

DIREZIONE DIDATTICA STATALE

1° CIRCOLO

Via Anna Botto, 2 – 27029 VIGEVANO – Tel . 0381/20034 – Fax 0381/312973
e-mail: pvee03400a@istruzione.it

Prot. n. /A15B

Vigevano, 1 ottobre 2010

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI

(D. L.vo 196 del 30/06/03)

PREMESSA

La Direzione Didattica Statale 1° Circolo con sede in Vigevano – Via Anna Botto 2 – C.F. 85005240180, nella persona del suo legale rappresentante pro tempore D.Sc. dott. Maria Bonecchi(C.F. BNCMRA55B57A010D) ha redatto il seguente Documento Programmatico per la Sicurezza ai sensi e per gli effetti dell'art. 34 comma 1, lettera g) del D. L.vo n. 196/2003 e del disciplinare tecnico allegato al medesimo sub B “Disciplinare tecnico in materia di misure minime di sicurezza”, nonché della “Guida operativa per redigere il documento programmatico” pubblicata sul sito web del Garante.

Scopo del presente documento, di seguito denominato “DPS” è quello di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logistiche, secondo la descrizione e gli opportuni allegati, che fanno parte integrante del Documento, che saranno adottate da questa Istituzione Scolastica relativamente al trattamento dei dati personali, per le rispettive competenze, da parte del DSGA, degli Assistenti Amministrativi, del Personale Docente e dei Collaboratori Scolastici.

ARTICOLO 1 – RIFERIMENTI NORMATIVI

Legge 31/12/1996 n. 675 e successive modifiche;

Legge 31/12/1996 n. 676, recante delega al governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

DPR 28/07/1999, n. 318 – Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali;

Legge 24/03/2001 n. 127, recante delega al governo per l'emanazione di un T. U. in materia di trattamento dei dati personali;

Decreto legislativo 30/06/2003 n. 196 – Codice in materia di protezione dei dati personali, in particolare:

- degli articoli da 28 a 30 (Soggetti che effettuano il trattamento);
- degli articoli dal 31 al 36 (Misure di sicurezza);
- degli articoli 59 e 60 (Disposizioni relative a specifici settori – Trattamento in ambito pubblico);
- degli articoli 95 e 96 (Disposizioni relative a specifici settori – Istruzione);
- dell'articolo 180 (Disposizioni transitorie – Misure di sicurezza);
- dell'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza);

Per “definizioni” si rispettano quelle riportate all'art. 4 del D.L.vo 196/2003.

ARTICOLO 2 – OBIETTIVI DEL DOCUMENTO

Il “DPS”, redatto in ottemperanza a quanto disposto dal D.L.vo 196/2003 (Codice in materia di protezione dei dati personali) mira a regolamentare e garantire la riservatezza, la sicurezza e la protezione dei dati personali in possesso del 1° Circolo Didattico di Vigevano, nonché a porre in atto idonee strategie per la protezione delle aree e dei locali interessati a misure di sicurezza.

Il Documento garantisce che il trattamento dei dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Il tutto è disciplinato in modo da assicurare un elevato livello di tutela dei diritti e delle libertà di cui al c. 1 del presente articolo nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte del titolare del trattamento (art. 2 D.L.vo 196/2003). Ai sensi dell'art.1 del D.L.vo: “Chiunque ha diritto alla protezione dei dati personali che lo riguardano”.

Tali dati riguardano:

- Il personale che presta servizio presso l'istituzione scolastica;
- Gli alunni che frequentano questa Scuola;
- I genitori degli alunni o gli esercenti la potestà familiare per le notizie che trasmettono o portano a scuola;
- I fornitori.

In particolare, nel “DPS” vengono definiti i criteri tecnici e organizzativi per:

- a) la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ad accedere ai medesimi locali;
- b) i criteri e le procedure per assicurare l'integrità dei dati;
- c) i criteri e le procedure per la sicurezza della trasmissione dei dati, cartacei o telematici;
- d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati e dei modi per prevenire gli eventi dannosi.

ARTICOLO 3 – CAMPO DI APPLICAZIONE

1. Il “DPS” definisce le politiche e gli standard di sicurezza in merito ai dati da garantire e proteggere. Tali dati si distinguono in:
 - **dati personali comuni** (dati anagrafici o identificativi delle persone, indirizzi, recapiti telefonici, codici fiscali, dati bancari, informazioni circa la composizione familiare, la professione esercitata da un determinato soggetto, la sua formazione etc.);
 - **dati sensibili** (dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute, appartenenza a categorie protette, portatore di handicap, stato di gravidanza , vita sessuale etc.);
 - **dati giudiziari** (provvedimenti sul casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato o dei relativi carichi pendenti, la qualità di imputato o indagato ai sensi degli artt. 60 o 61 del Codice di Procedura Penale,avviso di garanzia, separazioni, affidamento dei figli, etc.).
2. I trattamenti sono realizzati prevalentemente negli uffici di direzione e segreteria, nell' archivio della sede centrale, nelle aule scolastiche ove sono conservati, durante l'anno scolastico, i registri degli alunni di classe, il giornale dell'insegnante, l'agenda per la programmazione didattica, i documenti di valutazione e i portfolio degli alunni che saranno meglio individuati nell'opportuna sezione di questo DPS.
3. I dati sono trattati con fascicoli e atti cartacei e con strumenti elettronici di elaborazione. Per i dati sensibili si garantiranno maggiori misure di riservatezza con fascicolazione a parte, con eventuale cifratura o individuando criteri per criptare i dati stessi.
4. Il Responsabile e gli Incaricati di effettuare il trattamento dei dati utilizzano i fascicoli cartacei e i personal computer in dotazione degli uffici.
5. I computer degli uffici di segreteria sono collegati in rete e ad internet, così come ad internet è collegato il computer dell'ufficio di direzione.
6. Gli Incaricati che hanno accesso ad atti e documenti informatici degli uffici sono forniti di password personali e utilizzano codici identificativi. Tali password sono adeguatamente custodite in buste chiuse dal Responsabile in luogo sicuro.

ARTICOLO 4 – SOGGETTI CHE EFFETTUANO IL TRATTAMENTO PER LA PROTEZIONE DEI DATI PERSONALI

Il D.L.vo 196/2003 sulla protezione dei dati personali individua all'art. 4 i soggetti che sono coinvolti nel trattamento dei dati personali:

- **il titolare:** la persona fisica e giuridica cui compete la responsabilità finale ed assume decisioni fondamentali riferite alle modalità di trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- **il responsabile:** la persona fisica, dotata di particolari caratteristiche di natura morale e di competenza tecnica, con precise capacità ed affidabilità, preposta dal titolare al trattamento dei dati personali, ivi compreso il profilo della sicurezza;
- **gli incaricati:** le persone fisiche autorizzate a compiere operazioni di trattamento e che materialmente provvedo al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile;
- **l'amministratore di sistema:** il soggetto cui è conferito il compito di “sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base di dati e di consentirne l'utilizzazione”. Tale figura è individuata dall' art. 1 del DPR 318/99, mentre non viene riproposta nel D.L.vo 196/2003 che pur conserva una propria funzionalità per la garanzia delle misure di sicurezza logica del sistema informatico della gestione dei dati. Pertanto si ravvisa la necessità di individuare tale figura con delega di compiti definiti.

1 - **IL TITOLARE DEL TRATTAMENTO** (art. 28 D.L.vo 196/2003)

Titolare del trattamento, come definito nella Premessa, è il legale rappresentante pro tempore di questa Istituzione Scolastico, D.Sc. dott. Maria Bonecchi.

E' onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino e garantiscano che vengano adottate le misure di sicurezza.

Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita dei dati medesimi, anche accidentale, l'accesso non autorizzato o il trattamento non consentito, previe istruzioni fornite per iscritto (art. 31 D.L.vo 196/2003).

2 - **RESPONSABILE DEL TRATTAMENTO IL** (art. 29 D.L.vo 196/2003)

In relazione all'attività del Titolare del trattamento, è prevista la nomina di uno o più Responsabili del trattamento, con compiti diversi a seconda delle funzioni svolte.

Il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare (art. 29 c. 4 D. L.vo 196/03). Il Titolare del trattamento affida al Responsabile del trattamento l'onere di individuare, nominare ed indicare per iscritto gli Incaricati del trattamento.

In particolare, **il Titolare del trattamento individua, designa e nomina quale Rappresentante del trattamento dei dati il DSGA Patrizia Rogna**, persona con capacità professionali, esperienza e affidabilità, tale da fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

Il Responsabile del trattamento dei dati ha il compito di:

- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete, nonché l'elenco delle tipologie dei trattamenti effettuati;
- Attribuire ad ogni utente (User) o Incaricato un codice identificativo personale (User-id) per l'utilizzazione dell'elaboratore;
- Verificare con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali;
- Informare il Titolare nella eventualità che si siano rilevati dei rischi.

Altresì al Responsabile del trattamento dei dati è affidato il compito di **gestire e custodire le password** per l'accesso ai dati da parte degli Incaricati. Egli predisponde, per ogni Incaricato del trattamento, una busta sulla quale è indicato lo USER-ID utilizzato: all'interno della busta deve essere indicata la password utilizzata dall'Incaricato per accedere alla banca-dati.

Le buste con le password debbono essere conservate in luogo chiuso e protetto (nell'armadio blindato dell'ufficio riunioni del DS)

Il Titolare del trattamento dei dati informa il Responsabile sulle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore fornendogli una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile del trattamento è a tempo indeterminato, decade per revoca in qualsiasi momento o con il venir meno dei compiti che giustificavano il trattamento.

3 - **GLI INCARICATI DEL TRATTAMENTO** (art. 30 D.L.vo 196/2003)

Ai Responsabili del trattamento è affidato il compito di nominare, con comunicazione scritta, gli Incaricati del trattamento dei dati.

La designazione di ciascun Incaricato del trattamento dei dati deve essere effettuata con lettera di incarico in cui sono ben specificati i compiti che gli sono affidati e l'ambito del trattamento consentito.

Gli Incaricati del trattamento devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli Incaricati deve essere assegnata una parola chiave e un codice identificativo personale.

La nomina degli Incaricati del trattamento deve essere controfirmata dall'interessato per presa visione.

In particolare, tenuto conto del piano di lavoro e delle attività predisposto dal DSGA per il corrente anno scolastico e adottato dal D.S., **il Responsabile del trattamento individua e nomina i seguenti Incaricati con annesso ambito del trattamento dei dati consentito:**

SETTORE SERVIZI DI AMMINISTRAZIONE ALUNNI E SUPPORTO ALLA DIDATTICA		
N. 1 incaricato	FUNZIONI AMMINISTRATIVE	OGGETTO
Perin Elena	Assistente amministrativo	Iscrizioni e verifica frequenza alunni, predisposizione fascicolo, rilascio nulla osta e trasmissione fascicoli.
		Gestione fascicoli alunni H, predisposizione convocazione Gruppo di lavoro.
		Organici
		Gestione adozione libri di testo, predisposizione cedole librarie
		Statistiche relative agli alunni e all'edilizia scolastica
		Gestione infortuni alunni

SETTORE SERVIZI DI AMMINISTRAZIONE DEL PERSONALE		
N. 1 incaricato	FUNZIONI AMMINISTRATIVE	OGGETTO
Armiento Maria	Assistente amministrativo	Gestione fascicoli, rilascio certificati, gestione assenze, gestione della carriera, predisposizione atti personale in quiescenza
		Gestione graduatorie di istituto
		Stipula contratti a tempo determinato
		Acquisizione documentazione personale supplente

SETTORE SERVIZI CONTABILI		
N. 1 incaricato	FUNZIONI AMMINISTRATIVE	OGGETTO
Patrizia Rogna	DSGA	Acquisizione dati stipula contratti a t.i.
		Stipendi al personale con contratto a t.d.
		Liquidazione compensi accessori e indennità
		Versamento ritenute e contributi
		Dichiarazioni e conguaglio fiscale
		Rilascio certificazioni (disoccupazione, CUD)
		Contabilità bilancio ecc.

SETTORE SERVIZI AFFARI GENERALI		
N. 1 incaricato	FUNZIONI AMMINISTRATIVE	OGGETTO
ORLANDI Raffaella	Assistente amministrativo	Alunni (aiuto nella predisposizione degli atti)
		Progetti di istituto
		Rapporti con Enti locali
		Diffusione circolari interne
		Protocollo, corrispondenza in uscita, archiviazione atti.

SETTORE SERVIZI DI AMMINISTRAZIONE ALUNNI E PERSONALE		
N. 1 incaricato	FUNZIONI AMMINISTRATIVE	OGGETTO
BUCONTE Stefania	Assistente amministrativo	Gestione beni patrimoniali – informatica-
		Alunni (collaborazione con Bocca)
		Personale (collaborazione con Armiento)
		Dichiarazione dei servizi

SETTORE SERVIZI AFFARI GENERALI		
N. 1 incaricato	FUNZIONI AMMINISTRATIVE	OGGETTO
Fluidi Piera	Assistente amministrativo	Gestione rapporti con enti, segnalazione guasti
		Collaborazione gestione fascicoli alunni
		Collaborazione gestione fascicoli personale
		Elezioni scolastiche, detrazioni fiscali

TUTTI I COLLABORATORI SCOLASTICI:

nei loro specifici incarichi o nelle loro mansioni generali previste dal CCNL nell'area specifica di appartenenza (accoglienza e sorveglianza nei confronti degli alunni, ausilio materiale nei confronti degli alunni in situazione di difficoltà, custodia e sorveglianza nei locali scolastici, vigilanza nei confronti del pubblico evitando ed inibendo l'intrusione di persone estranee, collaborazione con i docenti e con il personale di segreteria, pulizia dei locali) osserveranno la massima privacy, evitando di diffondere notizie che devono restare private, in particolare quando ricevono o portano in giro Circolari Ministeriali, Note degli Uffici Superiori o circolari interne in visione al personale docente.

Tale personale deve ricevere idonee ed analitiche informazioni da parte del Responsabile del trattamento sulle mansioni loro affidate e sugli adempimenti cui sono tenuti in ragione della riservatezza che si deve per l'incarico affidato e per il fatto di essere dipendenti di questa pubblica istituzione scolastica.

Agli Incaricati del trattamento il Responsabile consegnerà una copia della normativa che riguarda la sicurezza del trattamento dei dati in vigore al momento della nomina. Tale nomina è a tempo indeterminato, decade per revoca, o con il venir meno dei compiti che giustificavano il trattamento.

– AREA DOCENTI

- **Inss. Enrica Rossin** (C.F. RSSNRC63M66L872E) e **Laura Gregorio**. (C.F. GRGLMR60T51D901V) – **Ambito di supporto al D.S.:**

- L'INS. Enrica Rossin coordina il plesso Ramella; è incaricata di sostituire il D.Sc. per brevi assenze con delega alla firma; è referente per l'organizzazione dei problemi relativi all'utenza, ai rapporti con i genitori e con gli enti esterni; vigila sulla puntualità degli insegnanti; accede ai dati trattati dai docenti di scuola primaria.
- L'INS. Laura Gregorio. è incaricata di sostituire il D.Sc. quando contemporaneamente è assente la collaboratrice l'Ins. ROSSIN ENRICA, coordina i plessi di scuola dell'infanzia, accede ai dati degli alunni di scuola dell'infanzia, è referente per l'organizzazione dei problemi relativi all'utenza ai rapporti con genitori e con enti esterni.

- Ins. Tiozzo Deborah(CFTZZDRH71A68L872K) - **Ambito di competenza:** incaricata della gestione del laboratorio d'informatica, assicura il corretto uso dei sistemi, dei programmi, d'Internet, della tenuta in ordine di tutto il materiale e dei software. Tra i suoi compiti, oltre che organizzare un organigramma per l'accesso delle classi nel laboratorio, inibiranno i siti di Internet indesiderati utilizzando quanto necessario per il conseguimento del fine con l'utilizzo di filtri presenti sul mercato (SmartFilter), pur con i limiti che questi inevitabilmente presentano. Il filtro è un sistema automatico che limita l'accesso ad Internet, escludendo la possibilità di collegarsi a siti Web di contenuto non desiderato o pornografico.

Il laboratorio di informatica è finalizzato:

- Ad attività didattiche con intere classi o gruppi di alunni
- A corsi di aggiornamento per docenti e personale ATA
- Ad aggiornamento individuale dei docenti per acquisire la formazione di base sulle TIC.

Gli alunni saranno sempre accompagnati da un insegnante che sarà garante e direttamente responsabile dell'utilizzo del laboratorio.

Alla porta di accesso del laboratorio, gli incaricati apporranno una scheda in cui l'utente segnalerà l'inconveniente hardware o software verificatosi nell'utilizzo del p.c., avvertendo contemporaneamente i responsabili di laboratorio o l'Amministratore di sistema.

E' compito specifico degli Incaricati garantire il buon funzionamento dei sistemi presenti in laboratorio e la gestione del materiale di consumo, delle richieste di assistenza tecnica, nonché dell'inventario del laboratorio.

Al di fuori del normale orario di utilizzo, il laboratorio deve rimanere chiuso a chiave: questa viene custodita da un collaboratore scolastico individuato dal Responsabile del trattamento dei dati. I docenti interessati possono fare richiesta verbale della chiave direttamente alla suddetta persona avendo cura, al termine, di restituirla alla stessa.

L'Istituto possiede un sito web accessibile da Internet ove sono pubblicati i documenti prodotti dalla scuola (POF – Progetti in sintesi), è possibile inserire delle news o eventi salienti a cura dell'insegnante Deborah Tiozzo. Sul sito sono altresì pubblicati i nominativi del personale dipendente, privi di tutti i dati personali, per tutto ciò quanto prima (a inizio dell'anno scolastico) saranno acquisite le liberatorie.

- **DOCENTI DI SCUOLA DELL'INFANZIA E DI SCUOLA PRIMARIA** a tempo indeterminato o determinato e tutte le altre unità di personale che a qualunque titolo hanno rapporto di lavoro anche occasionale (stipule di contratti o convenzioni) con l'Istituzione Scolastica eviteranno di diffondere notizie che resteranno segrete sia per quanto attiene i dati personali comuni, sia per i dati sensibili che hanno acquisito in virtù del loro ufficio.

Il docente, per la sfera di competenza, rientra nell'ambito degli incaricati sia per le categorie di dati cui può accedere, sia per la tipologia di trattamento e vincoli specifici ai sensi dell'art. 4 del D.L.vo 196/2003, sia per le istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi. I dati trattati dai docenti si rinvergono nei registri dei verbali degli OO.CC., nei registri di classe, dell'insegnante, di modulo per la programmazione, d'intersezione e d'interclasse, nei documenti di valutazione, nelle diagnosi funzionali per la situazione di handicap, nelle assenze degli alunni, in eventuali certificati medici, etc. Il trattamento dei dati da parte dei docenti è definito puntualmente da norme di legge.

Tale personale riceverà specifica informazione/formazione da parte del Titolare del trattamento circa gli specifici doveri e gli adempimenti cui sono tenuti in ragione del loro ufficio, della riservatezza che si deve ai dati che trattano per il fatto di essere dipendenti di questa pubblica istituzione scolastica.

4) **L' AMMINISTRATORE DI SISTEMA** (art. 1 DPR 318/99)

L'Amministratore di Sistema garantisce la tutela e il corretto uso dei sistemi informatici e delle banche-dati in essa contenuti.

Dato l'elevato utilizzo delle strumentazioni informatiche, il Titolare del trattamento ritiene opportuno conferire la nomina di Amministratore di Sistema al DSGA Patrizia Rogna, in quanto persona capace, idonea, esperta nell'utilizzo dei sistemi informatici e dei relativi programmi

In particolare l'Amministratore di Sistema:

- Si identifica con il Responsabile del trattamento dei dati;
- rispetta le misure di sicurezza previste dalla legge e specificate nel DPS;
- garantisce la massima riservatezza nel trattamento dei dati;
- L'Amministratore di Sistema, l'Responsabile del trattamento dei dati:
- prende tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvede al ricovero periodico degli stessi con copie di back up;
- si assicura della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro (cassaforte del DS);
- fa in modo che sia prevista la disattivazione dei Codici identificativi personali (User-id), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali (User-id) per oltre 6 mesi;
- protegge gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

ARTICOLO 5 - DIRITTI DELL' INTERESSATO

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, come pure l'aggiornamento, la rettifica o, quando vi ha interesse, l'integrazione dei dati.

L'interessato ha altresì diritto di richiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge.

I dati saranno resi noti solo ai diretti interessati e a persone, enti e organismi che per legge sono titolari a ricevere i dati stessi.

Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali (D.L.vo 196/2003). Pertanto per adempiere ai doveri d'ufficio, a disposizioni normative, a precisi obblighi di circolari non si richiede il consenso dell'interessato nell'invio di dati a persone od organismi titolari per legge a ricevere i dati stessi.

I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato.

ARTICOLO 6 - ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

1) Le situazioni dei rischi che incombono sui dati possono riguardare:

- Dati su materiale cartaceo;
- Dati su attrezzature informatiche;
- I luoghi e i contenitori che custodiscono sia i materiali cartacei, sia le attrezzature informatiche.

2) I materiali cartacei a rischio sono:

- Raccoglitori e faldoni che raccolgono i documenti contenuti nei fascicoli del personale;
- Schede personali degli alunni;
- Registri (di classe, di modulo, giornale dell'insegnante, di presenza);
- Registro dello stato del personale;
- Decreti e certificati sulle persone;
- Anagrafe fornitori;
- Contratti e convenzione;
- Documentazione finanziaria e contabile;
- Registro infortuni;
- Moduli di iscrizione, istanze, etc
- Atti affissi agli albi.

4) I dati informatici a rischio sono quelli contenuti nei documenti di cui al comma 2 del presente articolo e immessi nei personal computer degli uffici.

5) Gli eventi che possono generare danni e che comportano rischi per la sicurezza dei dati personali si distinguono sotto un triplice aspetto:

a. Comportamento degli operatori:

- Sottrazioni di credenziali di autenticazione;
- Carenza di consapevolezza, disattenzione o incuria;
- Manomissioni e comportamenti sleali o fraudolenti;
- Errore materiale;

b. Eventi relativi agli strumenti:

- Azione di *virus* informatici o di programmi suscettibili di recare danno;
- Spamming, tecnica di sabotaggio o posta spazzatura: vettore attraverso il quale si fanno circolare virus e codici maligni di ogni tipo con l'obiettivo di compromettere il funzionamento dei computer a catena e rendere al contempo più difficile il tracking, cioè l'individuazione da parte delle forze di polizia preposte al compito di garantire la sicurezza della società dell'informazione, ma è altresì piaga planetaria e veicolo per vendere software contraffatti, in una sorta di e-commerce illegale;
- Hacker: persona che utilizza la sua abilità informatica in modo fraudolento con lo scopo di elaborare un virus o penetrare in una rete di computer protetta;
- Malfunzionamento, indisponibilità o degrado degli strumenti;
- Accessi esterni non autorizzati;
- Intercettazioni di informazioni in rete;

c. Eventi relativi al contesto fisico-ambientale:

- Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, etc.), nonché dolosi, accidentali o dovuti ad incuria;
- Accesso di estranei o persone non titolari di incarichi e responsabilità nel trattamento dei dati
- Errori umani nella gestione della sicurezza fisica.
- Accessi esterni non autorizzati;
- Vandalismo;
- Intercettazioni di informazioni in rete;
- Sottrazione di strumenti contenenti dati;
- Guasto ai sistemi complementari (impianto elettrico, gruppo di continuità, climatizzazione, etc.).

ARTICOLO 7 – MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI, NONCHE' LA PROTEZIONE DELLE AREE E DEI LOCALI

1) MISURE DA ADOTTARE

Al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità, sono state adottate le seguenti misure:

- Individuazione e nomina del responsabile del trattamento dei dati (per l'accesso ai computer e alla rete si richiede autenticazione, identificazione e password per ogni Incaricato);
- Individuazione del Responsabile per garantire tutte le misure di sicurezza predisposte per la conservazione e utilizzazione dei dati,
- Misure di prevenzione per eliminare gli eventuali incendi con adeguate modalità di gestione degli stessi (impianto elettrico a norma, idranti (ove disposti), estintori, etc.);
- Individuazione dei locali e contenitori (armadi, armadi di sicurezza, armadi blindati, classificatori con serrature, apparecchiature e strumenti di raccolta dei dati adeguati e sicuri, etc.);
- Regolamentazione sia per il personale che per gli esterni nell'accesso ai locali e alle attrezzature che conservano dati, archivi e documentazione,
- Attuazione di misure di protezione attiva e passiva dei locali (porte con serrature di sicurezza, inferriate, archivio, sistemi di allarme ove collocati, adeguate misure antincendio con raccolta di materiali in locali protetti da porte specifiche di sbarramento);
- Trasposizione dei dati informatici su minidisk su materiale stampato;
- Periodico salvataggio dei dati del server su unità rimovibili (i-o megazip).

- Periodicamente (almeno ogni tre mesi) verificare la funzionalità e l'efficienza delle misure di protezione e delle strutture operative che ne hanno la responsabilità, anche mediante la compilazione di apposite schede di monitoraggio.
- Installazione di Firewall sul server al fine di impedire ingressi di pirati o intercettazioni sulla rete informatica di questa istituzione scolastica con la configurazione di password e impostazione di tutte le misure di sicurezza necessari

2. CRITERI, PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI

Il Responsabile del trattamento, Amministratore di Sistema, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.

In particolare per ogni banca di dati devono essere definite le seguenti specifiche:

- Il tipo di supporto da utilizzare per le copie di back-up;
- Il numero di copie di back-up effettuate ogni volta;
- Verificare se i supporti utilizzati per le copie di back-up sono riutilizzati e in questo caso con quale periodicità;
- Concordare preventivamente se per effettuare le copie di back-up si utilizzino procedure automatizzate e programmate;
- Trasporre i dati informatici contenuti in minidisk, su materiale stampato;
- Valutare la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- Assegnare il compito periodico di effettuare le copie di back-up agli Incaricati del trattamento.

3. CUSTODIA E CONSERVAZIONE DELLE COPIE DI BACK-UP

Le copie di back-up devono essere adeguatamente conservate a cura del Responsabile del trattamento nell'armadio blindato sito in segreteria. Tali siti di custodia delle copie di back-up devono essere protetti da:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni ed atti vandalici
- Incendio
- Allagamento
- Furto
- Condizionamento ambientale
- Impianti elettrici a norma e gruppi di continuità

L'accesso ai supporti utilizzati per il back-up dei dati è limitato:

- Al Titolare del trattamento
- Al Responsabile del trattamento della sicurezza dei dati/Amministratore di sistema
- Agli Incaricati

Quando il Responsabile del trattamento, Amministratore di Sistema, decide che i supporti magnetici utilizzati per le copie di back-up delle banche- dati non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando le informazioni in esso contenute.

4. PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita degli stessi a causa di virus informatici, il Responsabile del trattamento dei dati, Amministratore di sistema, stabilisce quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Il Responsabile del trattamento stabilisce inoltre la periodicità, con cui devono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza dei dati trattati

E' consigliabile che gli Incaricati che utilizzano i sistemi informatici annotino gli eventuali virus rilevati, e, se possibile, la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezioni o contagio da virus, il Responsabile del trattamento, unitamente all' Amministratore di Sistema, deve provvedere a:

- Isolare il sistema

- Verificare se ci sono altri sistemi infettati con lo stesso virus informatico
- Identificare l'antivirus adatto e bonificare il sistema infetto
- Installare l'antivirus adatto su tutti i sistemi
- Compilare un modulo di "Report dei contagi da virus informatici"
- Conservare in luogo sicuro a cura del Responsabile del trattamento i moduli compilati.

5.PROTEZIONE DELLE AREE E DEI LOCALI

a) **Sicurezza di area**

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze nello svolgimento dei servizi. Le contromisure si riferiscono alla protezione perimetrale dei siti, ai controlli fisici all'accesso, alla sicurezza degli archivi e delle attrezzature informatiche rispetto ai danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

L'edificio scolastico dove ha sede la Direzione (o presidenza) perimetralmente è protetto da inferriate. Tutte le scuole sono dotate di impianto elettrico a norma e di appositi estintori.

Si precisa inoltre che:

- nessuno accede all'archivio se non autorizzato
- i fascicoli prelevati dall'archivio permangono al di fuori del sito per il tempo strettamente necessario e successivamente vengono riposti al proprio posto
- gli incaricati accedono ai soli dati personali la cui conoscenza sia strettamente necessaria per evadere una pratica
- i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono essere conservati e custoditi con le necessarie precauzioni.

ARTICOLO 8 – CRITERI E MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

- 1) Per prevenire e diminuire i danni causati da danneggiamenti, smarrimenti, inaffidabilità della base dati:
 - a) per i dati cartacei si potrà ricostruire copia da documenti e atti in possesso degli interessati (personale in genere) o di altri enti cui sono stati trasmessi (Scuole, MIUR, Ufficio Scolastico Regionale, CSA, ASL, Comune);
 - b) per i dati informatici si potranno ricostruire i dati danneggiati ricavando gli stessi da atti documenti "stampati" o si potranno riportare in via precauzionale su dischetti custoditi in luoghi fisici diversi i dati contenuti negli archivi informatici fissi.
- 2) Ogni Incaricato della gestione di dati avrà l'accortezza di effettuare periodicamente il salvataggio dei dati su dischetti custoditi dallo stesso.
- 3) Il Responsabile del trattamento, d'intesa con gli Incaricati di collaborare nell'Amministrazione di Sistema, ha il compito di verificare di sovente o almeno ogni sei mesi la situazione dei Sistemi operativi installati sulle apparecchiature con le quali vengono trattati i dati. La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda:

La sicurezza dei dati trattati

- Il rischio di distruzione o di perdita dei dati
- Il rischio di accesso non autorizzato o non consentito
- Ad evitare danneggiamento o perdita di dati si rende estremamente importante:
- La disponibilità delle versioni più avanzate dei Sistemi Operativi utilizzati
- La segnalazione di Fix o System-Pack per la rimozione di errori o malfunzionamenti
- La segnalazione di Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione, di danneggiamento o distruzione dei dati
- Nel caso esistano evidenti rischi sui Sistemi operativi, l'Amministratore di sistema, Responsabile, informano il Titolare perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore ad evitare che possano essere smarriti, danneggiati o distrutti.

ARTICOLO 9 – INTERVENTI FORMATIVI PER GLI INCARICATI DEL TRATTAMENTO

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno i bisogni formativi di cui necessitano gli Incaricati, specie per le innovazioni che nel campo telematico/tecnologico/informatico

avvengono di continuo. E' necessario tenere il personale in tale campo continuamente informato e all'altezza dei compiti che devono espletare, per meglio conoscere i rischi che incombono sui dati, per avere una ottimale conoscenza delle misure di sicurezza e degli adeguati comportamenti da adottare, delle responsabilità circa i dati danneggiati, persi o distrutti.

Gli interventi formativi sono particolarmente opportuni al momento dell'ingresso in servizio di personale nuovo, per immissione in ruolo o per trasferimento, in occasione dell'adozione di nuovi strumenti o dell'installazione di altri software. E' opportuno documentare gli interventi formativi.

Una adeguata informazione/formazione va data a cura, sempre del Responsabile, anche ai collaboratori scolastici.

Parimenti una informazione/formazione va estesa e organizzata dal Titolare del trattamento nei confronti del personale docente.

Gli interventi formativi atterranno sulle disposizioni applicative del D. L.vo 196/2003.

Le varie tipologie di corsi di formazione potranno essere effettuati singolarmente da questa Istituzione Scolastica o in rete con altre Scuole.

Per gli Incaricati del trattamento un corso si rende urgente immediatamente dopo l'affidamento dei compiti e delle responsabilità e comunque entro il primo semestre di ciascun anno scolastico.

Sarà messo a disposizione del personale il D. L vo 196/2003.

ARTICOLO 10 – NORME FINALI

Il "DPS" potrà essere integrato e aggiornato in qualunque periodo dell'anno, ma almeno entro il 31 ottobre di ogni anno.

Per quanto non regolamentato nel presente DPS si applicano le norme contenute nel D.L.vo 196/2003 e dallo stesso richiamate.

Il D.S. – titolare del trattamento dei dati - si impegna ad adottare, nella fase di graduale attuazione degli interventi previsti dalla normativa sulla tutela della privacy, ogni possibile misura destinata a salvaguardare la sicurezza dei dati personali, siano essi contenuti nei documenti cartacei che registrati mediante strumenti elettronici. Tali misure riguarderanno gli aspetti organizzativi, logistici e procedurali miranti ad evitare con ogni mezzo qualsiasi incremento di rischi di distruzione o perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito. Il presente documento verrà portato all'attenzione della Giunta Esecutiva e del Consiglio di Circolo, con gli opportuni adeguamenti che deriveranno dalla verifica annuale dell'assegnazione degli incarichi e delle specifiche competenze, come previsto dall'allegato B, n. 26 sul Disciplinare tecnico in materia di misure minime di sicurezza, per riferire sulla sua avvenuta redazione con data certa, per informazione ai componenti, per adozione ed assunzione di delibera, anche al fine di porre il Titolare in grado di attuare gli adeguamenti fisici, logistici, tecnologici ed informatici urgenti e necessari per le finalità previste dalla legge.

IL TITOLARE DEL TRATTAMENTO DATI