del Dirigente Scolastico;**
- **Riunioni con gli addetti per verificare collegialmente in modo costruttivo il progressivo affinamento nell'applicazione delle procedure previste e del D.Lgs 196/2003;**
- **Disponibilità per gli Incaricati di un certo numero di copie di un manuale di procedure da seguire per la sicurezza, come riportato al relativo capitolo del presente Manuale, in modo che tutti conoscano le regole proprie e quelle di altre categorie di Incaricati con cui collaborano;**
- **Istituzione delle seguenti figure, eseguita allo scopo di responsabilizzare altri soggetti e creare un monitoraggio amichevole, accettato e continuo**:

Il Custode delle parole chiave (password)

Il "Custode delle parole chiave" ovvero l'incaricato di custodire le "parole chiave" utilizzate da tutti gli utenti / incaricati del trattamento con strumenti informatici, è il DSGA.

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 username e password). Se l'utente dispone di più credenziali, dovrà ricevere altrettante buste chiuse.*
   Ogni busta 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) *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 seguenti caratteristiche: 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 eventuali problematiche riferibili alla gestione delle parole-chiave.*
8) *Gestire gli eventuali codici di cifratura (se 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.

Il Custode delle chiavi degli archivi ad accesso controllato

Pur se facoltativo, si ritiene opportuno prevedere la nomina del "Custode delle chiavi" degli archivi ad accesso controllato anche al fine di responsabilizzare maggiormente il personale Incaricato.

Il custode ha la responsabilità della gestione degli archivi ad accesso controllato ove per "controllato" si intende quell'archivio al quale possono accedere solamente le persone incaricate per iscritto dei trattamenti di dati personali conservati in tale archivio. Gli Incaricati dovranno pertanto richiedere, ogni volta, al "Custode" la chiave per accedervi e restituirla immediatamente dopo l'uso direttamente nelle mani dello stesso Custode. In caso di assenza, ci si potrà rivolgere al suo sostituto.

Per le emergenze, copia delle chiavi saranno a disposizione anche del Titolare o di altri da lui delegati che assicurino un uso esclusivo per le situazioni d'emergenza e della custodia con modalità di elevata sicurezza: le chiavi saranno collocate in busta chiusa controfirmata dal Custode, con l'apposizione di opportuna dicitura esterna e consegnate al Titolare / DSGA, i quali avranno cura di conservarle in luogo sicuro. Dopo un eventuale utilizzo in emergenza, le copie delle chiavi saranno rimesse in busta chiusa a cura del Custode con le stesse modalità di cui sopra. Il Custode terrà la chiave con sé o in luogo sicuro e la consegnerà temporaneamente ed esclusivamente alle persone autorizzate secondo le indicazioni ricevute dal Titolare / Responsabile del trattamento.

Le chiavi dovranno essere tenute dall'Incaricato per il tempo tecnico strettamente necessario all'accesso all'archivio.

Il Supervisore dei Backup e degli aggiornamenti del software"

Considerando la particolare complessità e delicatezza di tali operazioni, che coinvolgono pesantemente la sicurezza dei dati contenuti nel Sistema Informativo Scolastico, si ritiene necessario istituire tale figura al fine di garantire la gestione delle seguenti problematiche:

1) *Verificare che siano fedelmente applicati i punti dell'Allegato B sopra citati*
2) *Verificare che siano fedelmente eseguite alle scadenze previste i backup e le altre attività descritte nel Regolamento per la Protezione dei Dati, comprese le istruzioni relative al piano di Disaster Recovery e di Continuità Operativa.*
3) *Verificare che siano eseguiti alla giusta cadenza gli aggiornamenti dei sistemi operativi, dell'antivirus, del firewall, e del software in generale.*
4) *Gestire l'armadio di sicurezza contenente le copie di back up dei dati elettronici monitorandone la buona tenuta secondo le regole descritte*
5) *Verificare che i supporti originali del sistema operativo e dei programmi utilizzati siano mantenuti nel predetto armadio, in vista delle procedure di Disaster Recovery e di Continuità Operativa*
6) *Ricevere per la distruzione o formattazione i supporti utilizzati, in particolare se contenenti dati sensibili*
7) ***In generale, monitorare l'evoluzione della situazione e mensilmente riferirne al Titolare o al Responsabile**.*

Il Tecnico manutentore dell'hardware e del software

La designazione a Incaricato del Tecnico manutentore si rende obbligatoria in quanto quest'ultimo partecipa, per quanto indirettamente, alla gestione di dati (anche sensibili) e deve esserne ben consapevole soprattutto quando, come nel caso attuale dell'Istituto, tale tecnico è appartenente a una ditta esterna.

La nomina non è necessaria quando l'intervento avviene direttamente presso la scuola, sotto la vigilanza di un incaricato, con modalità che assolutamente escludono la possibilità di vedere o copiare dati personali.

5. Misure da adottare per garantire integrità e disponibilità dei dati

Sulla scorta dell'analisi dei rischi che incombono sui dati, vengono descritte nel presente paragrafo le misure in essere e da adottare a contrasto dei rischi individuati nell'analisi condotta, che riguardano sostanzialmente le seguenti aree:

- la protezione delle aree e dei locali nei quali si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede pertanto alla descrizione:

- delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati.

5.1 La protezione di aree e locali

Per quanto concerne il rischio d'area legato ad eventi di carattere distruttivo, i locali con le banche dati cui ha accesso il personale di segreteria e quelle di pertinenza del Dirigente Scolastico sono protetti da dispositivi antincendio (estintori) ai sensi del D.Lgs. 81/2008 e succ. mod. ed int. . **Le apparecchiature risultano sollevate dal pavimento con apposito supporto**. **Il sistema server, ove è fisicamente allocato il data base delle applicazioni, é dotato di apposito gruppo di continuità (UPS)**.

Per quanto riguarda invece le misure atte ad impedire intrusioni dall'esterno, come si evince nella descrizione dei luoghi fisici effettuata in precedenza, i locali innanzi detti presentano una situazione generale di sufficiente sicurezza relativamente a possibili intrusioni dall'esterno che avvengano fuori dall'orario di lavoro, quando i locali non sono presidiati.

Non risulta installato alcun sistema antifurto.

5.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, etc.), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi al responsabile del trattamento o direttamente al titolare.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire,

durante l'intero ciclo di svolgimento delle operazioni di trattamento, per poi restituirli all'archivio al termine di tale ciclo.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione.

A tale fine, agli incaricati vengono messi a disposizione:

- cassetti chiudibili a chiave in modo valido;
- armadi chiudibili a chiave;
- cassaforte ad accesso controllato;

nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'incaricato dovrà invece riporre in archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Particolari cautele vengono previste per il trasporto di documenti, atti e supporti contenenti dati sensibili all'esterno dei locali riservati al loro trattamento: per questi casi, è stato prescritto che il trasporto debba avvenire in buste e/o contenitori debitamente sigillati.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse tipologie di dati trattati.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa deve avvenire in luoghi, armadi, casseforti, o dispositivi equipollenti, che possono essere chiusi in modo efficace e sicuro.

Gli archivi contenenti dati sensibili o giudiziari sono controllati mediante l'adozione dei seguenti accorgimenti:

- al personale che utilizza una scrivania prospiciente all'archivio fisico viene dato l'incarico di vigilare sullo stesso, avendo ricevuto precise istruzioni in merito all'obbligo del presidio continuo da parte di almeno un Incaricato durante tutto l'orario di apertura dell'archivio al fine di garantire il controllo autorizzato degli accessi;
- il personale preventivamente autorizzato ad accedere agli archivi, deve richiedere la chiave di accesso all'Incaricato che ha il compito di custodirla.

Si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura mediante l'adozione dei seguenti accorgimenti:

- la chiave dell'archivio è affidata, dopo l'orario di chiusura, al titolare o al responsabile del trattamento, o in alternativa ad uno o più soggetti incaricati per iscritto, i quali provvedono ad annotare in un apposito registro i nominativi di coloro che hanno richiesto di accedere all'archivio fuori dall'orario di lavoro.

Essendo le dotazioni degli uffici adeguate, gli impianti e le attrezzature di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari, appaiono soddisfacenti al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti.

Nei locali accessibili al pubblico è prevista l'affissione di un cartello recante la fascia oraria nella quale é consentito l'accesso.

5.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici sono previste le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità dell'Incaricato affinché a ciascuno strumento elettronico possa accedere solo chi è autorizzato;
- realizzazione e gestione di un sistema di autorizzazione che ha il fine di consentire a ciascun Incaricato solo il trattamento di quelle tipologie di dati alle quali è autorizzato e limitare i trattamenti effettuabili a quelli strettamente necessari per lo svolgimento delle proprie mansioni;
- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus);
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (hard disk esterni, CD, etc.), nei quali siano contenuti dati personali.

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'istituzione scolastica, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali;
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente con strumenti elettronici non contenenti dati personali, o contenenti solo dati personali destinati alla diffusione.

Per tutti gli altri casi, è prevista una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato le credenziali vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la

medesima credenziale. Tale regola è operativa ed applicata da tutti gli Incaricati operanti all'interno della rete amministrativa e della rete didattica. La rete privata del laboratorio informatico presenta alcune limitazioni sull'utilizzo totale delle politiche innanzi indicate; considerato, però, l'utilizzo a fini di formazione che ne viene fatto, tale limitazione tecnica non crea particolari rischi legati alla sicurezza dei dati.

- nei casi in cui una componente della credenziale di autenticazione è costituita dal codice per l'identificazione (username), attribuito all'incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi. Tale regola diventa ancora più stringente per la particolare situazione di forte mobilità di personale che caratterizza le Istituzioni Scolastiche pubbliche italiane.

▪ **è invece ammesso, qualora sia necessario o comunque opportuno dal D.S., che ad una persona venga assegnata più di una credenziale di autenticazione.**

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento;
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi da ritenersi sporadico.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- dovere di custodire i dispositivi, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici;
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza;
- dovere di elaborare in modo appropriato la password e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username) attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema;
  - successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia;
- buona norma è che alcuni caratteri che costituiscono la password, da un quarto alla metà, siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare).

Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata;
- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, si osserva che:

- risulta impostato un sistema di autorizzazione, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative. L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.

Il profilo di autorizzazione non viene in genere studiato per ogni singolo incaricato, ma è generalmente impostato per classi omogenee di incaricati (ad es. attribuendo un determinato profilo di autorizzazione a tutti i collaboratori scolastici dell'area didattica, ed attribuendone un altro a coloro che lavorano nell'area amministrativa). E' possibile che a incaricati della stessa area possono però essere attribuite permissioni diversificate (ad es. permettere ad un Incaricato di poter effettuare qualsiasi tipo di transazione applicativa all'interno dell'area autorizzata e ad un altro Incaricato permettere l'accesso alle funzioni in sola lettura senza poter modificare i dati presenti). L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato o di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento che sono indispensabili per svolgere le mansioni assegnate.

Periodicamente, e comunque almeno annualmente (ovvero agli inizi dell'anno scolastico), viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto

riguarda l'ambito di trattamento consentito sia ai singoli incaricati che anche agli addetti alla manutenzione e gestione degli strumenti elettronici.

Per quanto riguarda la protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

-Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o ancora l'alterazione del suo funzionamento (comunemente conosciuti come virus).

A tale fine, la Scuola è dotata di un sistema antivirus di classe client / server che consente l'aggiornamento automatico giornaliero di tutte le stazioni PC collegate nella rete scolastica senza alcun intervento dell'utente. L'aggiornamento viene effettuato automaticamente dal server via rete esterna dal sito del produttore del software; all'accensione del PC client viene immediatamente controllato il livello di aggiornamento dell'antivirus e, se necessario, il server provvede ad aggiornalo.

Anche se l'aggiornamento antivirus è automatico, tutti gli incaricati sono stati comunque istruiti in merito al controllo periodico dell'allineamento della definizione dei virus alla data più recente (1-2 giorni) e, in generale, sulle norme di comportamento da tenere per minimizzare il rischio di essere contagiati.

-Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, ovvero la protezione da chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, che il nuovo codice privacy ha reso obbligatoria per i casi in cui si trattino dati sensibili o giudiziari.

A tale riguardo, la Scuola ottempererà nel più breve tempo possibile all'adozione di tutti gli strumenti di cui sopra. -Il terzo aspetto riguarda l'utilizzo di appositi programmi, la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi.

Per quanto concerne i supporti rimovibili, contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

La scuola ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e formattati nel momento in cui è cessato lo scopo per cui i dati vi sono stati memorizzati;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati (riformattando il supporto) e provvedendo alla distruzione fisica del supporto quando necessario per i fini in esame.

6. Criteri e modalità di ripristino dei dati

Piano di backup, disaster-recovery e di continuità e Misure per garantire integrità e disponibilità dei dati

6.1 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 benché con firma digitale servono:

- per produrre documenti cartacei conservati 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, MIUR, ecc.) cessando la necessità di conservarli in forma elettronica appena la comunicazione ha avuto effetto.
- per ricevere comunicazioni provenienti dall'esterno, delle quali di norma si fa una copia cartacea che viene conservata e che è l'unica ad avere valore legale. L'unica eccezione é l'allegato che non si ritiene utile stampare o 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.

6.1.1 Dati elettronici gestiti

Dati gestiti con software di produttività individuale

Per software di produttività individuale si intendono tutte quelle applicazioni, spesso contenute anche nelle utilities del Sistema Operativo, necessarie per scrivere testi, comporre tabelle e prospetti utili all'Incaricato per il disbrigo delle normali attività del posto di lavoro. Ciascun incaricato, in relazione alle proprie competenze, produce pertanto documenti che provvede a memorizzare in apposite cartelle di lavoro sul disco fisso del proprio PC. I documenti così prodotti, oltre ad essere stampati, possono essere riutilizzati utilmente dallo stesso Incaricato per produrre in tempi brevi ulteriori documenti aventi traccia simile incrementando produttività ed efficienza.

La gestione dei rischi legati alla perdita accidentale di questa tipologia di files è sicuramente la più semplice in quanto il documento è sempre presente nell'archivio cartaceo per i motivi stessi per il quale è stato prodotto (stampare). Il reperimento dei dati contenuti in un tale tipo di documento, quindi, assai raramente può costituire un problema.

Un esempio particolare di utilities è la posta elettronica, normalmente gestita con strumenti accorpati nel Sistema Operativo. I documenti ricevuti con tali sistemi vengono sempre stampati e, quando necessario protocollati. Stessa prassi viene utilizzata in trasmissione. Esiste, quindi, sempre una copia cartacea da cui prelevare i dati.

Dati gestiti con software "AXSIOS di SISSI"

Come è noto l'Istituto Scolastico dispone, del pacchetto applicativo cosiddetto "AXSIOS di SISSI". Per tale ragione, i dati elettronici la cui perdita creerebbe più problemi sono proprio quelli contenuti nel data base di AXSIOS di SISSI, in quanto rappresentano la quasi totalità delle informazioni necessarie per la gestione amministrativa e contabile della Scuola con le seguenti gestioni: Alunni, Personale, Libri di testo, Magazzino, Finanziaria, Gest. fiscale, Minute Spese, Stipendi ,..).

L'applicazione prevede l'utilizzo in modalità client / server che permette l'utilizzo del data base, presente solo sul sistema server, da più stazioni client (PC) distribuite nei vari uffici di segreteria, dotate del necessario software client di AXSIOS di SISSI. Orbene, possono verificarsi due possibilità di rischio:

- rischio di guasto del disco fisso del PC con perdita dell'applicazione;
- rischio di guasto del server con perdita del data base.

Nel primo caso il fermo riguarderà solo il posto di lavoro guasto. Sarà sufficiente, dopo la sostituzione / formattazione del disco, reinstallare il software di base e l'applicazione per continuare ad operare normalmente.

Nel secondo caso, poiché esiste un periodico backup del data base con cadenza settimanale, in caso di perdita totale di dati sarebbe possibile ricostruire in tempi relativamente brevi gli archivi aggiornati alla data di ultimo backup (max una settimana). La ricostruzione dei dati non salvati non dovrebbe peraltro costituire un lavoro troppo laborioso in quanto sarebbe quasi sempre possibile rintracciare nell'archivio cartaceo corrente i documenti necessari a ricostruire l'allineamento.

Dati gestiti con altri software forniti da Enti e Istituzioni

Presso gli uffici amministrativi dell'Istituto Scolastico sono utilizzati alcuni software applicativi messi a disposizione, nelle varie forme, da Istituzioni ed Enti Pubblici (MIUR, INPS, INPDAP, Tesoro/Finanze, …) al fine di facilitare la gestione di specifici adempimenti istituzionali con relativa ricezione / trasmissione, anche automatica, di dati prima gestiti solo su supporto cartaceo e trasmessi con altri mezzi meno efficienti (servizio postale, consegna diretta, …). Tali software, concessi formalmente dagli Enti competenti su appositi supporti auto-installanti, in qualche caso permettono anche la disponibilità locale dei dati inseriti e quindi dispongono di un'apposita procedura automatica di backup / recovery che viene utilizzata per la gestione in sicurezza. I rischi legati alla perdita totale di tali dati sono comunque di facile gestione in quanto, i dati sono in genere prodotti e stampati dagli Incaricati solo al momento dell'invio telematico dopodiché continuano ad essere disponibili e accessibili dall'Incaricato, generalmente via Web, presso l'Ente ricevente .

6.1.2 Conseguenze di un blocco

Blocco di breve durata di un Server o di un PC con archivi unici

Nel caso di blocco :

- di un solo computer non in rete, 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 che tale guasto riguardasse un PC di rete (client), se i dati e i programmi di lavorazione dei dati sono memorizzati nel server, passando a un altro terminale il problema può risolversi senza particolari inconvenienti.

Blocco di un computer in rete (client)

Il blocco di un singolo PC collegato in rete non costituisce, di per se, mai un problema anche quando il blocco si protrae per qualche giorno in quanto è sempre possibile far eseguire le stesse funzioni da un PC in rete alternativo. Fanno comunque eccezione i casi in cui il PC bloccato è predisposto per eseguire in via esclusiva alcune funzioni non replicabili da altra stazione. Il PC di Posta elettronica o l'unico PC abilitato ad accedere ad Internet possono, per esempio, creare qualche disfunzione in quanto molto raramente ci sono messaggi di posta elettronica che non possano attendere un giorno o comunicazioni che non possano essere procrastinate.

Va tuttavia riconosciuto che sarebbe buona norma avere, comunque, almeno un secondo PC in grado di poter compiere tali operazioni. Ciò significa che il computer previsto "di riserva":

- deve essere già collegato in rete e disporre del SW (Browser, SW di posta) disabilitato ma semplicemente e velocemente riconfigurabile;
- deve avere già caricati, ma disabilitati, eventuali programmi necessari per eseguire i collegamenti richiesti dalla funzione bloccante.

Blocco di media-lunga durata di un Server o PC con archivi unici

Nel caso di blocco prolungato :

a) di un solo computer non in rete, 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 può ritenere danno grave un fermo prolungato per circa 3-4 giorni, gravissimo dopo una settimana.

Come si può facilmente intuire, tali fermi possono portare ad un blocco parziale o totale di strutture organizzative o di attività scolastiche in corso creando disagi e improduttività gravi.

E' quindi necessario aver predisposto alcune importanti misure preventive che, in caso di eventi prevedibili, evitino fondamentalmente due possibili rischi gravi:

- la messa fuori uso completa e prolungata del "sistema informatico" o di parti vitali di esso;
- la perdita irreversibile degli archivi elettronici (data base).

Per tale ragione è normalmente sufficiente aver implementato delle procedure di "Disaster Recovery" ovvero di tutto ciò che metteremo in essere al fine di ripristinare nei tempi tecnici minimi possibili (2-3 giorni) il "normale" funzionamento del nostro sistema informativo conseguente ad un evento "disastroso" come sopra indicato. E' chiaro che ai fini del ripristino abbiamo dovuto

preventivamente aver reso disponibili tutte le "risorse" indispensabili a garantire il buon esito dell'operazione.

A fronte dei tempi di ripristino sopra indicati (2-3 giorni) che risultano operativamente accettabili, non sembra perciò indispensabile adottare un piano di continuità operativa orientato a ridurre ulteriormente i tempi preventivati in quanto la predisposizione di qualsiasi soluzione alternativa comporterebbe costi economici infinitamente superiori a quelli eventualmente causati dal blocco temporaneo.

6.2 Procedure di Backup

6.2.1 Analisi della situazione

Presso l'Istituto Scolastico, attualmente vengono eseguiti due tipi di back up:

- backup settimanale su disco fisso del server gestionale (disco separato) del data base di AXSIOS di SISSI;
- backup settimanale via rete degli archivi di lavoro dei PC client su disco fisso del server gestionale (disco separato);
- backup mensile di tutti gli archivi sopra indicati su CD o altri supporti
- backup su CD o altri supporti per i lavori del personale docente dopo ciascuna sessione di lavoro.

Ciascun utente dei PC in rete dispone sul disco fisso separato del server di una sua cartella ad uso esclusivo ove effettua i propri salvataggi settimanali. Un apposito incaricato provvede mensilmente ad effettuare i salvataggi complessivi su supporti di memorizzazione di massa.

Al momento ancora non è installato un software per la registrazione degli eventi ovvero file in cui viene memorizzato tutto ciò che si verifica nel computer, ad esempio l'accesso di un utente al computer o il verificarsi di un errore di un programma. La risoluzione di tale inadempienza sarà perseguita dall'istituzione scolastica nel più breve tempo possibile

6.2.2 Procedure di Backup in uso

1) In applicazione del principio che le copie di backup non devono essere esposte al rischio di essere rovinate da un evento che possa distruggere contemporaneamente anche gli elaboratori, custodiamo le copie di backup dei dati nonché i dischi originali dei programmi in una "cassaforte", resistente all'effrazione, collocata in stanza diversa da quella in cui è ubicato il server.

2) Per maggiore sicurezza, attualmente disponiamo di copie di backup sia settimanale che mensile. Sul disco fisso di salvataggio sono sempre presenti i salvataggi dell'ultima settimana e di quella precedente per evitare che un salvataggio andato male precluda la possibilità di effettuare il restore dei dati. Dopo ogni backup viene controllata la presenza fisica dei files previsti. Per i files salvati in formato leggibile, dopo il salvataggio si provvede a controllarne l'utilizzo in maniera statistica. Per i files provenienti da salvataggi effettuati tramite tools di backup automatico ne vengono solo

visualizzate le caratteristiche allo scopo di verificare che essi risultino almeno consistenti. Tutti i backup mensili verranno conservati per un periodo di 12 mesi dalla data di memorizzazione dopodiché verranno distrutti (rottura fisica).

3) Per evitare errori umani, procedurali, organizzativi o delle macchine, sono previsti periodici test di ripristino (da effettuare su un computer diverso da quello dove sono i dati correnti).

4) Si ritiene che la periodicità di un backup ogni 7 giorni sia al momento adeguata. Se e quando si arrivasse a veri e propri "documenti originali elettronici", ovvero quando si avrà la disponibilità di supporti di backup più veloci e maneggevoli, la periodicità potrebbe essere portata a 2 giorni o anche 1 giorno.

5) E' stato organizzato un censimento dei dati da salvare. Per quanto riguarda i files di testo o prodotti con altri programmi standard (esempio: WP, foglio elettronico,..), non contenenti dati sensibili, ogni utilizzatore ha avuto istruzioni 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 backup.

6) 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.

6.3 Procedure di "Disaster Recovery" e Piano di Continuità

Nell'ipotesi che un evento catastrofico possa distruggere o possa rendere indisponibili tutti gli elaboratori, rendendo così impossibile la continuazione dell'attività di gestione scolastica connessa all'utilizzo di tali elaboratori, sono state predisposte alcune misure interne finalizzate ad accorciare al minimo possibile i tempi di ripartenza del sistema complessivo nonché sono state predisposte le relative procedure cosiddette di "disaster recovery". E' stato fatto inoltre un accordo informale con una delle società che fornisce servizi di assistenza HW e SW all'Istituto affinché metta a disposizione tutta l'assistenza tecnica necessaria anche con la fornitura temporanea, in affitto, di apparecchiature o parte di esse necessarie alla ripartenza in esercizio utilizzando il SW in dotazione alla Scuola.

A tale scopo, nella cassaforte sono conservati i dischi di backup e di tutti i programmi necessari al funzionamento, in modo da poterli reinstallare.

6.3.1 Descrizione delle misure adottate e da adottare

Attualmente, al fine di garantire la massima sicurezza possibile degli archivi elettronici memorizzati, sul server gestionale sono già da tempo utilizzati strumenti di mirroring dei dati attraverso

un sistema RAID che garantisce la duplicazione contemporanea dei dati su due dischi fissi separati in modo da garantirne l'utilizzo anche in caso di distruzione fisica di uno dei due. Il dispositivo utilizzato consente anche la ricostruzione automatica degli archivi sul secondo disco, dopo la sua sostituzione.

A protezione da eventuali possibili rischi di mancanza o alterazioni dei valori dell'alimentazione elettrica, il server gestionale è dotato di Gruppo di continuità (UPS) di adeguata potenza in grado di effettuare lo shutdown automatico in caso di prolungata assenza di alimentazione.

I programmi originali del software in uso sono collocati nell'armadio di sicurezza di segreteria in modo che un evento disastroso abbia minime possibilità di distruggerli.

Si sta anche esaminando la possibilità economica di acquisire in futuro un computer (server) aggiuntivo compatibile con il software gestionale usato dalla segreteria e di collocarlo in altra area della scuola in modo da evitare che un medesimo evento non possa rendere indisponibili contemporaneamente il server operativo e questo computer di riserva. Per tale intervento si presume una spesa pari ad € 1'000,00. Nel frattempo il server aggiuntivo potrebbe essere proficuamente utilizzato come server della didattica. In tale computer sarebbero già pre-caricati i programmi e le directory utilizzate in segreteria, 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 circa 4 ore, il che costituirebbe, insieme alle misure già sopra indicate per i posti di lavoro e considerati i brevissimi tempo di ripristino previsti, una concreta realizzazione del piano di continuità operativa.

6.3.2 Controllo dei supporti dati e Prove di ripristino dei dati

Per evitare errori umani, procedurali, organizzativi o delle macchine, verranno periodicamente eseguiti:

- Prove di leggibilità dei supporti per dati;
- Test di ripristino (su un computer diversi da quelli ove sono memorizzati i dati correnti).

Tutti i supporti dati utilizzati ai fini di backup o restore sono normalmente conservati in cassaforte e gestiti dal DSGA. Data la breve cadenza temporale dei backup previsti per gli archivi (dati), non si prevedono particolari procedure per il controllo della leggibilità dei supporti. Sono previste comunque alcune cautele che vanno rispettate come:

- l'accurato controllo visivo esteriore del supporto, scartando tutti quelli che presentano difetti (supporto conservato fuori dalla custodia, piccole abrasioni del supporto, ecc..)
- la sostituzione obbligatoria del supporto normalmente utilizzato per i backup dopo un numero max di 20 operazioni di salvataggio;

Per quanto riguarda la leggibilità dei supporti backup di applicazioni o supporti originali di Sw applicativi in uso vengono eseguiti con cadenza almeno annuale test di installazione degli stessi su elaboratori diversi da quelli utilizzati in operativo.

Per ragioni di disponibilità di tempo, considerato che la scuola è oberata di lavoro nei mesi di settembre ed ottobre per l'inizio dell'anno scolastico e che tali mesi dovranno essere prioritariamente dedicati alla conclusione della formazione degli incaricati, soltanto nel mese di novembre 2013 è ipotizzabile di poter eseguire i test di ripristino.

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 possa essere già predisposto per l'eventuale sostituzione.

Alle prove sarà presente un tecnico informatico per dare utili consigli e sovrintendere all'esecuzione. Saranno presenti tutti gli Incaricati e gli ADS o assimilati che hanno avuto l'istruzione di realizzare il backup periodico, anche allo scopo di far comprenderne meglio le motivazioni e le corrette finalità delle operazioni in questione.

Tutti i supporti di dati non più utilizzati e/o utilizzabili dovranno essere distrutti (rottura fisica).

7 Interventi formativi e relativa pianificazione

In riferimento alle classi omogenee di funzioni applicative individuate:

1. **Titolare : Il Legale Rappresentante pro - tempore, cioè il Dirigente scolastico**
2. **Responsabile del trattamento: il DSGA per i trattamenti di Segreteria e Collaboratori**
3. **Incaricati Collaboratori del D.S.: Docenti delegati (in sostituzione del D.S.)**
4. **Incaricati Docenti e Assimilati**
5. **Incaricati Assistenti Amministrativi della Segreteria**
6. **Incaricati Operatori Scolastici e Personale ausiliario**
7. **Incaricati Membri degli Organi Collegiali (anche alunni e persone esterne alla scuola)**
8. **Tutti coloro che ricoprono e/o la carica di ADS o assimilati.**

Sono previsti interventi formativi sul trattamento, finalizzati ai seguenti aspetti:

- **profili della disciplina sulla protezione dei dati personali che appaiono più rilevanti per l'attività svolta, e delle conseguenti responsabilità che ne derivano;**
- **rischi che incombono sui dati;**
- **misure disponibili per prevenire eventi dannosi;**
- **modalità per aggiornarsi sulle misure di sicurezza adottate dal titolare.**

Tali interventi sono programmati in modo tale da avere luogo al verificarsi di una delle seguenti circostanze:

- **al momento dell'ingresso in servizio. All'inizio di ogni anno scolastico il Titolare ed il Responsabile del trattamento programmeranno attività formative per il personale che prende servizio presso l'Istituzione e che non è stata precedentemente sottoposta a formazione sui contenuti del codice della privacy e sui doveri da esso derivanti. Gli interventi formativi potranno essere realizzati anche in collaborazione con altre istituzioni scolastiche;**

- **in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;**
- **in relazione a novità che si dovessero presentare nelle norme di legge e/o in relazione all'evoluzione tecnica del settore, che implicano modifiche rilevanti nel trattamento di dati personali;**
- **in relazione a gravi non conformità rilevate in sede di verifica da parte del Titolare dell'efficacia delle misure di sicurezza di cui si tratta.**

Gli interventi formativi possono avvenire sia all'interno, a cura di soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

E' previsto la distribuzione di un opuscolo divulgativo ed esauriente che illustrerà quanto inerente la sicurezza dei dati.

Argomenti da approfondire con una certa urgenza , dedicando una o più sessioni a ciascuno di questi argomenti:

1) Classificazione dei dati
2) Regole conseguenti alla classificazione dei dati nel trattamento, nell'archiviazione cartacea, nella gestione al computer, nella comunicazione e nella diffusione
3) Informativa, in particolare per dati sensibili e giudiziari
4) Valutazione dei presupposti di legittimità dei trattamenti e in particolare della comunicazione e diffusione
5) Mansionario privacy, ruoli e regole delle varie funzioni
6) Misure di sicurezza organizzative/comportamentali, in particolare gestione delle credenziali, dei profili di autorizzazione, dei files separati. Gestione degli archivi ad accesso controllato e degli archivi in genere.
7) Gestione del backup, del ripristino dei dati, dei test di efficacia delle procedure; gestione dell'aggiornamento del software, cenni sulle tecniche di cifratura
8) Comportamenti per prevenire i virus, utilizzo del programma antivirus e del firewall. Gestione prudente della posta elettronica.

8. L'affidamento del trattamento di dati personali a esterni

Nel casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal D.Lgs. 196/2003, all'esterno della struttura del Titolare, dovranno adottarsi tutti i criteri atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime.

9. Controllo generale sullo stato della sicurezza

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile per la sicurezza e le persone da questo appositamente incaricate provvedono con frequenza mensile, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento;
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file dei software di sicurezza installati, dei sistemi operativi e delle applicazioni. Attraverso questa analisi, effettuata eventualmente con strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette;
- verificare l'integrità dei dati e delle loro copie di backup;
- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici non più riutilizzati vengano distrutti;
- verificare il livello di formazione degli incaricati;
- verificare tutto quanto inerente gli ADS.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi. Per tali attività il Titolare potrà avvalersi della consulenza di un tecnico esterno.

Dell'attività di verifica svolta viene redatto un verbale, che viene conservato dal Titolare.

10. Dichiarazioni d'impegno e firma del documento

L'originale del presente documento viene custodito presso la sede del Dirigente Scolastico per essere esibito in caso di controlli.

Su richiesta tale documento può essere reso disponibile per la libera visione:

• di ciascun incaricato e/o ADS del trattamento dei dati personali;

• dei soggetti esterni del trattamento dei dati personali;

• di chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un

trattamento congiunto di dati personali.

Al presente documento, sottoscritto dallo stesso Titolare Dott.ssa Gabriella Cirocco viene attribuita data certa mediante la registrazione con il timbro di protocollo e il relativo numero attribuito.

San Giorgio del Sannio(BN), gennaio 2014

f.to Il Titolare
Dirigente Scolastico
Dott.ssa Gabriella Cirocco

f.to Il Responsabile
D.S.G.A.
Aurelia Cerulo

ALLEGATO 1

Elenco dei trattamenti di dati personali

Elenco trattamenti

A - **Alunni / Famiglie**
Dati trattati da Docenti e Personale Amministrativo

B - **Personale dipendente**
Dati trattati da Personale Amministrativo

C – **Gestione Finanziaria**
Dati trattati da Personale Amministrativo

D – **Gestione Fornitori / Acquisti**
Dati trattati da Personale Amministrativo

E – **Gestione Istituzionale**

Dati trattati da Personale Amministrativo (archivio, protocollo, posta elettr., …..)

F – **Movimentazione documenti**
Dati trattati da Collaboratori Scolastici e Personale Ausiliario

G – **Organi Collegiali**
Dati trattati dagli Organi Collegiali

H – **Soggetti esterni**
Dati trattati a vario titolo da soggetti esterni (Collaboratori, Consulenti,.)

Matrice dei trattamenti:

TIPI DI DATI TRATTATI

Alunni/ Famiglie	X	X	X	X		X
Personale dipendente	X			X		X
Collaboratori scolastici	X			X		
Gestione finanziaria	X			X		X
Gestione Amministrativa	X			X		
Fornitori/Acquisti	X			X		
Organi collegiali	X			X		
Soggetti esterni	X		X	X	X	
Sito WEB scolastico	X	X				
UNITA'	**A**	**B**	**C**	**D**	**E**	**F**

La legenda delle unità è la seguente:

A – Dirigente Scolastico e Collaboratori del D.S.
B – Docenti – Supplenti docenti
C – Membri degli organi collegiali
D – Segreteria
E – Collaboratori scolastici
F – Soggetti e Società esterne

A - Alunni

I dati personali riguardanti gli alunni sono trattati:
- ai fini didattici (da Docenti e D.S.)
- ai fini gestionali (da D.S., DSGA e Personale Amministrativo)

A1- Dati trattati dai docenti

a) Dati personali comuni per qualsiasi attività didattica e organizzativa
b) Scelta di avvalersi dell'insegnamento della religione cattolica (dato sensibile)
c) Assenze per motivi di salute (dato particolare o sensibile) o familiari (dato particolare) con visione di certificati medici di avvenuta guarigione (dato particolare o sensibile); giustificazioni di assenze dovute a festività religiose di religioni non cattoliche (festività ebraiche, ecc.): dato sensibile in grado di rivelare la convinzione religiosa
d) Certificazioni mediche per esonero da educazione fisica con diagnosi (dato sensibile)
e) Comunicazioni scuola - famiglia (dati particolari)
f) Alunni portatori di handicap che incidono sulla didattica e documentazione per l'integrazione (dato sensibile)
g) Registri contenenti note disciplinari e provvedimenti di sospensione,ecc. (dato particolare)
h) Valutazioni intermedie e finali, votazioni, su profitto - grado di impegno - condotta, - profilo psico-attitudinale, ecc. di ogni alunno assegnato (dati particolari) su moduli e registri
i) Elaborati scritti riportanti in taluni rari casi informazioni delicate sulla sfera personale e familiare dell'alunno (dati particolari di grado elevato)
j) Informazioni su situazione di problemi di salute dell'alunno che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la vita dell'alunno (allergie, asma grave, diabete grave, epilessia, cardiopatie gravi, ecc.) o imbarazzanti (disturbi di continenza, ecc.), messe a disposizione dai genitori o dall'interessato. Se l'informazione è orale l'insegnante è tenuto al riserbo. Se esiste qualche comunicazione scritta, trattasi di dato sensibile.
k) Registri di classe, contenenti dati comuni e particolari, affidati all'insegnante di turno.
l) Registro del docente in cui sono annotati dati comuni e particolari. Il docente è responsabile della riservatezza del registro.
m) Registro dei verbali dei Consigli di classe: dati di tipo comune e particolare; è conservato a cura del Dirigente in armadio chiuso a chiave.
n) Registri e documenti in occasione di esami e concorsi
o) Elenchi di alunni, dipendenti e genitori per attività varie della scuola
p) Elenchi di alunni in caso di visite d'istruzione o viaggi (dato comune)
q) Partecipazione a commissioni scolastiche (dati personali)
r) Partecipazione alla gestione delle elezioni degli organi collegiali (dati comuni)
s) Partecipazione ad attività del sindacato interno con conoscenza (dati sensibili)
t) POF - Piano Offerta Formativa (dati neutri)
u) Orientamento scolastico in ingresso e in uscita (con profili psicologici - dato anche particolare o raramente sensibile)

Ogni docente, nel momento in cui è assegnato alla scuola diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita istruzione scritta.

A2 - Dati trattati da Assistenti Amministrativi e D.G.S.A.

1. Fascicolo personale (accompagna l'alunno in tutta la sua carriera) che conterrà tutti i documenti riferibili a lui individualmente, nonché le pagelle pregresse e l'allegato con la valutazione sull'insegnamento della religione. Al termine della carriera scolastica o in caso di ritiro viene conservato in un archivio storico. (dati comuni, particolari, raramente sensibili o giudiziari). Contiene anche la foto dell'alunno (tipo "fototessera")
2. Atti connessi alla pre-iscrizione, all'iscrizione iniziale e annuale
3. Documento di scelta da parte dell'alunno di avvalersi dell'insegnamento della religione cattolica (dato sensibile) ; Allegato della pagella con la valutazione dell'eventuale insegnamento della religione: (dato sensibile)
4. Tasse e contributi scolastici, richieste e di documentazioni per esoneri da tasse e contributi o per ottenere benefici economici (sussidi, borse di studio o libri scolastici): in taluni casi ci sono documenti con dati particolari (redditi , copia di dichiarazioni Irpef da cui si evincono redditi e patrimonio immobiliare e altre notizie particolari; nucleo familiare anche in seguito a divorzio, stato di genitore celibe/nubile, attestazione di assegni ricevuti dal coniuge divorziato o separato; in casi rarissimi ci dono dati giudiziari e dati sensibili)
5. Elenchi degli alunni e genitori per l'elezione Organi Collegiali
6. Documenti riferiti a vaccinazioni obbligatorie (dato particolare) o all'inosservanza dello stesso (dato sensibile)
7. Certificazioni di altri enti su stati e qualità (iscrizione, frequenza, profitto, esiti scolastici, carriera scolastica, ecc.)
8. Documenti che attestano la persona con la patria potestà per alunni minorenni in situazione particolare o in stato di affido ecc. (in taluni casi ci sono documenti con dati particolari riservatissimi (composizione del nucleo familiare anche in seguito a divorzio o separazione; sentenze di affido; in casi rarissimi sono dati giudiziari e dati sensibili)
9. Certificazioni e altri documenti sulla presenza di handicap che incidono sulla didattica (dato sensibile). Copie e risultati di test psicologici o psicoattitudinali (rarissimi, ma possono essere dato sensibile)
10. Certificazioni di altri enti su stati e qualità (iscrizione, frequenza, profitto, carriera scolastica, ecc.)
11. Redazione e trasmissione (anche per via telematica) ad altre scuole di foglio notizie alunni, con informazioni sulla carriera scolastica e i documenti in possesso della scuola (dati comuni, in qualche caso particolari)
12. Anagrafica dell'alunno con registrazione pagamento tasse, esiti finali dell'anno scolastico, nominativi genitori o esercenti patria potestà (tutti dati comuni o in rari casi particolari)
13. Assenze per motivi di salute (dato particolare o sensibile) o familiari (dato particolare) con visione di certificati medici di avvenuta guarigione (dato particolare o sensibile); giustificazioni di assenze dovute a festività religiose di religioni non cattoliche (dato sensibile)
14. Certificazioni mediche per esonero da educazione fisica (dato sensibile)
15. Note disciplinari e provvedimenti disciplinari gravi (dato particolare)
16. Valutazioni intermedie e finali, votazioni, profitto, impegno, condotta, profilo psicoattitudinale, ecc.(dati particolari)
17. Certificazioni mediche per infortuni a scuola per denuncia a Questura, Inail, assicurazione (dato sensibile)
18. Pagelle, diplomi, esiti e ammissioni agli esami, registro voti e assenze, registro esami di maturità e idoneità o integrativi (dati particolari); Diplomi e pagelle. Registri voti e assenze e registro esami maturità è eseguito in forma cartacea

19. Certificazioni della scuola o di altri enti su stati e qualità (iscrizione, frequenza, profitto, carriera scolastica, ecc.)
20. Lettere alla famiglia su profitto, mancanze disciplinari, comportamenti inadeguati, assenze ingiustificate e altro (in alcuni casi dati particolari)
21. Lettere o documenti provenienti dagli alunni o dalla famiglie che segnalino comportamenti inadeguati o censurabili da parte di docenti o del personale o di altri alunni, ivi comprese petizioni e richieste di ispezioni da parte delle Autorità scolastiche superiori: (in alcuni casi dati particolari)
22. Documenti o comunicazioni della famiglia su problemi di salute dell'alunno che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la vita dell'alunno (allergie gravi, asma grave, diabete grave, epilessia, cardiopatie gravi, ecc.) o imbarazzanti (disturbi di continenza, ecc.) o che necessitano assenze parziali per terapie: (dati sensibili).
23. 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
24. Orientamento scolastico in ingresso e in uscita (con profili psicologici il dato é particolare o raramente sensibile)
25. Prestiti della biblioteca (dati comuni)
26. Pratiche riferite a organizzazione di viaggi con agenzie: verifica dei requisiti di legge e della convenienza economica: (dati comuni e in qualche caso particolari). Pratiche di selezione degli autotrasportatori per trasporto di alunni: verifica dei requisiti di legge e della convenienza economica (dati comuni e in qualche caso particolari)
27. Attività extrascolastiche (nuoto o altro): verifica dei requisiti di legge e della convenienza economica (dati comuni e in qualche caso particolari)

Dati neutri

28. 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)
29. 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)
30. Iter per l'adozione dei testi scolastici (dati comuni o neutri)
31. Determinazione del calendario scolastico
32. POF (dati neutri)

Atti rari o straordinari

33. 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)

MODALITÀ DI RACCOLTA DEI DATI:

1) Gran parte dei dati provengono dall'interessato
2) Per chi è trasferito o comunque proviene da altra scuola, quest'ultima trasmette un foglio notizie e la parte rilevante del Fascicolo Personale (documenti anagrafici, documenti scolastici, eventuali certificati medici)
3) Alcuni dati provengono dalla visione del libretto personale dello studente o da comunicazioni scritte della famiglia o da comunicazioni verbali dello studente

MODALITÀ DI TRATTAMENTO:

1) La gestione del Fascicolo Personale è realizzata senza l'ausilio di strumenti elettronici.
2) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi o con apposito software.
3) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati.

B - Personale dipendente

Dati trattati da Assistenti Amministrativi e D.G.S.A.

1. Fascicolo personale che accompagnerà il dipendente in tutta la sua carriera presso l'Istituto (compreso il periodo di quiescenza) e che conterrà tutti i documenti riferibili a lui individualmente, nonché i documenti ricevuti da altre scuole o enti (dati particolari o anche sensibili). In caso di cessazione del rapporto o trasferimento il fascicolo viene conservato in un archivio storico. Tale fascicolo contiene potenzialmente tutti i documenti sopra elencati, tranne quelli sensibili o giudiziari o particolari archiviati a parte.
2. 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 (dati comuni o particolari)
3. Elenchi di alunni, dipendenti e genitori per attività varie della scuola
4. Presenze del personale non docente, tramite firma su registro collocato nella stanza della Segreteria Amministrativa (dato particolare) con trascrizione cartacea e redazione di un documento che riporta l'orario complessivo del dipendente nel mese
5. Certificati medici generici per assenze per malattia (dato sensibile)
6. Assenze per malattia (dato sensibile) e relativi atti concessivi (dato particolare o sensibile)
7. Richieste, certificazioni, dichiarazioni e concessioni di permessi per handicap di un familiare (dato sensibile) o relativi alla fruizione di permessi, riduzioni d'orario e simili per motivi di salute o per condizione di handicap o invalidità (dati sensibili), aspettativa per motivi di salute (dato sensibile), assenze retribuite al 100% perché connesse a ricoveri ospedalieri, gravi patologie o dovute a terapie invalidanti certificate (dato sensibile) e relativi atti concessivi (dato sensibile), permessi retribuiti o congedi per gravi e documentati motivi e per particolari patologie dei familiari e relativi atti concessivi (dato sensibile), permesso per particolari impegni (partecipazione a processi, visite o terapie mediche, impegni familiari, ecc.): dato particolare, raramente sensibile, permessi per assistenza ai figli : dato particolare
8. Richieste, certificazioni, dichiarazioni e concessioni relativi a stato di gravidanza e al rischio di aborto o interdizione o astensione o riduzione orario per allattamento (dati sensibili)
9. Gestione richieste e concessioni relativi part-time (dato particolare a bassa sensibilità)
10. Trasmissione di concessioni per alcuni di questi atti a Enti pubblici di controllo (Ragioneria dello Stato, ecc.)
11. Tutte le altre pratiche per permessi, assenze, congedi, aspettative, ecc., eseguita a volte su moduli cartacei e più spesso mediante programma di elaborazione testi. In quest'ultimo caso i documenti elettronici possono contenere dati sensibili o particolari
12. Pratiche relative all'organico, ai trasferimenti e alle utilizzazioni
13. Richieste, certificazioni, dichiarazioni e concessioni su particolari situazioni personali o familiari che danno diritto a punteggi o preferenze (dati particolari e a volte sensibili) o per utilizzo facilitazioni di graduatoria o di punteggio per trasferimento (dato particolare e a volte sensibile) Idem per Grandi invalidi di guerra (dato sensibile)
14. Contratto di assunzione (dati comuni)
15. Richieste, certificazioni, dichiarazioni e concessioni per immissione in ruolo, ricostruzione di carriera, ricongiungimenti di periodi assicurativi e riscatto di periodi a fini pensionistici (dati particolari)
16. Valutazioni del periodo di prova, note di merito o demerito, provvedimenti disciplinari (dati particolari)

17. Pratiche di cessazione o dispensa dal servizio: per inidoneità fisica (dato sensibile), per incapacità o persistente insufficiente rendimento (dato particolare). Destituzione per motivi disciplinari (dato particolare), per reati (dato giudiziario). Dispensa dal servizio per esito sfavorevole della prova (dato particolare)
18. Pratiche per la tutela dei dipendenti in particolari condizioni psicofisiche
19. Pratiche per riconoscimento di invalidità per causa di servizio (dato sensibile)
20. Trasmissione per via telematica al MIUR di dati comuni e particolari relativi all'assunzione in servizio
21. Richiesta del part - time
22. Domande, dichiarazioni, certificazioni, curriculum per inserimento in graduatorie di aspiranti a supplenze (dato particolare e sensibile quando è presente un fatto che può dar diritto a punteggi per ragioni di handicap o invalidità fisica), formazione, gestione e diffusione delle graduatorie (dato pubblico), depennamenti (dato comune). Spesso questa gestione implica comunicazioni, anche telematiche, da e ad altre scuole e al MIUR.
23. Pratiche relative alle domande di supplenza temporanea, all'inserimento in graduatorie (dati particolari o sensibili) e alla consultazione o diffusione di queste (dati pubblici)
24. Nomina e g
25. Gestione carriera del docente di religione (possibile dato sensibile)
26. Gestione nomine per commissari d'esami, anche mediante via telematica (dati comuni)
27. Domande di quiescenza (dato particolare) e relativa pratica (dato particolare)
28. Richieste e certificazioni di gravidanza per mantenimento del posto di persona non di ruolo i (dato sensibile) e relativi atti concessivi (dato sensibile)
29. Trattamento di certificati di buona condotta (dato particolare), certificati di sana e robusta costituzione (dato sensibile), dichiarazione sui carichi pendenti nel casellario giudiziario (dato giudiziario)
30. Gestione incentivi economici su fondo d'Istituto e in genere
31. Documentazione da trasmettere al CAF per il mod. 730, reddito annuo e patrimonio (dati particolari) e sul conferimento dell'X per mille a chiese od organizzazioni religiose (dato sensibile): ricevuta in busta chiusa per la trasmissione al CAF
32. Lavoratori a tempo determinato: gestione della retribuzione con documenti cartacei e programma informatico: calcolo stipendio, cedolino stipendio (dato particolare), prospetti di spesa, scheda fiscale interna (dato particolare), inserimento di assenze e scioperi che comportano riduzione di stipendio (dato parasensibile o sensibile), ritenute per delega sindacale (dato sensibile) e altre ritenute (dato particolare), gestione fiscale (in particolare, detrazioni: dato particolare) e gestione previdenziale (dato particolare). Gestione richieste e attribuzioni delle detrazioni fiscali anche per dipendenti a tempo indeterminato (dato particolare e in qualche caso sensibile).
33. Trattamenti di missione (dati comuni)
34. Gestione richieste, certificazioni, dichiarazioni e concessioni relativamente a benefici di natura economica, assegno per nucleo familiare (dati particolari o sensibili)
35. Gestione e trasmissione all'INPDAP per via cartacea del progetto di liquidazione TFR per ogni dipendente a tempo determinato.
36. Domande di prestiti, cessione del quinto ecc., motivate con ragioni personali o familiari (particolari o sensibili)
37. Denuncia infortuni (per via cartacea) (dato particolare o sensibile)
38. Gestione eventuali pignoramenti dello stipendio e di ritenute per eventuali danni erariali (dato particolare ad elevata sensibilità)
39. Trasmissione mensile per via telematica all'INPS dei DM10 (dato anonimo)
40. Trasmissione al Tesoro per via cartacea o telematica dei compensi accessori a fine del conguaglio fiscale.

41. In generale qualsiasi ulteriore pratica connessa alla gestione del dipendente dal punto di vista retributivo, fiscale, previdenziale e amministrativo.
42. Dichiarazione di iscrizione a un sindacato con delega al versamento mensile dei contributi (dato sensibile).
43. Dichiarazione di adesione a sciopero e registrazione dell'assenza per sciopero (dato potenzialmente sensibile, comunque almeno particolare). Gestione dei permessi per assemblea sindacale (dato particolare).
44. Trasmissioni dati per ritenute per sciopero al Ministero del Tesoro (dato sensibile)
45. Gestione materiali sindacali, circolari, proclamazioni di sciopero, gestione contratto integrativo della scuola, rapporti con RSU e sindacati
46. Gestione richieste, certificazioni, dichiarazioni e concessioni in relazione a permessi e distacchi per attività sindacali (dato sensibile)
47. Gestione rapporti con Rappresentante dei Lavoratori per la Sicurezza (la nomina è dato sensibile, probabilmente)
48. Certificazioni della scuola stessa su stati e qualità (dati particolari) e gestione delle certificazioni di altri enti su stati e qualità (dati particolari)
49. Redazione dell'orario di insegnamento docenti, con comunicazione ad altre scuole per docenti a scavalco (dati comuni)
50. Convocazione di riunioni, consigli di classe, collegio docenti, scrutini ecc., con comunicazione anche ad altre scuole per i docenti a scavalco (dati comuni)
51. Richiesta e concessione di autorizzazione a svolgere altre attività lavorative per persone in part - time e di svolgimento di attività libero - professionale (dati particolari)
52. Cartella sanitaria ai sensi del D.M. 81/2008 (custodita in busta chiusa) (dato sensibile) e giudizio di idoneità o inidoneità al lavoro (dato sensibile). Corrispondenza con dipendenti su particolari situazioni personali o professionali (dati particolari o sensibili).
53. Controversie di lavoro (dato particolare)
54. Denunce per violazioni penali (dato giudiziario)
55. Pratiche di dipendenti che usufruiscano di permessi o aspettative perché ricoprono cariche pubbliche (dato sensibile)
56. 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
57. Corsi e convegni o della partecipazione agli stessi e relative autorizzazioni (dati comuni o neutri)
58. Atti relativi al collegio docenti e alle commissioni di lavoro formate da docenti
59. Pratiche che richiedono una risposta o la produzione di un certificato o documento a volte sono realizzate su modulo cartaceo, più spesso con programma di elaborazione testi.
60. Tutte le altre pratiche citate nell'elenco

MODALITÀ DI RACCOLTA DEI DATI:

- Gran parte dei dati provengono dall'interessato
- Per chi è trasferito o comunque proviene da altra scuola, quest'ultima trasmette un foglio notizie e la parte rilevante del Fascicolo Personale (documenti anagrafici, documenti scolastici, eventuali certificati medici o elenchi di assenze, ecc.)
- Alcuni dati provengono dalla consultazione di archivi elettronici del MIUR.

MODALITÀ DI TRATTAMENTO:

- La gestione del Fascicolo Personale è realizzata senza l'ausilio di strumenti elettronici.

- Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi o con apposito software.
- Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati.

C - Gestione finanziaria

Dati personali trattati da Assistenti Amministrativi e D.S.G.A

1. Predisposizione del Bilancio Preventivo e del Conto Consuntivo e loro trasmissione. Gestione degli atti connessi al bilancio: mandati, ordinativi di pagamento, reversali, rapporti con l'Istituto Cassiere (dati anonimi o particolari)
2. Atti connessi al funzionamento del Consiglio d'Istituto e della Giunta Esecutiva. Predisposizione e gestione delle delibere.
3. Gestione di preventivi per acquisti di beni e servizi, anche tramite l'utilizzazione telematica del Programma di Razionalizzazione della Spesa per Beni e Servizi della P.A.
4. Individuazione periodica dell'Istituto Cassiere e dei successivi rapporti con lo stesso.
5. Gestione assicurazioni (dati comuni e particolari)
6. Versamenti Irpef e fiscali in genere, previdenziali, ecc.
7. Trasmissione all'USP dei dati relativi al fabbisogno economico (dati anonimi)
8. Rapporti con i revisori dei conti
9. Affitto di sale, ecc. ; convenzioni per macchinette bevande e merendine, per conferimento pasti, ecc.
10. Corrispondenza operativa, (dati comuni o particolari). I documenti prodotti dalla scuola per lo più sono realizzati mediante programma informatico di elaborazione testi.
11. Gestione contabile e fiscale (dati comuni e particolari). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio, che richiede password di accesso.
12. Inventario, compresa biblioteca (dati neutri).

MODALITÀ DI RACCOLTA DEI DATI:

I dati provengono dall'interessato o dal MIUR o da Enti Pubblici (in particolare locali).

MODALITÀ DI TRATTAMENTO:

- I dati sono raccolti in un apposito Fascicolo, gestito senza l'ausilio di strumenti elettronici.
- Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato , più spesso con programma di elaborazione testi o con apposito software.
- Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati.

D – Acquisti di beni e servizi

Dati trattati da Assistenti Amministrativi e D.S.G.A.

1. Acquisti di beni e servizi, nonché di affitti e prestazioni: offerte e preventivi, referenze, redazione di relazioni e prospetti comparativi delle offerte, ordini di acquisto, fatture, contratti, operazioni di collaudo (dati particolari), comprese prestazioni, servizi, forniture ad altre scuole, nonché introiti per affitto sale, spazi per macchinette automatiche distributrici, ecc.
2. Corrispondenza operativa, (dati comuni o particolari). I documenti prodotti dalla scuola per lo più sono realizzati mediante programma informatico di elaborazione testi.
3. Gestione di contabilità e fiscale (dati comuni e particolari). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio.
4. Inventario della scuola e dei beni di proprietà dell'ente locale.
5. Corrispondenza con l'ente locale in ordine alle forniture di sua competenza
6. Gestione della biblioteca

MODALITÀ DI RACCOLTA DEI DATI:

I dati provengono dall'interessato o da altre scuole ed Enti.

MODALITÀ DI TRATTAMENTO:

- I dati sono raccolti in un apposito Fascicolo, gestito senza l'ausilio di strumenti elettronici.
- Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato , più spesso con programma di elaborazione testi o con apposito software.
- Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati.

E - Gestione Istituzionale – Protocollo - Posta

Dati trattati da Assistenti Amministrativi e D.G.S.A.

1. Tutti i documenti in ingresso e in uscita vengono protocollati (gestione di dati comuni, particolari, sensibili, giudiziari). I documenti protocollati vengono passati all'Incaricato che deve trattare la pratica, che si occupa anche dell'archiviazione o della spedizione. Tuttavia documenti di valenza istituzionale perpetua o pluriennale sono archiviati a parte. I fonogrammi vengono trascritti e trattati come un documento cartaceo ricevuto. Agli atti è sempre conservato il documento cartaceo con il timbro di protocollo.
2. Corrispondenza operativa (dati comuni o particolari). I documenti prodotti dalla scuola per lo più sono realizzati mediante programma informatico di elaborazione testi.
3. Elenchi di alunni, dipendenti e genitori per attività varie della scuola
4. Elenchi e documenti riguardanti le elezioni per organi collegiali (dati comuni)
5. Circolari e normative (dati neutri)
6. Messaggi da parte di Autorità di Pubblica Sicurezza per problemi particolari e gestione del relativo trattamento.
7. Posta elettronica tramite Intranet
8. Posta elettronica tramite Internet
9. Corrispondenza con l'Ente locale proprietario dell'immobile (dati normalmente neutri)

MODALITÀ DI RACCOLTA DEI DATI:

I dati provengono dall'interessato o da enti esterni o privati

MODALITÀ DI TRATTAMENTO:

- I dati sono raccolti in un apposito Fascicolo, gestito senza l'ausilio di strumenti elettronici.
- Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato , più spesso con programma di elaborazione testi o con apposito software.
- Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati.

F – Collaboratori Scolastici - Movimentazione documenti

Dati trattati da Collaboratori Scolastici e Personale Ausiliario

1. Documenti ai fini della loro movimentazione: ricezione, trasporto, consegna e invio di documenti contenenti dati personali, aperti o in busta chiusa
2. Registri scolastici ai fini della loro movimentazione
3. Documenti contenenti dati personali allo scopo di dare indicazioni di massima agli utenti
4. Documenti e registri ai fini della loro custodia temporanea (breve periodo)
5. Elenchi di alunni, dipendenti e genitori per attività varie della scuola
6. Documenti contenenti dati personali per eseguire fotocopie e fax
7. Collaborare ad operazioni di archiviazione di documenti cartacei
8. Collaborare ad operazioni di scarto ed eliminazione di documenti cartacei
9. In generale, svolgere attività di supporto a tutti i trattamenti svolti nella scuola.

MODALITÀ DI RACCOLTA DEI DATI:

I dati provengono: dalla scuola stessa, da altri alunni o genitori, da privati o enti pubblici quali gli ambiti territoriali scolastici, dagli uffici postali e dagli spedizionieri.

MODALITÀ DI TRATTAMENTO:

Solo le azioni strettamente necessarie per compiere i trattamenti sopraelencati, da svolgere con diligenza e cautela.

PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Nessuno

ARCHIVI CARTACEI UTILIZZATI:

Collaborazione tecnica alla gestione di tutti gli archivi cartacei dislocati lontano dalla segreteria

PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA

Spedizione o consegna di plichi predisposti dalla Segreteria o dal Dirigente

G - Organi collegiali

Dati trattati da parte di persone, anche esterne, facenti parte degli organi collegiali

1. Tutte le informazioni di ordine generale e particolareggiato necessarie al Presidente del Consiglio di Istituto per il corretto espletamento delle sue funzioni: es. convoca le riunioni dell'Organo collegiale ed è autorizzato a spedire corrispondenza alle famiglie e agli alunni (anche dati sensibili)
2. Tutte le informazioni necessarie ai componenti per partecipare e contribuire alla discussione e deliberare in riferimento all'oggetto delle riunioni degli Organi collegiali (dati neutri e personali)
3. Elenchi di alunni, dipendenti e genitori per attività varie della scuola
4. Contenuto dei registri dei verbali, relative dichiarazioni a verbale presenti (anche dati sensibili) alla cui stesura partecipano
5. Dati riguardanti terzi all'interno dell'O.C. (es. alunni e genitori eletti nei Consigli di classe partecipano al trattamento)

I Collaboratori Scolastici sono incaricati dei trattamenti che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati di cui sopra.

MODALITÀ DI RACCOLTA DEI DATI:

I dati provengono dalla scuola stessa o da altri alunni o genitori

MODALITÀ DI TRATTAMENTO:

1) I trattamenti sono verbalizzati in appositi registri o prendono la forma di deliberazioni.
2) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati.

PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Nessuno

ARCHIVI CARTACEI UTILIZZATI :

1) Archivio corrente delibere di CdI e GE
2) Archivio storico delibere di CdI e GE
3) Registri dei verbali dei Consigli di classe, dei CdI e della GE

PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA

Eventuale comunicazione di delibere o mozioni. Documenti cartacei

H – Soggetti esterni - Collaboratori / Consulenti

Dati trattati da Assistenti Amministrativi e D.G.S.A.

1. Gestione di offerte e curriculum: elementi di storia personale, profilo culturale , profilo attitudinale, relazioni (dati particolari)
2. Gestione di corrispondenza operativa (dati comuni o particolari).
3. Trasmissione cartacea o telematica alla Scuola Pubblica di provenienza e solo telematica al Dipartimento della Funzione Pubblica dei dati personali di collaboratori esterni relativamente alle prestazioni economiche per anagrafe delle prestazioni.
4. Gestione di contabilità e fiscale (dati comuni e particolari). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio.

MODALITÀ DI RACCOLTA DEI DATI:

I dati provengono dall'interessato o da altre scuole ed Enti

MODALITÀ DI TRATTAMENTO:

- I dati sono raccolti in un apposito Fascicolo, gestito senza l'ausilio di strumenti elettronici.
- Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi o con apposito software.
- Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati.

ALLEGATO 2

Caratteristiche di aree, locali e strumenti

Il trattamento dei dati viene eseguito presso la sede centrale dell'Istituto ove sono allocati gli uffici amministrativi.

1. Descrizione aree e locali(sintetica descrizione a cura del titolare)

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

2. Strumenti e relativa mappa dei trattamenti

Elenco dei dati trattati e luoghi fisici (locali) del trattamento con supporti cartacei

	Codifica	***Tipologia dei dati***			***Sede***	***Stanza***	***Archivio***	
	Trattam.to	***Com***	***S***	***G***		***Trattamento***	***Cartaceo***	
							corrente	storico
Alunni (Uffici)	A	X	X	X	SD0		X	X
Alunni (Docenti)	A	X	X		SD0		X	X
Alunni (Docenti)	A	X	X		SD0		X	
Alunni (Docenti)	A	X	X		SD0		X	
Alunni (Docenti)	A	X	X		SD0		X	
Pers.le Dipendente	B	X	X		SD0		X	X
Gest. Finanziaria	C	X	X		SD0		X	X
Gest. Istituzionale	D	X	X	X	SD0		X	X

Gest. Fornitori	E	X	X	X	SD0		X	X
Collab. Scolastici	F	X	X	X	SD0		X	X
Organi Collegiali	G	X	X	X	SD0		X	X
Consulenti esterni	H	X	X		SD0		X	X
WEB	I	X						

Elenco strumenti utilizzati per il trattamento con strumenti cartacei (Archivi fisici)
(compilazione a cura del titolare o del responsabile)

Tipologia	***Sede***	***Stanza Tratt.to***	***Cod. Tratt.to***	***Tipologia dei dati***			***Archivio***	
				C	***S***	***G***	corrente	storico

Elaboratori

Elaboratori non in rete

Per elaboratori non in rete si intendono quelli non accessibili da altri elaboratori e, più in generale, da altri strumenti elettronici. Esistono elaboratori non in rete.

Elaboratori in rete(compilazione a cura del titolare o del responsabile)

Per elaboratori in rete privata si intendono quelli accessibili, da altri elaboratori o più in generale da altri strumenti elettronici, solo attraverso reti proprietarie, sulle quali possono viaggiare unicamente i dati del titolare del sistema.

Si dispone di N°_____ reti LAN private presso i **laboratori di informatica**, locali ad accesso controllato.

Su tutte le macchine dei laboratori viene utilizzato software didattico finalizzato all'esecuzione di esercitazioni da parte degli alunni. Il laboratorio viene utilizzato altresì per corsi extracurricolari sia per la formazione prettamente informatica sia per la formazione in altre discipline.

Le postazioni risultano dotate di sistema antivirus.

I dati trattati sono esclusivamente afferenti la sfera didattica e formativa e quindi sono da ritenersi praticamente neutri.

L'accesso al laboratorio avviene secondo uno specifico regolamento emesso dall'Istituto che ne definisce dettagliatamente anche l'utilizzo.

Elaboratori in rete pubblica

Per elaboratori in rete pubblica si intendono quelli che utilizzano, anche solo per alcuni tratti, reti di telecomunicazione disponibili al pubblico, ivi inclusa la rete Internet. L'Istituto in esame è cablato per l'accesso alla rete pubblica.

Pur utilizzando la stessa infrastruttura fisica, risultano definite due diverse reti logiche:

- Rete didattica (che serve le aule e i laboratori);
- Rete gestionale (che serve la Dirigenza e gli uffici amministrativi).

L'accesso fisico sulla rete esterna (Internet) é realizzato mediante apparati Router aventi configurazioni differenti in modo da non rendere visibili e accessibili i posti di lavoro di ciascuna rete definita.

ALLEGATO 3

Lista incaricati

Titolare: ISTITTO COMPRENSIVO STATALE " Rita Levi Montalcini " via G. Bocchini, 37 San Giorgio del Sannio(BN)
Legale Rappresentante p. t.: Dott.ssa Gabriella Cirocco

Responsabile del trattamento: DSGA Rag. Cerulo Aurelia

Cognome / Nome	**Sede**	***Funzione***	**Trattamenti**
		Assistente Amministrativo	

Cognome / Nome	**Sede**	***Funzione***	**Trattamenti**
		Collaboratore Scolastico	

Cognome / Nome	**Sede**	***Attività***	**Trattamenti**
		Revisore dei Conti	H
		Medico Competente D.Lgs 81/2008	H
		RSPP D.Lgs 81/2008 e s.m.i.	H
		Consulente Sicurezza D.Lgs 81/2008 e s.m.i.	
		Manutenzione Immobili ed impianti	H

Insegnanti con Delega	**Sede**	***Funzione***	**Trattamenti**
		Docente - Vicario	Tutti
		Collaboratore D. S.	Tutti
		Collaboratore D. S.	Tutti
		Collaboratore D. S.	Tutti
		Collaboratore D. S.	Tutti
		Collaboratore D. S.	Tutti
		Funzione Strumentale POF	A
		Funzione Strumentale POF	A
		Funzione Strumentale POF	A
		Funzione Strumentale POF	A
		Funzione Strumentale POF	A
		Funzione Strumentale POF	A
			A
			A
			A
			A
			A

Genitori eletti in OO.CC.	**Sede**	***Attività***	**Trattamenti**
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G
			G

			G
			G
			G
			G

ALLEGATO 4
PROCEDURE DI PROTEZIONE DATI

Mansionario

1 Regole generali del Codice della Privacy DLgs 196/03

Istruzioni che vanno applicate da tutti gli Incaricati

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

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;

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

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.

2 Procedure per Trattamenti con supporto cartaceo

Istruzioni applicate a: Assistenti Amministrativi e DSGA, Collaboratori Scolastici per quanto di loro pertinenza.
A conoscenza di: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto alla Segreteria

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 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).

Informative per la raccolta di dati

Dati comuni o particolari

Ogni raccolta di dati personali **comuni o particolari** deve 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 per intero 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 MIUR, alla Regione, al Tesoro, alla Ragioneria Provinciale dello

Stato, all'INPS 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.

Dati sensibili o giudiziari

Ogni raccolta di dati personali sensibili o giudiziari deve 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 i certificati medici e le relazioni mediche, va graffettata ad essi 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.

Trattamento su richiesta dell'Interessato

Qualunque trattamento di dati su richiesta dell'Interessato, se presentato da terzi deve essere tassativamente autorizzato da delega scritta. Ovviamente per gli alunni minorenni, il genitore o la persona esercente la patria potestà non ha bisogno di delega. Per gli alunni maggiorenni anche il genitore ha bisogno della delega. La delega va allegata all'informativa o all'istanza o alla ricevuta.

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, ancorché 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).

Verifica della legittimità del trattamento in corso

Il Responsabile o l'Incaricato devono costantemente chiedersi se la fase dello specifico trattamento dati in corso rientra nel preciso recinto di responsabilità.

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:

1. 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.
2. 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).
3. Ogni fase del trattamento rispetti le norme di legge e di regolamento.
4. In ogni fase del trattamento siano adottate le misure di sicurezza previste per la categoria alla quale il dato appartiene.
5. Se il dato è sensibile o giudiziario, siano rispettati i presupposti per avere la legittimazione a trattarlo.
6. In caso di comunicazione o diffusione, che il dato rientri nelle categorie autorizzate.

Documenti di Alunni e Personale alla conclusione del ciclo o del rapporto

Alla conclusione del ciclo di studi ovvero alla chiusura del rapporto di lavoro, ad Alunni e Personale 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 verbalino, ovviamente valutando prima se ci sono documenti che non sia opportuno eliminare (ad es. diplomi originali e simili).

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

Classificazione immediata di ogni documento/protocollo

Non appena un Incaricato si accorge che un documento contiene dati personali o di livello superiore a "comune" o "anonimo" deve conservarlo temporaneamente - prima dell'inoltro – in un'apposita cartella chiusa posta sotto il suo diretto controllo. Per maggiore sicurezza potrà, in alternativa, scrivere a matita sull'angolo destro superiore del foglio la sigla descrivente il tipo di dato: "P" = dato particolare, "S"= dato sensibile, "G"= dato giudiziario, seguita da "b" se si tratta di dato che per la sua natura rivela un'informazione poco pericolosa per l'interessato (es. certificato medico generico privo di diagnosi e di qualsiasi riferimento all'evento che lo ha generato), "a" per tutti gli altri casi.

Trattamento di un documento ricevuto

L'Incaricato che riceve "brevi manu" allo sportello o in altro luogo della scuola documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza, deve assicurarsi che sia contenuto in busta chiusa e inserirlo nella posta in arrivo per il Dirigente Scolastico.

Incaricati del trattamento di 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.

Responsabilità dell'affidamento all'Incaricato

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 accedervi o tanto meno abbandonarli momentaneamente sul tavolo; nei momenti di non utilizzazione dovrà conservarli dentro un cassetto o un armadio chiuso a chiave, del quale soltanto l'Incaricato ha la chiave.

Custodia separata per dati relativi allo stato di salute

Per dati relativi allo stato di salute ed alle abitudini sessuali (omosessualità, 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.

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 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 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.

   Per i dati personali comuni dovrà utilizzarsi una 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. 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.

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. Riteniamo che la scuola non abbia 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.

   Per i dati dati sensibili e giudiziari dovrà utilizzarsi una protezione dall'accesso fisico non autorizzato**:** l'accesso è limitato agli Incaricati del trattamento . Gli archivi devono essere ad **accesso controllato**. Tali documenti 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 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.

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 di quali 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.

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.

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 DSGA o dal Custode delle chiavi.

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. Per i documenti contenenti dati particolarmente sensibili, invece del nome sulla busta si deve scrivere un codice, la data attuale e la scadenza per la 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 dei cosiddetti "Armadi di sicurezza" (permanentemente chiusi a chiave, ad accesso controllato, in una stanza normalmente chiusa a chiave quando non presenziata.

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.

Conservazione di registri e altri documenti non più utilizzati

Molti documenti e registri sono utilizzati per un intero anno scolastico e 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 e chiusi con carta e scotch; sull'involucro viene riportato il contenuto e la scadenza per l'eliminazione. Vengono conservati in una stanza chiusa a chiave ad accesso selezionato. L'eliminazione dei documenti avviene mediante la relativa Procedura.

Archiviazione nel fascicolo personale

Per l'alunno iscritto o il dipendente in servizio, i documenti 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, fino a fine anno scolastico, poi eliminati con la procedura prevista. Il fascicolo personale è conservato nel relativo archivio corrente con armadio metallico chiuso a chiave negli orari non lavorativi e normalmente presidiato da almeno un Incaricato dei trattamenti, in una stanza in cui non sono ammessi di regola estranei, la quale viene chiusa a chiave al di fuori dell'orario lavorativo.

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, quindi archiviato nel corrispondente archivio storico, collocato in una stanza chiusa a chiave, ad accesso selezionato.

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 relativa Procedura.

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.

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.

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, in modo che il documento non venga mai lasciato in giacenza vicino alla fotocopiatrice né prima né dopo la fotocopiatura e in modo particolare se l'operazione avviene in una stanza ad accesso libero.

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.

Pulizia dei locali contenenti archivi

L'accesso di dipendenti o estranei per la pulizia dei locali contenenti archivi cartacei deve 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.

Ingresso personale esterno per manutenzione

L'accesso di dipendenti o estranei per la manutenzione dei locali contenenti archivi cartacei o delle attrezzature in tali stanze contenute, deve essere effettuata solo con i contenitori chiusi a chiave. In caso contrario, le operazioni devono essere effettuate in presenza di un Incaricato. Se i documenti con 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.

Ingresso di altre persone in segreteria

Di norma l'ingresso in segreteria, 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 Procedure per Trattamenti con strumenti elettronici

Istruzioni applicate a: Assistenti Amministrativi e DSGA, Collaboratori Scolastici per quanto di loro pertinenza
A conoscenza di: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto alla Segreteria

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 consistono in un codice per l'identificazione dell'Incaricato (user-id o username o 'nome utente') fisso e parzialmente riservato 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) nonché la diligente custodia della tessera magnetica in possesso ed uso esclusivo dell'Incaricato.
5. La parola chiave, quando é prevista dal sistema di autenticazione, deve 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 deve 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 deve 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. … per il computer … e la data). La busta va data al DSGA o 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.

Sistema di autorizzazione

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.

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 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 back up, dell'antivirus, del firewall e dei sistemi di ripristino dati in caso di "disastro informatico".

Salvataggio dei dati (backup)

Gli Incaricati sono tenuti a salvare i dati con frequenza almeno settimanale. Pertanto procederanno al backup su opportuni dispositivi di memoria di massa. Questi ultimi verranno riposti nell'armadio protetto di cui è Responsabile il DSGA e che deve restare sempre chiuso.

Cifratura dei file recanti dati idonei a rivelare lo stato di salute e la vita sessuale

Per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, il file va salvato mediante il sistema di cifratura che viene fornito dal DSGA. Le parti di documento o archivio che riguardano questi dati vanno archiviate, se possibile, in un file separato e specifico, rispetto agli altri dati personali dell'interessato (e ,se possibile, in una directory separata)

Ciò viene fatto allo scopo che gli accessi agli dati dell'interessato non implichino anche la possibilità di vedere anche questi dati particolarmente protetti. Quando si trattano dati personali idonei a rivelare lo stato di salute o le abitudini sessuali o in generale dati particolarmente sensibili, nei limiti del possibile si deve farlo con una sessione priva di interruzioni o di abbandoni della postazione, in modo da rendere la visione dei dati su schermo il più breve possibile. Nel caso di interruzioni, si deve chiudere il file. Se altre persone, anche Incaricati, si avvicinano al computer di lavoro, devono essere invitati ad allontanarsi.

La parola chiave o simile utilizzata per la cifratura dev'essere nota soltanto all'Incaricato, che la scriverà su un foglio di carta con il nome e la collocazione del file e la password. Tale foglio sarà chiuso in busta sul cui esterno si scriverà il nome e la collocazione del file e quant'altro serve per l'identificazione. La busta sarà affidata al DSGA o al nominato "Custode delle Password" se nominato, che la riporrà in luogo sicurissimo.

Programmi e dispositivi firewall

<u>Accessi abusivi logici (cioè eseguiti attraverso la logica del software)</u>

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. Altra ipotesi è quella di un PC ponte tra l'esterno e la scuola.

Programmi antivirus

Virus, worms 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 il 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. 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.

Uso di supporti rimovibili

I floppy disk, i CD etc. 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 etc.) devono essere utilizzati esclusivamente per le copie di sicurezza (back-up) e subito devono essere riposti nel luogo sicuro indicato.

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)

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.

Pulizia dei locali

L'accesso di dipendenti o estranei per la pulizia dei locali contenenti dischi di back-up deve 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 salva schermo con password di ripristino) oppure deve presenziare un Incaricato del trattamento di tali dati.

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, deve essere effettuata solo con i contenitori chiusi a chiave. Se dati sensibili o giudiziari non sono chiudibili in contenitore, l'intervento deve essere effettuata 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.

Variazione degli Incaricati

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

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.**

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 DSGA) 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.

4 Trattamenti da parte dei docenti

Istruzioni applicate a: Docenti.
A conoscenza di: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto ai docenti

Registri

I registri personali devono essere sempre custoditi in modo sicuro.

I registri di classe devono essere consultabili solo dagli alunni della classe interessata e si deve vigilare perché non vi siano accessi non autorizzati. I collaboratori scolastici sono Incaricati di riporli in luogo sicuro quando terminano le lezioni.

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

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 che non sia strettamente necessaria. Quindi eventuali certificati medici vanno visionati solo se necessario, e subito restituiti all'interessato affinché li consegni in segreteria. Questo vale in particolare per i certificati di esonero o limitazione presentati per educazione fisica; l'insegnante prenda nota dei limiti da osservare e faccia recapitare dall'interessato il certificato in segreteria. A volte l'insegnante ottiene informazioni su particolari, anche gravi, problemi di salute dell'alunno che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la vita dell'alunno (allergie con pericolo di grave shock anafilattico, asma grave con pericolo di soffocamento, diabete grave, epilessia, cardiopatie gravi, ecc.) o imbarazzanti (disturbi di continenza, ecc.), messe a disposizione dai genitori o dall'interessato. Se l'informazione è orale l'insegnante è tenuto al riserbo. Se esiste qualche comunicazione scritta, trattasi di dato sensibile e va trattato con particolari cautele, chiedendo al Titolare o al DSGA come fare.

Anche informazioni su particolari diete seguite dall'alunno o per motivi di salute o per motivi religiosi sono da considerare dato sensibile, pertanto va rivelato soltanto nei casi strettamente necessari ed omettendone la ragione.

Nel caso di alunni portatori di handicap che incide sulla didattica, la visione e la detenzione della relativa documentazione per l'integrazione è un dato di massima sensibilità in quanto idoneo a rivelare lo stato di salute.

Pertanto i documenti dovranno essere visti soltanto dai docenti e personale strettamente necessario, conservati con elevata cautela, poi consegnati in segreteria mettendoli in busta chiusa su cui sarà annotato nome dell'interessato, descrizione del contenuto, data e l'annotazione "Da conservare separatamente in armadio sicuro".

Al suo posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione.

Elaborati contenenti notizie particolari o sensibili

Nel caso un elaborato consegnato alla scuola contenga dati personali o familiari particolari o sensibili, va custodito con cura e poi consegnato personalmente in segreteria mettendolo in busta chiusa su cui sarà annotato nome dell'interessato, descrizione del contenuto, data e l'annotazione "Da conservare separatamente in armadio sicuro". Al suo posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione.

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.

Gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro 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)

Istruzioni applicate a: membri di organi collegiali.

A conoscenza di: Collab. del Dirigente, Assistenti Amm.vi, DSGA e Collaboratori Scolastici in quanto di supporto

Gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro 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 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

e Pers. Ausiliario

Istruzioni applicate a: Collaboratori Scolastici e Personale Ausiliario.
A conoscenza di: Collaboratori del Dirigente, Assistenti Amministrativi e DSGA in quanto di supporto

Gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro 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 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.

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.

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 DSGA 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 DSGA deve presenziare un addetto alla segreteria.

La Presidenza, 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 PC 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.

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 5

ELENCO DEGLI AMMINISTRATORI DI SISTEMA ED ASSIMILATI

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, siano raggruppati in un elenco, si procede alla stesura dell'elencazione di cui prima

1) Sig _____ Incaricato Esterno inquadrato come amministratore di sistema, Addetto alla manutenzione e gestione dell'hardware e 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 _____ Incaricato Esterno inquadrato come amministratore di sistema, Addetto alla manutenzione e gestione dell'hardware e 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.

3) Sig _____ Incaricato Esterno inquadrato come amministratore di sistema, Addetto alla manutenzione e gestione dell'hardware e 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.

5) Sig. _____, Dipendente inquadrato come amministratore di sistema, Addetto al backup periodico e mensile dei dati

6) Sig. _____, Dipendente inquadrato come amministratore di sistema, Addetto al backup periodico e mensile dei dati

7) Sig. _____, Dipendente inquadrato come amministratore di sistema, Addetto al backup periodico e mensile dei dati

8) Sig. _____, Dipendente inquadrato come amministratore di sistema, Addetto alla funzione di <Custode delle password>

9) Sig. _____, Dipendente inquadrato come amministratore di sistema, Addetto alla funzione di <Custode delle password>

10) Sig. _____, Dipendente inquadrato come amministratore di sistema, Addetto alla funzione di <Custode delle password>

11) Sig. _____, Incaricato Esterno inquadrato come amministratore di sistema, Addetto alla gestione del sito web

12) Sig. _____, Incaricato Esterno inquadrato come amministratore di sistema, Addetto alla gestione del sito web

13) Sig. _____, Incaricato Esterno inquadrato come amministratore di sistema, Addetto alla gestione del sito web

San Giorgio del Sannio(BN), gennaio 2014

f.to IL TITOLARE
Dott.ssa Gabriella Cirocco

N.B.: Si precisa che per la conoscenza di quanto nel presente documento non compilato è possibile, secondo la normativa in merito vigente, fare richiesta scritta direttamente al Titolare.