ISTITUTO COMPRENSIVO STATALE «VITTORINO DA FELTRE»
Via Finalmarina, 5 - 10126 TORINO Cod. M.P.I. TOIC8A100T
Tel. 011/6967809 - Fax 011/6635218 - e-mail: TOIC8A100T@istruzione.it

Sede centrale elementare Via Finalmarina, 5 Torino	*Sezione staccata elementare* O.I.R.M. - C.so Polonia, 94	*Scuola dell'infanzia* Via Garessio, 24 - Torino	*Plesso Fermi Scuola Sec. I grado P.ssa Giacomini 24 Torino*

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Il Dirigente dell'Istituzione Scolastica

Visto il decreto legislativo 30 giugno 2003 n. 196 recante il codice in materia di protezione di dati personali, e segnatamente gli art. 34 e ss., nonché l'allegato B del suddetto D. Lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

Considerato che l'Istituzione Scolastica: Istituto Comprensivo VITTORINO DA FELTRE, con sede in via Finalmarina 5 a Torino in quanto dotata di un autonomo potere decisionale, ai sensi dell'art. 28 del d. Lgs. n. 196 del 2004, deve ritenersi titolare del trattamento di dati personali;

Attesto che la suddetta istituzione scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli art. 31 e ss. Del d. Lgs. n. 196 del 2003,

Adotta il presente Documento programmatico sulla sicurezza dei dati redatto ai sensi e per gli effetti dell'art. 34, comma 1, lettera g) del D. Lgs. 196/2003 e del disciplinare tecnico allegato B.

1. *SCOPO DEL DOCUMENTO E APPLICABILITA'*

Scopo di questo Documento Programmatico per la Sicurezza nel seguito indicato DPS, è di delineare i criteri, le modalità operative e le misure organizzative, fisiche e logiche adottate dall'Istituto per garantire:

a. la disponibilità delle informazioni per gli utenti del sistema;
b. l'integrità delle informazioni, che quindi possono essere create, modificate o cancellate solo dalle persone autorizzate a svolgere tali operazioni;
c. l'autenticità e la garanzia della provenienza dei dati;
d. la riservatezza delle informazioni, che possono essere fruite solo dalle persone autorizzate.

In questo documento vengono definiti in particolare:

- l'elenco dei trattamenti di dati personali;
- i tipi di dati trattati;
- la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- i modi per individuare e valutare i rischi;
- l'analisi dei rischi che incombono sui dati;
- le misure adottate per garantire l'integrità e la disponibilità dei dati in seguito a distribuzione o danneggiamento;
- gli interventi formativi previsti per gli incarichi del trattamento;
- i criteri da adottare in caso di affidamento del trattamento a soggetti esterni all'istituto;
- le modalità di verifica e valutazione delle misure adottate.

Le indicazioni contenute nel presente documento devono essere utilizzate per gestire i rischi connessi alle attività di trattamento dei dati personali, sia in seno all'istituto che da parte dei responsabili esterni.

2. *CARATTERISTICHE DELL'ISTITUTO*

Le persone

Gli alunni iscritti ai corsi sono n. 962
L'organico del personale:
docente, compreso il personale che presta servizio anche in altre istituzioni scolastiche, è costituito da n. 95 Docenti;
A.T.A. Consta di n. 19 unità così distribuite:

n. 1 Direttore dei servizi generali e amministrativi,
n. 6 assistenti amministrativi,
n. 12 collaboratori scolastici.

Le strutture

La scuola è così articolata:
sede n. 1 – centrale sita nel Comune di Torino in Via Finalmarina, 5;
sede n. 2 – sita nel Comune di Torino in Via Garessio 24
sede n. 3 – sita nel Comune di Torino in Piazza Polonia presso l'Ospedale Infantile Regina Margherita
sede n. 4 – sita nel Comune di Torino in Piazza Giacomini, 24.

Struttura dell'edificio:
I locali dove vengono trattati dati personali, sia per mezzo di documenti cartacei che attraverso applicazioni ed archivi informatici, sono situati nell'area separata dedicata agli uffici il cui accesso è sempre presidiato durante il normale svolgimento dell'attività lavorativa.

Misure di sicurezza (TU81/2008)
Il sistema antincendio è costituito da estintori manuali a polvere ed anidride carbonica omologati. E' garantita la manutenzione con controllo d'efficienza semestrale da parte di una società specializzata e si è provveduto ad assicurare la continuità nell'addestramento di personale preposto sull'uso degli estintori stessi.
Inoltre la sede è provvista di rilevatori di fumo.
E' stato predisposto un piano di evacuazione, sono ubicati nei punti necessari e visibili al pubblico le procedure scritte da seguire in caso d'emergenza, è funzionante l'impianto di illuminazione d'emergenza nei locali d'accesso al pubblico.

Alimentazione elettrica e sistemi di continuità
L'impianto elettrico è a norma come anche la cablatura della rete informatica. Esiste la dichiarazione di conformità firmata dall'installatore. E' presente per le postazioni di lavoro e il server un sistema d'alimentazione specifico e dedicato.

3. *RESPONSABILITA'*

I responsabili, gli incaricati del trattamento e i manutentori del sistema sono individuati con apposito provvedimento che specifica finalità e modalità del trattamento autorizzate nonché tipologie di comunicazione e diffusione ammesse (Allegato C).

Titolare del trattamento

Titolare del trattamento è l'Istituto Comprensivo Vittorino da Feltre, con sede in via Finalmarina 5 a Torino nella veste del suo rappresentante legale pro-tempore, il Dirigente Scolastico dr.ssa Giuseppina FUSCO.
Il Dirigente Scolastico in qualità di titolare del trattamento dei dati:

- è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione di misure di sicurezza;
- procede alla predisposizione delle misure ritenute indispensabili nella struttura e ne dispone l'adozione;
- individua il responsabile del trattamento e con apposito incarico ne stabilisce la responsabilità in merito al rispetto degli adempimenti e delle prescrizioni stabiliti sulla base del D. Lgs. 196/03;
- si avvale della collaborazione del DSGA e dei responsabili dei diversi settori per la definizione della modulistica e delle procedure.

Responsabile del trattamento

Al responsabile del trattamento sono attribuiti incarichi di ordine organizzativo e direttivo, ed egli provvede a:

- individuare e designare per iscritto gli incaricati del trattamento che operano sotto la sua diretta autorità indicando puntualmente l'ambito del trattamento consentito;
- impartire loro specifiche istruzioni scritte relative alle modalità di trattamento ammesse;
- organizzare la formazione per gli incaricati;
- procedere alle verifiche specificate nell'incarico.

E' individuato quale responsabile del trattamento dei dati comuni e sensibili: signora Margherita IOSCA.

Amministratore di sistema

Il titolare del trattamento conferisce l'incarico di Amministratore di Sistema al soggetto incaricato di sovrintendere alle Risorse Informatiche dell'Istituto secondo quanto stabilito nel *Disciplinare interno* (*Allegato B*) per l'utilizzo delle strutture informatiche degli Uffici si Segreteria, della rete Internet e della posta elettronica.
L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al personal computer di ciascun dipendente..

Incaricati del trattamento

L'assegnazione del personale docente e ATA alla specifica unità operativa, per la quale è individuato con atto formale, comporta l'automatico incarico al trattamento autorizzato per iscritto agli addetti all'unità medesima e la consegna, a cura del Responsabile del Trattamento, delle specifiche istruzioni scritte relative alla modalità di trattamento ammesse.
In relazione alle limitate dimensioni della struttura e per il fatto che non si ravvisano ragioni di tutela della riservatezza tali, da imporre che uno o più incaricati non possano accedere ad alcune tipologie di dati personali oggetto di trattamento, non appare necessario prevedere profili di autorizzazione distinti per le diverse persone.
Di norma tali incarichi sono assegnati a partire dal 1° settembre, data di inizio del nuovo anno scolastico che coincide con le assegnazioni di sede del personale. Al presente documento è allegato l'elenco dei provvedimenti adottati con i relativi estremi (*Allegato C*).
Sia per i trattamenti effettuati con strumenti elettronici, che per quelli che avvengono senza l'ausilio di tali strumenti, l'autorizzazione al trattamento è soggetta ad aggiornamento periodico e comunque almeno annuale, quando viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione riguardo l'ambito di trattamento consentito sia ai singoli incaricati che agli addetti alla manutenzione e gestione degli strumenti elettronici.

4. *DATI E BANCHE DATI*

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare:
sono precisate le finalità del trattamento;
sono individuati i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili ed alla categoria di soggetti cui essi si riferiscono (alunni, personale dipendente, fornitori,....);
sono definite le operazioni di trattamento dei dati effettuate;
sono descritte le aree, i locali e gli strumenti con i quali si effettuano i trattamenti.

Finalità del trattamento

Al fine di perseguire le finalità istituzionali, l'Istituto Comprensivo Vittorino da Feltre effettua operazioni di trattamento di dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori con le seguenti finalità:

a. la selezione e il reclutamento del personale a tempo determinato, nonché l'instaurazione, la gestione e la cessazione del rapporto di lavoro;
b. la frequenza dei corsi di studio;
c. l'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione, di scrutini, di esami di licenza;
d. l'attivazione degli organismi collegiali e delle commissioni istituzionali previsti dall'ordinamento scolastico;
e. l'acquisizione di beni, servizi e opere;
f. la difesa in giudizio del Ministero dell'Istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrative, nonché quelle connesse alla gestione degli affari penali e civili;
g. le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc...) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche.

Tipologie di dati trattati

L'Istituto Comprensivo Vittorino da Feltre, con salvezza delle possibilità di procedere a successive integrazioni e/o correzioni, tratta i dati personali di natura comune o sensibile di seguito elencati:

a. dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del D. Lgs. n. 196 del 2003, univocamente riconducibili ad un soggetto fisico, identificato o identificabile, quali nominativo, dati di nascita, residenza, domicilio, stato di famiglia, codice fiscale;
b. dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del D. Lgs. n. 196 del 2003, univocamente riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la sede, la Partita IVA, il Codice fiscale, la titolarità di diritti o la disponibilità di beni strumentali;
c. dati identificativi, ai sensi dell'art. 4, comma 1, lettera d) del D. Lgs. n. 196 del 2003 così come descritti nelle schede allegate al D.M. 305 del 7/12/06 e relativi a origine, convinzioni religiose, filosofiche politiche e sindacali, stato di salute e vita sessuale;
d. dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi, individualizzati differenziati;
e. dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;
f. dati atti a rilevare la presenza presso l'istituzione scolastica dei destinatari dell'offerta formativa ovvero dei famigliari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale offerta;
g. dati inerenti negoziazioni e relative modalità di pagamento riguardo ad attività professionale a fini formativi;
h. dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;

i. dati contabili e fiscali;
j. dati inerenti la titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;
k. dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

I dati trattati da questa amministrazione sono noti all'istituzione scolastica, in ragione della produzione di atti e/o dichiarazioni raccolti su richiesta degli interessati a fruire direttamente o indirettamente (come nel caso dei minori sottoposti alla potestà ex art. 316 c.c.), dei servizi formativi o previa richiesta dell'Ufficio presso i medesimi ovvero presso altri soggetti pubblici e privati in particolare attraverso:

- documenti contabili connessi alla fornitura di prestazioni e/o di servizi e/o di lavori;
- documentazione bancaria, finanziaria e/o assicurativa;
- documenti inerenti il rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/ previdenziali;
- pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

I dati sono accolti e conservati su supporti cartacei e/o informatici e organizzati nelle seguenti banche dati:

- banca dati alunni;
- banca dati personale direttivo, insegnante e ATA a tempo indeterminato e determinato;
- banca dati fornitori (beni e servizi);
- banca dati – contabilità;
- banca dati – protocollo

per ognuna delle quali è predisposta una scheda di processo allegata al presente documento (*Allegato A*). I documenti e le banche dati settoriali allocate nelle varie postazioni di lavoro ricadono per le operazioni di salvataggio, condivisione e comunicazione significativa sotto la responsabilità dei diversi incaricati. Il sistema di abilitazioni dispone l'utilizzo delle informazioni ai soli utilizzatori a cui è assegnata la competenza in un dato ambito di lavoro.

Operazioni di trattamenti dei dati effettuate

Sono considerate operazioni di trattamento dei dati quelle di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco cancellazione e distruzione dei dati stessi oltre ad interconnessione e raffronti con altro titolare anche effettuate mediante strumenti elettronici.
Delle operazioni di trattamento sono incaricati gli operatori individuati annualmente con apposita nomina che contestualmente precisa le operazioni autorizzate in relazione alle banche dati e alle modalità di trattamento (informatizzato e non).

Il trattamento dei dati viene effettuato nei seguenti locali:

- Ufficio di Segreteria
- Aule

Archiviazione cartacea
I documenti sono conservati nei seguenti locali:

1. Archivio storico
2. Ufficio del Dirigente scolastico (cassettiera)
3. Ufficio del DSGA (armadio, cassettiera, computer);
4. Ufficio della Didattica nell'archivio corrente(schedari, armadi, computer in Segreteria);
5. Ufficio del Personale nell'archivio corrente (schedari, armadi, computer in Segreteria);
6. Ufficio della Contabilità nell'archivio corrente (schedari, armadi, computer nell'Ufficio DSGA);
7. Ufficio del Protocollo nell'archivio corrente (schedari, armadi, computer in Segreteria)
8. Ufficio di Segreteria Scuola Fermi (schedari e armadi)

Gli uffici sono chiudibili a chiave.

Gli armadi per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari sono adeguati a garantire la necessaria sicurezza ai dati personali contenuti negli atti, documenti e supporti ivi conservati in quanto muniti di apposite serrature e chiavi. E' presente una cassaforte destinata anche al ricovero dei supporti contenenti le copie di sicurezza delle banche dati informatiche.

Strumentazioni informatiche via Finalmarina
La situazione attuale delle attrezzature informatiche è la seguente:
Elenco delle postazioni:
Lab. Informatica:n. 21
Ufficio di Segreteria: n. 4 + Server
Ufficio di Direzione: 2
Inoltre tutte le aule sono cablate e dotate di un PC

Strumentazioni Informatiche Via Garessio

La situazione attuale delle attrezzature informatiche è la seguente:
n. 1 postazione informatica

Strumentazioni Informatiche Scuola ospedaliera
La situazione attuale delle attrezzature informatiche è la seguente:
n.14 computer portatili + n. 8 i pad

Strumentazioni Informatiche Piazza Giacomini
La situazione attuale delle attrezzature informatiche è la seguente:
n. 15 postazioni informatiche

Software operativi via Finalmarina

I PC del lab. Informatica sono dotati di sistema operativo Windows XP regolarmente licenziato (vedi registro software)
Il Server della segreteria è dotato di sistema operativo Windows 7 regolarmente licenziato (vedi registro software)
i Client della segreteria sono dotati di sistema opeativo Windows 7 regolarmente licenziato (vedi registro software)
I PC degli Uffici di Direzione sono dotati di sistema operativo Windows XP e Windows 7 regolarmente licenziato (vedi registro Software)
Tutti i programmi software applicativi sono coperti da contratto di manutenzione (migliorativa, correttiva) e assistenza tecnica.

5. *CRITERI PER L'INDIVIDUAZIONE DEI RISCHI E LA LORO VALUTAZIONE*

Criteri per l'individuazione dei rischi.

Per garantire la disponibilità, l'integrità, l'autenticità e la riservatezza delle informazioni, gli articoli da 33 a 36 del Testo Unico in materia di Trattamento dei dati personali di cui al D.Lgs. 30 giugno 2003, n. 196 prevedono l'obbligo di adottare misure minime di sicurezza, ai sensi dell'allegato B del disciplinare tecnico del Testo Unico, che possono essere individuate sulla base di tre grandi categorie di rischi:

- rischi connessi ad eventi relativi al contesto fisico ambientale;
- rischi connessi al mancato rispetto da parte degli operatori degli adempimenti e delle prescrizioni statuite sulla base del disposto Testo Unico in materia di trattamento di dati personali;
- rischi propri del sistema informatico utilizzato dall'Istituto Scolastico.

L'analisi dei possibili rischi è stata, pertanto, suddivisa in tre settori di rischio nettamente differenti e separati per tipologia e materia.

A. Eventi relativi al contesto fisico – ambientale

In questo settore sono stati identificati e valutati i rischi legati ad eventi di origine fortuita, dolosa o colposa (es. legati alla eventualità che persone non autorizzate possano accedere nei locali) e sono riferiti al luogo dove gli strumenti sono ubicati e quindi agli archivi esistenti negli uffici, agli elaborati in rete ed ai server ivi ubicati.

Fonti di rischio	*Rischio*
1. Accessi non autorizzati a locali ad accesso ristretto	• dispersione, perdita o alterazione, anche irreversibile, di dati; • visione abusiva di dati, furto di documenti, uso non autorizzato dei dati; • manomissione di programmi ed elaboratori; • impossibilità temporanea di accesso ai dati e di utilizzo dei programmi.
2. Asportazione e furto di strumenti contenti dati	• dispersione e perdita di dati, di programmi e di elaboratori; • accesso altrui non autorizzato
3. Eventi distruttivi dolosi oppure accidentali	• perdita di dati, dei programmi e degli elaboratori
4. Guasti a impianto elettrico	• perdita o alterazione, anche irreversibile di dati; • manomissione dei programmi e degli elaboratori; • impossibilità temporanea di accesso ai dati e di utilizzo dei programmi.

B. Comportamento degli operatori

In questo primo settore sono stati identificati e valutati i rischi legati all'attività delle persone (docenti e ATA) incaricate del trattamento dei dati.

Fonti di rischio	*Rischio*
5. Mancato rispetto del divieto di accesso agli archivi fisici o informatizzati non autorizzati	• sottrazione/presa visione/copia abusiva di informazioni e dati; • potenziale diffusione di dati anche quando non intenzionate (es. cestinare un semplice Documento cartaceo senza provvedere alla sua distruzione • distruzione/alterazione dei dati
6. Mancata custodia, anche temporanea, dei documenti estratti dall'archivio	
7. Mancata custodia della propria postazione informatica	
8. Mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio	
9. Mancata distruzione dei supporti raggiunta la finalità	
10. Mancata conservazione o restituzione dei documenti cartacei	• cancellazione anche accidentale di dati e conseguente loro perdita; • alterazione dati;
11. Errori materiali dei soggetti legittimati al trattamento dei dati	• trattamento illegittimo di dati per loro comunicazione a soggetti non autorizzati; • trattamento non conforme alle finalità della raccolta;
12. Comportamenti dolosi dei soggetti legittimati	• comunicazioni/diffusione di dati personali non previste preventivamente dalla legge;

C. **Eventi relativi agli strumenti**

In questo settore sono stati identificati e valutati i rischi legati alle infrastrutture tecnologiche (risorse hardware e software) e il rischio di intrusione nelle reti di comunicazione durante la normale attività del sistema informatico. Tali rischi sono collegati a:

- tasso di obsolescenza delle apparecchiature,
- modalità di esecuzione delle copie di sicurezza,
- funzionalità di accesso,
- quote disco condivise in lettura,
- rete di comunicazione accessibile al pubblico,
- utilizzo di periferiche di input.

Fonti di rischio	*Rischio*
1. Virus informatici	• perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori.
2. Sabotaggio HW e SW	• perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori;
3. Alterazione o distruzione di dati a causa di sabotaggio	• Impossibilità temporanea di accesso ai dati e di utilizzo dei programmi
4. Malfunzionamento, indisponibilità o degrado degli strumenti HW	
5. Malfunzionamento SW	
6. Guasto Tecnologico	

7. Accessi esterni non autorizzati	• Presa visione, copia abusiva, sottrazione di dati; • perdita o alterazione, anche irreversibile, di dati; • uso non autorizzato di applicativi; • manomissione di programmi e di elaboratori; • impossibilità temporanea di accesso ai dati e di utilizzo dei programmi
8. Perdita delle copie di back - up	• Presa visione, copia abusiva;
9. Perdita o riutilizzo non autorizzato di supporti magnetici	• Perdita, anche irreversibile, di dati.
10. Intercettazione delle trasmissioni di dati	• Diffusione di dati

Criteri per la valutazione dei rischi
La probabilità di accadimenti come quelli appena individuati è molto bassa.
Negli ultimi cinque anni non si sono verificati episodi di perdita, alterazione, comunicazione o diffusione di dati riservati.

6. *MISURE DI PROTEZIONE NECESSARIE IN RELAZIONE AL CONTESTO DESCRITTO*

Dopo aver analizzato e valutato i fattori di rischio di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, sono state individuate le misure di prevenzione e protezione più idonee a prevenire, ridurre o eliminare il rischio secondo quanto riportato nelle tabelle successive.

Misure fisiche

Rischio	*Misure di protezione*	
Sottrazione/presa visione/copia abusiva di informazioni e dati conseguente a: • accessi non autorizzati a locali ad accesso ristretto; • asportazione e furto di strumenti contenenti dati.	Vigilanza della sede	• Chiusura a chiave locali • Sistemi di allarme
	Custodia e archiviazione di atti, documenti e supporti	• Chiusura a chiave locali e armadi • Procedura gestione chiavi • autenticazione accessi • Custodia in armadi blindati
Perdita di dati dovuti a: • movimenti tellurici, scariche atmosferiche, incendi, allagamenti, eventi distruttivi dolosi, accidentali o dovuti ad incuria o vandalismo; • guasti a impianto elettrico, gruppo di continuità, climatizzazione, etc.	Adeguamento e manutenzione strutture ed impianti	• Impianto elettrico a norma • Sistemi di protezione antincendio • Impianto di messa a terra • Gruppo di continuità elettrica • PC sollevati da terra per proteggerli in caso di allagamento

Alle misure individuate devono accompagnarsi quelle di natura organizzativa che riguardano:
- l'assegnazione di incarichi, autorizzazioni e compiti al personale dipendente;
- le istruzioni operative agli incaricati per il servizio di sorveglianza, la custodia e l'archiviazione di atti, documenti e supporti, le modalità di accesso, il controllo delle presenze di personale e alunni;
- la definizione di procedure per i controlli fisici all'accesso, la gestione delle chiavi, il carico/scarico di documenti, la manutenzione degli impianti e dei locali.

Particolare attenzione è prestata per gli archivi e i documenti relativi a dati sensibili e giudiziari affinché ai dati non possano accedere persone prive di autorizzazione.

Misure organizzative

Individuati e valutate tutte le fonti di rischio, sono stati determinati i seguenti provvedimenti:
individuazione dei responsabili e degli incaricati al trattamento (*Allegato C*);
istruzioni operative per il personale con misure graduate per classi di dati (*Allegato B*)

Rischio	*Misure di protezione*	
Perdita o alterazione di dati dovuti a: • mancata conservazione o restituzione dei documenti cartacei; • ad errori materiali o a comportamenti imprudenti o negligenti	Istruzioni operative Controlli periodici	• Istruzioni organizzative e tecniche
Diffusione di dati causata da: • mancata custodia dei documenti o della propria postazione; • mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio; • mancata distruzione dei supporti raggiunta la finalità		• Istruzioni organizzative e tecniche sui comportamenti da tenere; • sorveglianza sulla distruzione dei supporti rimovibili; • presenza in segreteria di appositi distruggi documenti cartacei
Trattamento non conforme o illegittimo di dati e loro comunicazione o diffusione a soggetti non autorizzati	Assegnazione incarichi Istruzioni operative Controlli periodici	• Adozione di procedure riguardo a soggetti e modalità con cui i dati possono essere comunicati dalla segreteria scolastica verso l'esterno
Sottrazione/presa visione/copia abusiva di informazioni e dati conseguente al mancato rispetto del divieto di accesso agli archivi fisici o informatizzati non autorizzati.	Log file Ingresso controllato	• Organizzazione servizio di sorveglianza • Credenziali di accesso • consultazioni registrate • controllo fotocopiatura (fotocopiatrice con chiave e registrazione numero copie)

Si ritiene infine che solo un'adeguata conoscenza del disposto normativo può realmente e proficuamente garantire l'osservanza del medesimo ed, in definitiva, abbattere i rischi connessi a questo settore che è sicuramente il più rilevante e quindi quello a cui vanno dedicate le maggiori attenzioni per garantire un trattamento dei dati conforme alle prescrizioni legislative.

Misure logiche

Per i trattamenti effettuati con strumenti elettronici vengono individuate alcune misure per evitare:

- i rischi di intrusione
- la diffusione illegittima di dati,
- l'accesso abusivo.

Rischio	*Misure di protezione*

Perdita o alterazione di dati/applicativi dovuta a: • azione di virus informatici con conseguente dallo HW e/o SW; • alterazione HW e SW a causa di sabotaggio; • malfunzionamento, indisponibilità o degrado degli strumenti HW o SW; • perdita delle copie di back up.	Contratti di assistenza tecnica Servizio di manutenzione correttiva e straordinaria dei programmi	• Firewell antintrusione come modulo software; • servizio di filtraggio antivirus e antispamming per il controllo dei messaggi e degli allegati di posta elettronica; • controllo delle pagine Internet in ordine a cookies. Activex, java; • controllo antivirus in automatico di ogni file scaricato dalla rete o letto da supporti esterni quali Floppy Disk e CD-ROM; • aggiornamento automatico dell'antivirus; • back up dei programmi applicativi; • back up periodico; • deposito delle copie di sicurezza in armadi dislocati presso la Segreteria.

Misure di sicurezza suppletive relative al trattamento di particolari dati sensibili
In caso di trattamento di dati sensibili o giudiziari (punto 19,8 del D. Lgs: n. 196/2003) ed in particolare per i dati personali idonei a rivelare lo stato di salute, devono essere adottati particolari accorgimenti;

1. la custodia/archiviazione di tali dati separatamente dagli altri dati personali dell'interessato;
2. L'accesso, per la consultazione e/o modificazione è condizionato dal rispetto della procedura di identificazione per cui:
   a. l'incaricato deve essere precisamente individuato ed autenticato;
   b. l'incaricato può trattare i dati sensibili solo con un profilo di autorizzazione;
   c. l'incaricato deve essere in possesso della chiave di accesso.

I dati sensibili debbono essere nettamente separati e gestiti autonomamente in base al proprio profilo di autorizzazione; per quel che attiene i dati personali degli alunni riportati sui registri didattici va prevista apposita procedura per la loro raccolta e custodia;

Programma delle misure
Il programma delle misure di sicurezza adottate o da adottare per ogni categoria di rischi è sistematicamente aggiornato nell'ottica di un miglioramento continuo del Sistema Sicurezza dell'Istituto Scolastico con cadenza annuale e in tutte le occasioni in cui si riscontri necessità di intervento o non conformità (tecniche o normative).

7. *FORMAZIONE DEL PERSONALE*

La previsione di interventi formativi degli incaricati del trattamento rientra tra gli aspetti più importanti del presente documento.
In effetti, una gestione impropria da parte del personale ATA chiamato alla gestione dei dati personali nonché del corpo insegnante per quel che attiene il trattamento dei dati degli alunni effettuato con i registri di classe, la mancanza di chiare direttive esplicative e l'assenza di strumenti di controllo di facile e rapida applicazione costituiscono le cause principali del verificarsi, anche inconsapevole, di danni agli interessati ed in definitiva la causa prioritaria di trattamenti illegittimi e non conformi alle specifiche finalità dell'istituzione scolastica.
Gli interventi formativi sono programmati in modo da avere luogo al verificarsi di una delle seguenti circostanze:

- al momento dell'ingresso in servizio;
- in occasione di un cambiamento di mansioni che implichi modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti con conseguenti rilevanti modifiche nel trattamento di dati personali.

Scopo della formazione
Il D.Lgs. 196/2003 impone la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. Di conseguenza l'istituto programma interventi formativi degli incaricati del trattamento, finalizzati a renderli edotti nei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;

- misure disponibili per prevenire eventi dannosi e procedure da seguire;
- modalità per mantenersi aggiornati sulle misure di sicurezza adottate dal titolare.

Modalità di formazione degli incaricati del trattamento dei dati personali.
Sotto la diretta vigilanza e il coordinamento del Responsabile del Trattamento è prevista la predisposizione e l'applicazione di un adeguato e dettagliato piano di formazione del personale che contempla la possibilità di:

- *Aggiornamento Periodico* sotto la diretta vigilanza del Responsabile del Trattamento con cadenza almeno annuale stabilito in coincidenza con l'obbligo di aggiornamento del Documento Programmatico sulla Sicurezza;
- *Aggiornamento Specifico*, tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuovo banche dati oppure utilizzi nuovi strumenti informatici e/o nuove e diverse procedure mediante un programma individuale che deve essere impartito dal Responsabile in relazione alla nuova e specifica attività di trattamento svolta.

Gli interventi formativi possono avvenire:

- mediante la consegna di materiale esplicativo riguardante le norme, gli adempimenti richiesti nonché le misure minime di sicurezza applicate dall'Istituto;
- all'interno dell'Istituto, a cura del responsabile per la sicurezza, del responsabile al trattamento o di altri soggetti esperti nella materia;
- all'esterno dell'Istituto, presso soggetti specializzati.

Valutazione dell'efficienza del piano di formazione.
Il responsabile del Trattamento dei dati personali, dopo avere dettagliatamente individuato il contenuto del piano di formazione del personale ATA e degli insegnanti, appronta una serie di strumenti di verifica dell'efficienza della formazione impartita per essere certo che essa sia stata realmente recepita dagli incaricati del trattamento e che sia stata funzionale ad un appropriato e sicuro trattamento dei dati personali.

8. RIPRISTINO DEI DATI

Le misure ritenute idonee per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici sono:

1. residenza dei dati in una struttura documentale sul server condivisa in rete e non sui dischi dei singoli PC;
2. procedure automatiche di backup dei database e dei dati contenuti nel server su supporti adeguati alla qualità di dati che deve essere salvata;
3. copie di backup giornaliere su hard disk per le banche dati gestionali e istruzioni organizzative e tecniche che prevedono il salvataggio con frequenza almeno settimanale per quanto riguarda la gestione documentale;
4. etichettatura ed archiviazione dei supporti utilizzati per il back up dei dati con conservazione delle copie di sicurezza in cassaforte;
5. procedure di recupero immediato dei dati in caso di attacchi;
6. analisi e test di tutti i software in possesso dell'Istituto scolastico di tutti gli hardware nonché tutti gli altri strumenti informatici tecnico – operativi dell'intero sistema informatico scolastico.

Sono salvati anche i sistemi attraverso la copia della configurazione di sistema/rete su hard disk di back up e copie del sistema operativo e degli applicativi presenti nel server, tramite back up su hard disk e CD affinché siano ripristinabili. Si provvede al rifacimento di tali copie con periodicità dettata dagli interventi di manutenzione e aggiornamento del software di base (sistemi operativi, piattaforma database, ecc.) e dei programmi applicativi.
Per quanto riguarda i documenti cartacei e i supporti diversi da quelli elettronici contenenti dati personali, essi sono fascicolati e depositati:

- presso l'archivio generale per quanto riguarda: banche dati alunni, personale, contabilità, fornitori;
- nell'archivio corrente per quanto riguarda: banche dati alunni, personale, contabilità, fornitori.

9. *ATTIVITA' DI CONTROLLO E VALUTAZIONE*

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile del trattamento e le persone da questo appositamente indicate provvedono, in modo estemporaneo, anche con verifiche casuali e non annunciate e/o con controlli a campione, a verificare che le misure implementate, sia quelle tecnologiche che quelle organizzative, siano effettivamente applicate e svolgano correttamente le funzionalità per cui sono state adottate.
Tale verifica si sostanzia nelle 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;
- verificare l'integrità dei dati e delle loro copie di back up;
- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici, che non possono più essere riutilizzati vengano distrutti;
- verificare il livello di formazione degli incaricati.

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. In sede di valutazione il Titolare del trattamento, coadiuvato dal Responsabile del trattamento e dall'Amministratore di sistema, analizza l'efficacia degli strumenti adottati al fine di:

- rivedere se necessario l'indica di gravità dei rischi controllando quali danni si sono avuti o quali siano possibili, la frequenza degli accadimenti registrati, le circostanze in cui si sono subiti gli attacchi;
- individuare le misure che sono risultate non adeguate e che vanno riconsiderate.

Al responsabile del trattamento è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito. A tale fine, è previsto che al Responsabile venga affidato un budget annuo che può utilizzare in autonomia, nel rispetto delle normative di legge e di regolamento relative alle forniture pubbliche.
Il presente documento, è stato aggiornato il giorno 04 del mese di settembre 2013 assunto al protocollo dell'Istituto in data 09/12/2013 col numero 1277A22 e precedentemente adottato con determinazione del Dirigente dell'1 settembre 2011.
L'originale del presente documento viene custodito presso l'Amministrazione Scolastica, per essere esibito in caso di controlli.

Il Titolare del trattamento
IL DIRIGENTE SCOLASTICO
(Dr.ssa Giuseppina FUSCO)