# ISTITUTO COMPRENSIVO CARMAGNOLA II

✉VIA Marconi, 20 - 10022 CARMAGNOLA
☎ 011/9771020
toic8ap00r@istruzione.it - toic8ap00r@pec.istruzione.it
**Cod. Mec.: TOIC8AP00R – Cod. Fiscale: 94067040017**


**Prot. n° 1247/A19** **Carmagnola, 22 ottobre 2012**

# D. P. S.
# Documento Programmatico sulla Sicurezza dei Dati Personali
# (D. L.vo 196 del 30/06/03)

## Aggiornamento al 08.11.2013 per adeguamento operatori e variazione mail.

**Prot. n° 6551/A19** **Carmagnola, 08 novembre 2013**

## Aggiornamento al 30.09.2014

**Prot. n° 5876/A19** **Carmagnola, 30 settembre 2014**

**PREMESSA**

L'Istituto Comprensivo Carmagnola 2 con sede centrale in via Marconi, 20 Carmagnola, C.F. 94067040017, nella persona del Dirigente Scolastico Rosalinda Rambaldi, C.F. RMBRLN54H67I138L, 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 informare l'utenza e i lavoratori delle misure di sicurezza che saranno adottate da questa Istituzione Scolastica relativamente al trattamento dei dati personali

**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);

Decreto Ministeriale n° 305 del 7/12/2006- Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione;
Nota "La privacy a scuola. Dai tablet alla pagella elettronica." Garante per la privacy.
Per "definizioni" si rispettano quelle riportate all'art. 4 del D.L.vo 196/2003 cui si rimanda.

**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 dell'Istituto Comprensivo Carmagnola 2 di Carmagnola, 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 questo Istituto;
- 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:

- 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;
- i criteri e le procedure per assicurare l'integrità dei dati;
- i criteri e le procedure per la sicurezza della trasmissione dei dati, cartacei o telematici;
- 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 negli uffici di direzione e segreteria, nell' archivio della sede centrale, nelle aule scolastiche/plessi 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 fascicoli degli alunni sono custoditi in appositi armadi nell'ufficio di segreteria e di presidenza.

3. I dati sono trattati con fascicoli, 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 del 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 interna e alla rete internet; su tutte le postazioni e sul server è attivo e costantemente aggiornato un software antivirus.
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 (o suo delegato) in luogo sicuro.

**Articolo 4**
***Soggetti che effettuano il trattamento 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:
1. **il titolare** è 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;
2. **il responsabile** è 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;
3. **gli incaricati** sono le persone fisiche autorizzate a compiere operazioni di trattamento e che materialmente provvedono al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile;
4. **l'amministratore di sistema** è 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 ha una propria funzionalità per la garanzia delle misure di sicurezza logica del sistema informatico per la 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 Dirigente Scolastico Rosalinda Rambaldi**. 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 IL RESPONSABILE DEL TRATTAMENTO (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 e nomina quale **Responsabile del trattamento dei dati il DSGA di questa Istituzione Scolastica, Signora Giuseppa Tassone,** persona con inquadramento professionale e ruolo tale da dover 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; di attribuire ad ogni utente (User) o Incaricato un codice identificativo personale (User-id)

per l'utilizzazione dell'elaboratore; di verificare, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali; di informare il Titolare nella eventualità che si siano rilevati dei rischi. Inoltre 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 predispone, 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. Il Responsabile può delegare la gestione e custodia delle password.
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)
Al Responsabile 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, che per funzione lavorano su postazioni informatiche, 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 predisposte dal DSGA per il corrente anno scolastico e adottato dal D.S., il Responsabile del trattamento individua e nomina gli Assistenti Amministrativi in servizio (ed eventuali supplenti) Incaricati del trattamento dei dati:

| Operatore | Funzioni e Compiti |
|---|---|
| **DSGA** | **Gestione e coordinamento delle pratiche d'ufficio**<br>con la collaborazione degli assistenti amministrativi individuati e formati al bisogno |
| **Assistenti Amministrativi** | **gestione alunni**<br>informazione utenza interna ed esterna, iscrizioni alunni, tenuta fascicoli documenti alunni, richiesta o trasmissione documenti, gestione corrispondenza con le famiglie, gestione statistiche, gestione pagelle, diplomi, tabelloni scrutini, gestione assenze e ritardi, gestione e procedure per sussidi, gestione organizzativa viaggi d'istruzione, certificazione varie e tenuta registri, esoneri educazione fisica, infortuni alunni, libri di testo, pratiche portatori di handicap, collaborazione docenti funzioni strumentali per monitoraggio relativi agli alunni, esami di stato e ogni altra pratica inerente l'area e la funzione. |
| | **amministrazione del personale**<br>tenuta fascicoli personali di tutto il personale dell'Istituto, richiesta e trasmissione documenti, emissione contratti di lavoro, compilazione graduatorie supplenze, compilazione graduatorie soprannumerari docenti ed A.T.A. , registro certificati di servizio, convocazioni attribuzione supplenze, certificati di servizio, ricostruzioni di carriera, pratiche pensioni, visite fiscali, aggiornamento assenze e presenze personale con emissione decreti congedi ed aspettative, rilascio cud, certificati inps, rapporti dpt registro decreti, pratiche cause di servizio, anagrafe personale, autorizzazione libere professioni, preparazione documenti periodo di prova, controllo documenti di rito all'atto dell'assunzione, aggiornamento graduatoria, funzioni aggiuntive A.T.A. e ogni altra pratica inerente l'area e la funzione. |

| | |
|---|---|
| | **archivio protocollo area e progetti didattici gestione beni patrimoniali e contabilità di magazzino**<br>Ricevimento posta (cartacea e elettronica), tenuta registro protocollo, tenuta e controllo pratiche relative a tutti i progetti da realizzare, convocazione organi collegiali, pubblicazioni all'albo istituto, distribuzione modulistica varia personale interno, gestione circolari interne, pratiche per assemblee sindacali, inoltro comunicazioni verso l'esterno, tenuta dei registri di magazzino, emissione dei buoni d'ordine, acquisizione richieste d'offerte, carico e scarico materiale, redazione di preventivi, pratiche contabili, pratiche di verifica di regolarità contabile e qualunque altra pratica inerente il protocollo, la gestione dei beni e la contabilità e ogni altra pratica inerente l'area e la funzione. |
| | **gestione finanziaria**<br>liquidazione competenze fondamentali ed accessorie personale supplente ata e docente, liquidazione compensi corrisposti a vario titolo, elaborazione dati per il bilancio di previsione e consuntivo, schede finanziare pof, mandati di pagamento e reversali d'incasso e ogni altra pratica inerente l'area e la funzione. |

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, circolari interne in visione o semplici comunicazioni al personale docente. Tale personale deve ricevere idonee ed analitiche informazioni da parte del Responsabile del trattamento sulle mansioni affidate e sugli adempimenti cui i Collaboratori Scolastici 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 comunica l'avvenuta nomina, anche cumulativa per unità organizzativa, secondo la normativa in vigore. Tale nomina è a tempo indeterminato, decade per revoca, o con il venir meno dei compiti che giustificavano il trattamento.

AREA DOCENTI
L'unità organizzativa "**docenti**" è **incaricata** del trattamento dei dati personali degli alunni necessari allo svolgimento della funzione di istruzione ed assistenza scolastica; anche i docenti esterni incaricati ufficialmente di funzioni nella scuola (esami, corsi, concorsi e attività integrative) entrano a pieno titolo in questa categoria; ogni docente che cessa di far parte di questa unità organizzativa cessa automaticamente dalla funzione di Incaricato, ogni nuovo docente che entra a far parte di questa unità organizzativa assume automaticamente la funzione di incaricato.
I docenti sono autorizzati a trattare tutti i dati personali con cui entrano comunque in contatto nell'ambito dell'espletamento dell'attività di loro competenza e in particolare alla consultazione del fascicolo personale degli alunni e qualunque documento necessario per l'attività istituzionale.
Il Titolare reputa necessario

- autorizzare l'unità organizzativa "**docenti**" a trattare i dati sensibili e giudiziari con cui vengano a contatto durante l'attività di loro competenza nell'ambito dell'Istituto, se necessario;
- mettere a disposizione, con la pubblicazione sul sito, il Documento Programmatico sulla Sicurezza dei dati;
- consegnare, all'atto dell'assunzione in servizio, a ogni nuovo componente anche temporaneo dell'unità organizzativa in oggetto copia della presente determina o idonee indicazioni per la reperibilità sul sito;

- **ricordare che** gli incaricati devono attenersi rigorosamente a tutte le regole dettate dal D.L.vo 196/2003 e in particolare hanno l'obbligo di mantenere in ogni caso il dovuto riserbo per le informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, anche quando sia venuto meno l'incarico stesso (art. 326 del codice penale e art. 28 della legge 241/90).

**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 rinvengono nei registri dei verbali degli OO.CC., nei registri di classe, dell'insegnante, di modulo per la programmazione, d'intersezione, d'interclasse e di classe, 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) AMMINISTRATORE DI SISTEMA (art. 1 DPR 318/99) E INCARICATI DEL BACK-UP

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 Sig. Canu titolare della ditta Ai Computer in quanto persona capace, idonea, esperta nell'utilizzo dei sistemi informatici e dei relativi programmi. In particolare l'Amministratore di Sistema opera alle dipendenze del Responsabile del trattamento dei dati ed esegue le istruzioni dallo stesso impartite; rispetta le misure di sicurezza previste dalla legge e specificate nel DPS; garantisce la massima riservatezza nel trattamento dei dati; informa tempestivamente il Responsabile di anomalie nel funzionamento del sistema informatico che possono pregiudicare il corretto trattamento dei dati. L'Amministratore di Sistema, in collaborazione con il Responsabile del trattamento dei dati, prende tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati; fa in modo che sia prevista la disattivazione dei Codici identificativi personali (User-id) in caso di perdita della qualità, 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 (per tutte le specifiche si rimanda al contratto stipulato con l'Amministratore di Sistema).

**Sono incaricati di eseguire le copie di buck-up** il DSGA e tutti gli assistenti amministrativi che dovranno assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro (ad esempio cassaforte del DS).

**I docenti 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, sia per i dati sensibili che hanno acquisito in virtù del loro ufficio.

**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 titolati 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***

Le situazioni di rischio che incombono sui dati possono riguardare:

a. dati su materiale cartaceo;
b. dati su attrezzature informatiche;
c. luoghi e contenitori che custodiscono sia i materiali cartacei, sia le attrezzature informatiche.

a) 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 convenzioni;
- documentazione finanziaria e contabile;
- registro infortuni;
- moduli di iscrizione, istanze, etc
- atti affissi agli albi.

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

c) Gli eventi che possono generare danni e che comportano rischi per la sicurezza dei dati personali si possono raggruppare in 3 ambiti:

**Comportamento degli operatori**:

- sottrazioni di credenziali di autenticazione;
- carenza di consapevolezza, disattenzione o incuria;
- manomissioni e comportamenti sleali o fraudolenti;
- errore materiale;

**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 sorte 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;

**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'integrità e la disponibilità dei dati e 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 garantire tutte le misure di sicurezza per la conservazione e utilizzazione dei dati (per l'accesso ai computer e alla rete si richiede autenticazione, identificazione e password per ogni Incaricato);
- misure di prevenzione per eliminare gli eventuali incendi con adeguate modalità di gestione degli stessi (impianto elettrico a norma, idranti, estintori, rilevatori di fumo, 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 o altro supporto (CD rom, pendrive), e su materiale stampato;
- periodico salvataggio dei dati del server su unità rimovibili (CD rom, pendrive, memorie esterne);
- verifica periodica (almeno ogni tre mesi) della funzionalità e dell'efficienza delle misure di protezione e delle strutture;
- installazione di Firewall sul server al fine di impedire ingressi di hacker o intercettazioni sulla rete informatica.

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

Il Responsabile del trattamento, con il supporto dell' 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:

- tipo di supporto da utilizzare per le copie di back-up;
- numero di copie di back-up da effettuare;
- tempi e scadenze e modalità per effettuare le copie di back-up;
- trasposizione dei dati informatici su materiale stampato;
- stima della durata massima di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- assegnazione periodica del compito 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 direzione. 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.

**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
- all' Amministratore di Sistema.
- agli Incaricati

Quando il Responsabile del trattamento, in sintonia con l' 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 stabilisce, con il supporto dell'Amministratore di sistema, 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. Gli Incaricati che utilizzano i sistemi informatici annotano gli eventuali virus rilevati e 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", da conservare a cura del Responsabile del trattamento.

5. PROTEZIONE DELLE AREE E DEI LOCALI

**Sicurezza di area**

Gli interventi per la sicurezza di area servono per prevenire accessi fisici non autorizzati, danni o interferenze nello svolgimento dei servizi. Le misure 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 e gli Uffici di Segreteria perimetralmente è protetto da muro di cinta. Tutti gli edifici dell'Istituto sono dotati di sistema di allarme antintrusione. I Collaboratori Scolastici assegnati ai plessi hanno l'incarico di chiudere gli edifici al termine del servizio.
Si precisa 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 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 modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento***

In caso di danneggiamenti, smarrimenti, inaffidabilità della base dati:

- 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);
- per i dati informatici si potranno ricostruire i dati danneggiati ricavando gli stessi da atti e documenti "stampati" o si potranno salvare sul server che periodicamente prevede copie di riserva.

Ogni Incaricato della gestione di dati avrà l'accortezza di effettuare periodicamente il salvataggio dei dati sul server per permettere le consuete copie di sicurezza.
Il Responsabile del trattamento, d'intesa con gli Incaricati e con il supporto dell'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.

Per evitare danneggiamento o perdita di dati si rende estremamente importante la disponibilità delle versioni più avanzate dei Sistemi Operativi utilizzati, l'utilizzo di software antivirus di moderna concezione con segnalazione di errori o malfunzionamenti.
Nel caso esistano evidenti rischi sui Sistemi operativi, l'Amministratore di sistema e il Responsabile informano il Titolare perché siano presi gli opportuni provvedimenti alla scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore ed evitare che possano essere smarriti, danneggiarti 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 nel campo informatico.
E' necessario tenere il personale continuamente informato e all'altezza dei compiti che deve 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. Le varie tipologie di corsi di formazione potranno essere effettuate singolarmente da questa Istituzione Scolastica o in rete con altre Scuole compatibilmente con la dotazione finanziaria a disposizione dell'Istituto.
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 sempre al sopraggiungere di modifiche organizzative nel trattamento generale dei dati. 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, 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.
Gli Incaricati, Docenti, Assistenti Amministrativi e Collaboratori Scolastici che non si attengono alle indicazioni date dal Titolare e dal Responsabile e non rispettano la normativa (D.L. 196/2003 e successive modifiche ed integrazioni) incorrono nelle sanzioni normative previste.

Titolare del trattamento dei dati
Dirigente Scolastico
***Rosalinda Rambaldi***