



## **MINISTERO DELLA PUBBLICA ISTRUZIONE**

### **ISTITUTO TECNICO COMMERCIALE E PER GEOMETRA “ L.V. PASINI ”- SCHIO**

36015 Schio (VI) – Via Tito Livio 2 – tel. 0445 529902 – telefax 0445 531027

## **DOCUMENTO PROGRAMMATICO PER LA SICUREZZA**

in ottemperanza al D.Lgs. n. 196 del 30/6/2003  
(Codice in materia di protezione dei dati personali)

Il presente documento è aggiornato al 18.03.2011  
Le tabelle e gli allegati al presente documento ne formano parte integrante

Il Titolare del trattamento

D.S. Antonio Pagano

## INDICE

PREMESSA	pag.	4
1 ELENCO E NATURA DEI DATI PERSONALI TRATTATI	pag.	4
2 ELENCO DEI TRATTAMENTI DEI DATI PERSONALI	pag.	5
3 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'	pag.	6
4 PROCEDURE DI PROTEZIONE PER TRATTAMENTI CARTACEI	pag.	9
4.1 Trattamenti da parte degli Assistenti Amministrativi	pag.	9
4.1.1 Documenti d'ingresso	pag.	9
4.1.2 Informativa per la raccolta dei dati comuni o particolari	pag.	9
4.1.3 Informativa per la raccolta dei dati sensibili o giudiziari	pag.	10
4.1.4 Delega scritta	pag.	10
4.1.5 Documenti in uscita	pag.	10
4.1.6 Verifica della legittimità del trattamento in corso	pag.	10
4.1.7 Quando un alunno o un dipendente ci lascia definitivamente	pag.	11
4.1.8 Classificazione immediata di ogni documento/protocollo	pag.	11
4.1.9 Trattamento appena un documento viene ricevuto	pag.	11
4.1.10 Circoscrivere al massimo il numero di incaricati che trattano una pratica	pag.	11
4.1.11 Affidamento all'incaricato sotto la sua responsabilità	pag.	11
4.1.12 Custodia separata per i dati relativi allo stato di salute	pag.	11
4.1.13 Regole generali per la sicurezza degli archivi	pag.	11
4.1.14 Archiviazione separata	pag.	12
4.1.15 Conservazione di registri e altri documenti utilizzati per anni precedenti	pag.	13
4.1.16 Archiviazione nel fascicolo personale	pag.	13
4.1.17 Archiviazione nell'archivio storico	pag.	13
4.1.18 Scarto periodico dei documenti	pag.	13
4.1.19 Distruzione dei documenti	pag.	13
4.1.20 Appunti, bozze e copie superflue	pag.	13
4.1.21 Cautele nella fase di fotocopiatura e stampa	pag.	14
4.1.22 Movimentazione da parte di terzi	pag.	14
4.1.23 Ingresso di persone esterne per manutenzione o pulizia locali	pag.	14
4.1.24 Ingresso di altre persone in segreteria	pag.	14
4.2 Trattamenti da parte dei Collaboratori scolastici	pag.	14
4.2.1 Partecipazione alle procedure della segreteria (Par. 4.1)	pag.	14
4.2.2 Gestione di documenti scolastici	pag.	14
4.2.3 Custodia	pag.	14
4.2.4 Trasporto di documenti scolastici	pag.	15
4.3 Trattamenti da parte dei Docenti	pag.	15
4.3.1 Registri	pag.	15
4.3.2 Elaborati contenenti notizie particolari o sensibili	pag.	15
4.3.3 Certificazioni mediche e informazioni sullo stato di salute degli alunni	pag.	15

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

4.3.4 Gestione degli elenchi degli alunni	pag.	16
4.3.5 Gestione di documenti scolastici	pag.	16
4.4 Trattamenti su cartaceo da parte di Organi Collegiali(anche esterni)	pag.	16
4.4.1 Gestione di documenti scolastici	pag.	16
5 PROCEDURE DI PROTEZIONE PER TRATTAMENTI ELETTRONICI	pag.	16
5.1 Analisi dei rischi	pag.	16
5.2 Individuazione delle risorse da proteggere	pag.	17
5.3 Individuazione delle minacce	pag.	17
5.4 Individuazione delle vulnerabilità	pag.	18
5.5 Individuazione delle contromisure	pag.	19
5.6 Norme per il personale	pag.	20
5.7 Incident, response e ripristino	pag.	21
5.8 Procedure ad ogni variazione degli Incaricati	pag.	21
5.9 Scelta del software	pag.	21
5.10 Accesso ai dati in assenza dell'Incaricato	pag.	21
6 POLICY PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI	pag.	21
6.1 Policy per l'accesso alle risorse di rete	pag.	21
6.2 Policy per l'utilizzo delle postazioni PC	pag.	21
6.3 Policy per il rilascio di abilitazione navigazione internet	pag.	21
6.4 Policy per l'abilitazione al servizio di posta elettronica	pag.	22
7 PIANO DI FORMAZIONE	pag.	22
7.1 Aggiornamento del piano	pag.	22
8 CRITERI E MODALITA' DI SALVATAGGIO E DI RIPRISTINO DEI DATI	pag.	23
9 PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI	pag.	23
10 ELENCO ALLEGATI E TABELLE	pag.	24

## **PREMESSA**

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato dall'**Istituto**, previsti dal D.L.vo 30/06/2003 N. 196 "Codice in materia di protezione dei dati personali".

Il presente documento è stato redatto dal Dirigente Scolastico in qualità di responsabile della sicurezza, che provvede a firmarlo in calce.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

### **1 ELENCO E NATURA DEI DATI PERSONALI TRATTATI**

Con riferimento ai destinatari o famigliari dei destinatari dell'offerta formativa ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo, coinvolti in rapporti negoziali con l'istituzione scolastica, o aspiranti ad assumere tale ruolo, l'Istituto dichiara di trattare i dati di seguito elencati:

- Dato 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, stato relativo all'adempimento degli obblighi di leva.
- Dato 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;
- Dato C** Dati sensibili, ai sensi dell'art.4, comma 1, lett.d) del d.lgs. n.196 del 2003;
- Dato D** Dati giudiziari, ai sensi dell'art.4, comma 1, lett.e) del d.lgs. n.196 del 2003;
- Dato E** Dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi individualizzati differenziati;
- Dato F** Dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;
- Dato G** Dati riferibili a procedimenti giudiziari, pendenti in qualsiasi grado, o pregressi, di natura civile, amministrativa, tributaria, presso autorità giurisdizionali italiane o estere, diversi da quelli rientranti nell'art.4 comma 1, lett.e) del d.lgs. n.196 del 2003;
- Dato H** 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;
- Dato I** Dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- Dato L** Dati inerenti negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni;
- Dato M** Dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;
- Dato N** Dati contabili e fiscali;
- Dato O** Dati inerenti la titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;
- Dato P** Dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

## **2 ELENCO DEI TRATTAMENTI DEI DATI PERSONALI**

TR1: dati personali ALUNNI trattati dai DOCENTI

TR2: dati personali ALUNNI trattati dagli ASSISTENTI AMMINISTRATIVI

TR3: dati personali DIPENDENTI trattati dagli ASSISTENTI AMMINISTRATIVI

TR4: dati personali COLLABORATORI e FORNITORI trattati dagli ASSISTENTI AMMINISTRATIVI

TR5: dati personali di ARCHIVI GENERALI trattati dagli ASSISTENTI AMMINISTRATIVI

TR6: dati personali trattati dai COLLABORATORI SCOLASTICI

TR7: dati personali trattati da MEMBRI ORGANI COLLEGIALI (anche esterni alla scuola)

### **Finalità:**

L'Istituzione scolastica tratta dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori, anche mediante strumenti elettronici, al fine di perseguire le seguenti finalità istituzionali.

- a) adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi;
- b) somministrazione dei servizi formativi;
- c) gestione e formazione del personale, nelle sue varie componenti (docente e non docente, in ruolo presso altri apparati pubblici);
- d) adempimenti assicurativi;
- e) tenuta della contabilità;
- f) gestione delle attività informative curate ai sensi della legge 7 giugno 2000, n.150 contenente la "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni";
- g) attività strumentali alle precedenti.

### **Fonte dei dati:**

I dati trattati sono conservati su supporti informatici e/o cartacei e sono noti all'istituzione scolastica, in ragione della produzione:

- a) di atti e/o dichiarazioni provenienti da soggetti interessati a fruire direttamente, o a beneficio dei minori sottoposti alla potestà ex art.316 c.c., dei servizi formativi;
- b) documenti contabili connessi alla fornitura di prestazioni e/o di servizi e/o di lavori;
- c) documentazione bancaria, finanziaria e/o assicurativa;
- d) documenti inerenti il rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/o previdenziali.

Indicazioni più dettagliate relative alla tipologia di trattamenti sono riportate sulle tabelle allegate:

### **TABELLA 1 – Elenco dei trattamenti dei dati e strutture di riferimento.**

per ciascun trattamento sono riportate le seguenti informazioni:

- ✓ Finalità perseguita o attività svolta: descrive sinteticamente il trattamento in modo da consentire la comprensione immediata della tabella.
- ✓ Categorie di interessati: vengono individuati i trattamenti svolti, attraverso il codice identificativo del paragrafo 2.
- ✓ Natura dei dati: indica la natura dei dati trattati/conservati, attraverso il codice identificativo del paragrafo 1.
- ✓ Struttura di riferimento: sono indicate le strutture che trattano i dati indicati.
- ✓ Altre strutture che concorrono al trattamento: vengono indicate eventuali altre strutture che concorrono al trattamento dei dati indicati.
- ✓ Banca dati interessate: il codice identificativo delle banche dati interessate dal trattamento (vedi allegato 2).

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

- ✓ Apparecchiature utilizzate: contiene l'indicazione delle risorse hardware (PC) utilizzate per il trattamento dei dati

### **TABELLA 2...2.3 – Archivi e Data Base elettronici.**

per ciascuna banca dati sono riportate le seguenti informazioni:

- ✓ Codice identificativo della Banca Dati: consiste in un codice, definito dal titolare, che consente l'identificazione univoca di ciascuna Banca Dati.
- ✓ Denominazione: descrive la banca dati in modo da consentire la comprensione della tabella.
- ✓ Luogo conservazione: contiene l'indicazione del luogo in cui risiedono fisicamente i dati, cioè dove si trova (in quale sede, centrale o periferica, presso quale fornitore di servizi, etc.).
- ✓ Hardware ospitante: l'elaboratore sul cui disco fisso sono memorizzati i dati.
- ✓ Procedura di backup: riporta il riferimento al documento che descrive la procedura di salvataggio dei dati.
- ✓ Dati trattati: indica quali dati sono conservati/memorizzati, e se tra questi sono presenti dati sensibili o giudiziari.

### **TABELLA 3...3.1 - Elenco dei computer e degli uffici dove vengono trattati i dati.**

per ciascun luogo fisico di conservazione dei dati sono riportate le seguenti informazioni:

- ✓ N° PC o Denominazione PC: numero identificativo o denominazione del dispositivo hardware.
- ✓ Tipo PC: descrizione sintetica dell'apparecchiatura (desktop, server, ecc. )
- ✓ Sistema Operativo: indicare il sistema operativo installato sull'apparecchiatura.
- ✓ Denominazione ufficio: la denominazione usata per identificare il locale dove risiede il computer indicato (presidenza, segreteria, archivio, locale server, ecc.)
- ✓ Categorie trattamenti: definisce quali trattamenti vengono svolti utilizzando quella apparecchiatura (utilizzare il codice identificativo del paragrafo 2).
- ✓ Natura dei dati: indica quali dati sono trattati/conservati, attraverso il codice identificativo del paragrafo 1
- ✓ Banche dati residenti: identificare i codici relativi alle eventuali banche dati memorizzate nell'apparecchiatura (i codici delle banche dati sono quelli riportati nelle Tabelle 2, 2.1, 2.2, 2.3)
- ✓ Software utilizzato: identificare i software utilizzati per il trattamento
- ✓ Accesso: viene definito se l'accesso al locale è controllato dalla presenza di personale preposto ed se vi sono dispositivi di protezione per impedire l'accesso non autorizzato al locale (presenza di porte blindate, serrature, antifurto, etc...)
- ✓ Connessione: descrizione sintetica della rete informatica che collega i computer d'accesso ai dati utilizzati dagli incaricati: rete locale o internet.

## **3 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'**

Questo paragrafo vuole rappresentare la "fotografia" dell'organizzazione fatta dal Titolare (Dirigente Scolastico) al momento della redazione del presente DPS, al fine di eseguire l'analisi del rischio in tema di trattamento di dati personali, sulla base delle conoscenze del proprio contesto organizzativo.

L'elenco degli incaricati appartenenti alle singole categorie corrisponde all'elenco dei dipendenti validamente in servizio che ne fanno parte.

## **TITOLARE DEI TRATTAMENTI**

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

È onere del Dirigente Scolastico, quale Titolare dei trattamenti dei dati personali, assicurare e che vengano adottate le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, secondo le istruzioni indicate in questa procedura.

### **RESPONSABILE DEI TRATTAMENTI**

Viene designato il D.S.G.A. quale Responsabile dei dati svolti dall'unità organizzativa "Assistenti amministrativi", dall'unità operativa "Collaboratori scolastici" e dall'unità operativa "Assistenti tecnici".

Il Responsabile è autorizzato a trattare tutti i dati personali con cui entri comunque in contatto nell'ambito dell'espletamento dell'attività di propria competenza contenuti nelle banche dati, in archivi cartacei o informatici: TR1 - TR2 - TR3 - TR4 - TR5 - TR6 - TR7 (par. 2 - Elenco dei trattamenti dei dati personali).

Al Responsabile dei trattamenti vengono impartite le seguenti direttive di tipo generale:

- a) nominare gli Incaricati dei trattamenti di cui viene nominato Responsabile
- b) provvedere a organizzare ed istruire gli Incaricati a lui sottoposti, in particolare dando piena concretezza operativa alle Procedure di protezione dei dati contenute in questo documento.
- c) organizzare gli archivi cartacei in modo da garantire adeguata protezione dei dati, anche in relazione al loro grado di sensibilità e di delicatezza, nonché garantirne la protezione da eventi che potrebbero danneggiare o far perdere documenti.
- d) organizzare la gestione dei PC e dei dispositivi elettronici in modo da garantire adeguata protezione dei dati personali, anche in relazione al loro grado di sensibilità e di delicatezza, nonché garantirne la protezione da eventi che potrebbero danneggiare o far perdere documenti
- e) prendere le misure opportune per evitare accessi o intrusioni fisiche o tramite internet ai dati.
- f) per quanto non espressamente citato, di dare piena attuazione al Codice e al suo allegato B
- g) collaborare col Titolare nella predisposizione e successive revisioni del Documento Programmatico Sulla Sicurezza e degli altri documenti necessari.
- h) collaborare col Titolare nella predisposizione di attività formative degli Incaricati.
- i) gestire l'ingresso, all'atto dell'assunzione in servizio, dando a ogni nuovo componente anche temporaneo dell'unità organizzativa di cui è responsabile un'adeguata formazione individuale.

### **DOCENTI**

I trattamenti di dati svolti dall'unità organizzativa "Docenti" sono: per la propria sfera di competenza e secondo le indicazioni impartite dal "Titolare" o dal "Responsabile", TR1 (par. 2 - Elenco dei trattamenti dei dati personali).

Anche docenti esterni incaricati ufficialmente di funzioni nella scuola, quali esami, corsi, concorsi e attività integrative, entrano a pieno titolo in questa categoria.

### **ASSISTENTI AMMINISTRATIVI**

I trattamenti di dati svolti dall'unità organizzativa "Assistenti Amministrativi" sono: TR2 - TR3 - TR4 - TR5 (par. 2 - Elenco dei trattamenti dei dati personali).

### **COLLABORATORI SCOLASTICI**

Il trattamento di dati svolto dall'unità operativa "Collaboratori Scolastici" è: TR6 (par. 2 - Elenco dei trattamenti dei dati personali)

### **COLLABORATORI DEL DIRIGENTE SCOLASTICO**

L'unità organizzativa "Collaboratori del Dirigente Scolastico" è incaricata del trattamento di tutti i dati personali elencati al paragrafo 2 - Elenco dei trattamenti dei dati personali.

Questa scelta è necessaria, considerato che in assenza del Dirigente Scolastico, lo sostituiscono ufficialmente e quindi devono poter disporre di tutte le autorizzazioni di cui egli dispone, col vincolo di utilizzarle nei tempi e nelle misure delegate dal Dirigente.

### **MEMBRI DI ORGANI COLLEGIALI**

Si fa presente che ogni persona che cessa di far parte di questa unità organizzativa cessa automaticamente dalla funzione di Incaricato, che ogni nuovo designato che entra a far parte di questa unità organizzativa assume automaticamente la funzione di Incaricato, che in un determinato momento l'elenco degli incaricati appartenenti a questa categoria corrisponde all'elenco dei membri validamente in carica che ne fanno parte.

I trattamenti di dati svolti dall'unità organizzativa "Membri degli organi collegiali" sono:

TR7 (par. 2 - Elenco dei trattamenti dei dati personali).

### **CUSTODE DELLE PASSWORD**

Viene nominato un soggetto preposto alla custodia delle parole chiave, in relazione al fatto che l'allegato B) del Decreto Legislativo 196/2003, evidenzia la necessità di individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti alla custodia delle parole chiave o che hanno accesso ad informazioni che concernono le medesime.

### **AMMINISTRATORE DI SISTEMA**

L'Amministratore di Sistema deve utilizzare la massima riservatezza e discrezione nella manutenzione del sistema informatico e può accedere ai soli dati personali limitatamente alle necessità dello specifico intervento.

L'Amministratore di Sistema opera personalmente e dà direttive, in relazione alle operazioni di trattamento dei dati, cercando di evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta, in armonia con gli obblighi che gli derivano previsti dall'art. 31 dal Decreto Legislativo 196/2003.

In particolare l'amministratore di sistema è tenuto a:

- a) disattivare i codici identificativi in caso di perdita di qualità dei medesimi o di mancato utilizzo per un periodo superiore ai sei mesi,
- b) proteggere gli elaboratori contro i rischi di intrusione mediante idonei programmi e dall'azione di programmi di cui all'art. 615-quinquies del Codice Penale,
- c) verificare l'efficacia e l'aggiornamento dei programmi ogni sei mesi,
- d) indicare programmi per la custodia di copie di sicurezza e procedure per il ripristino della disponibilità dei dati e dei sistemi,
- e) distruggere i supporti di memorizzazione nel caso in cui non siano più riutilizzati.

(vedere anche lettera d'incarico).

### **ASSISTENTI TECNICI**

L'unità operativa "Assistenti Tecnici" è incaricata di svolgere tutte le operazioni di installazione e manutenzione dell'hardware e del software in dotazione dell'istituto, nonché collaborare con l'amministratore di sistema e coadiuvarlo in tutte le attività che riguardano la manutenzione della rete informatica dell'istituto e la gestione dei server con delega ad intervenire anche in sua assenza.

### **WEBMASTER**

Si occupa della gestione e manutenzione del sito e della rete intranet dell'istituto. Collabora col Titolare per la pubblicazione sul sito e sull'intranet delle informazioni riguardanti: attività varie svolte dall'Istituto, adempimenti burocratici scolastici di interesse pubblico o interno, organizzazione dell'istituto ecc. Collabora inoltre col Titolare e l'Amministratore di sistema per il rispetto della Privacy e la protezione dei dati durante la navigazione sul sito.

**TABELLA 4 - Elenco del personale incaricato del trattamento in ogni struttura e PC utilizzati.**

per ciascun incaricato del trattamento sono riportate le seguenti informazioni:

- ✓ Cognome e nome: individua il soggetto incaricato del trattamento
- ✓ Struttura di riferimento: riporta l'indicazione della struttura di appartenenza di ogni incaricato
- ✓ Strumenti utilizzati: riporta le informazioni relative allo strumento utilizzato (p.e. n° PC).
- ✓ Responsabilità aggiuntive: riporta le eventuali responsabilità aggiuntive rispetto all'incarico per il trattamento dei dati, (p.e. "responsabile del trattamento", "custode delle password", "custode delle chiavi di un armadio" ecc.).

**PROCEDURE DI PROTEZIONE PER TRATTAMENTI SU SUPPORTO CARTACEO**

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

Per quanto riguarda le norme generali di prevenzione, In considerazione di quanto disposto dal DPR 318/1999, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Titolare del trattamento di dati oggetto del trattamento;
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Titolare del trattamento dei dati, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Titolare del trattamento dei dati, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- Consegnare a persone non autorizzate dal Titolare del trattamento dei dati, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.

E' fatto comunque divieto di accedere agli uffici ed agli archivi (luoghi di conservazione dei trattamenti), alle persone non espressamente autorizzati dal titolare o dal responsabile.

**TRATTAMENTI DA PARTE DEGLI ASSISTENTI AMMINISTRATIVI**

**4.1.1 Documenti in ingresso**

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

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

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

(paragrafi 4.1.2 e 4.1.3).

### **4.1.2 Informativa per la raccolta di dati comuni o particolari**

La raccolta di dati personali comuni o particolari deve essere preceduta dalla sottoscrizione per attestazione della presa visione dell'apposita informativa (art. 13 del codice) fornita dal Titolare. Per i dati la cui raccolta non sia obbligatoria verrà rilasciata la firma per il consenso al trattamento. Per quanto riguarda dipendenti, collaboratori, commissari d'esame ecc. l'informativa verrà rilasciata al momento dell'inizio del rapporto di lavoro.

Nel caso in cui le finalità o le modalità di trattamento dei dati, per una determinata istanza, non siano comprese tra quelle indicate nell'informativa "generale" della scuola, risulterà necessario redigere un'informativa "specificata" da riportare direttamente sul modulo per la raccolta dati. In casi eccezionali l'informativa può essere applicata al modulo originale, occorre però che vi sia coincidenza di date ed un chiaro riferimento al documento a cui ci si riferisce.

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

### **4.1.3 Informativa per la raccolta di dati sensibili o giudiziari**

Vale quanto indicato al paragrafo precedente. Si ricorda che, nel fornire l'informativa, i soggetti pubblici fanno espresso riferimento alla legge che prevede gli obblighi in base ai quali viene effettuato il trattamento dei dati sensibili e giudiziari.

Per quanto attiene ai dati sensibili e giudiziari il trattamento "è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e le finalità di rilevante interesse pubblico perseguite." (articolo 20 e articolo 21 comma 1).

### **4.1.4 Delega scritta**

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

### **4.1.5 Documenti in uscita**

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

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

Prima di consegnare o spedire documenti, verificare che esistano in atti le necessarie, adeguate informative. Nel caso di documenti in uscita è necessario all'atto della consegna o dell'invio, verificare che la persona che riceve il documento sia legittimata al ritiro e all'utilizzo (delega).

### **4.1.6 Verifica della legittimità del trattamento in corso**

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

- Il trattamento sia connesso con l'esercizio delle funzioni istituzionali (principio di pertinenza) e che esse non siano perseguibili attraverso il trattamento di dati anonimi (necessità).
- Le modalità del trattamento siano tali da determinare il minimo sacrificio possibile del diritto alla riservatezza dell'Interessato (principio di non eccedenza: è illegittimo chiedere un dato in più di quello che è strettamente necessario).
- Ogni fase del trattamento rispetti le norme di legge e di regolamento.

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

- In ogni fase del trattamento siano adottate le misure di sicurezza previste per la categoria alla quale il dato appartiene
- Se il dato è sensibile o giudiziario, siano rispettati i presupposti per avere la legittimazione a trattarlo
- In caso di comunicazione o diffusione, che il dato rientri nelle categorie autorizzate

### **4.1.7 Quando un alunno o un dipendente ci lascia definitivamente**

Ad ogni alunno o dipendente che ci lascia definitivamente vanno consegnati tutti i documenti contenenti dati personali che la scuola non sia obbligata a conservare. Nel caso non fosse possibile trattare direttamente con l'Interessato, si deve mandare un avviso per il ritiro. Nel frattempo i materiali da consegnare vanno posti in busta chiusa. Al ritiro va fatta firmare una ricevuta. Se, passato un lasso ragionevole di tempo, l'interessato o un suo delegato non si presenterà a ritirarli, si avvierà una procedura di distruzione dei documenti, con apposito verbalino. In ogni caso qualunque fascicolo personale che transiti dall'archivio corrente a quello storico, deve essere prima depurato di tutti dati personali non più necessari.

### **4.1.8 Classificazione immediata di ogni documento/protocollo**

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

### **4.1.9 Trattamento appena un documento viene ricevuto**

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

### **4.1.10 Circoscrivere al massimo il numero di Incaricati che trattano una pratica**

I documenti contenenti dati personali di tipo sensibile, giudiziario devono essere visti e conosciuti dal minor numero possibile di Incaricati. Le pratiche relative a tali documenti devono essere seguite nell'intero iter possibilmente da una sola persona, salvo diversa disposizione del Dirigente o del Responsabile.

### **4.1.11 Affidamento all'Incaricato sotto la sua responsabilità**

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

Nei casi in cui i documenti con dati sensibili/giudiziari debbano essere trattati per un certo periodo di tempo, vengono mantenuti sotto la responsabilità dell'Incaricato per il più breve tempo possibile. L'Incaricato ha istruzione di elaborare le pratiche riferite a questi documenti con discrezione e, nei momenti di non utilizzazione, di conservare questi documenti dentro un cassetto o un armadio chiuso a chiave.

### **4.1.12 Custodia separata per i dati relativi allo stato di salute**

Per dati relativi allo stato di salute vi è l'obbligo di custodia separata rispetto agli altri dati trattati per finalità che non richiedono il loro utilizzo.

### **4.1.13 Regole generali per la sicurezza degli archivi**

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

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

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

- perdita accidentale dei dati.

### Dati personali comuni - protezione dall'accesso fisico non autorizzato :

i documenti contenenti dati personali comuni sono conservati in archivi ad accesso selezionato: pertanto l'accesso ai dati è consentito ai soli Incaricati del trattamento.

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

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

### Protezione dei locali archivio contenenti dati personali sensibili :

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

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

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

### Protezione dal rischio di perdita dei dati dovuta ad eventi fisici

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

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

### Misure logistiche :

Il personale addetto al trattamento di dati personali deve porre in essere le misure necessarie a ridurre al minimo i rischi di:

accesso fisico non autorizzato;

furto o manomissione dei dati da parte di malintenzionati;

distruzione o perdita dei dati dovuta ad eventi fisici;

perdita accidentale dei dati.

### Chiusura a chiave dei contenitori metallici:

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

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

### **4.1.14 Archiviazione separata**

I documenti contenenti dati sensibili, giudiziari o particolari ad alto livello di delicatezza vanno di norma chiusi in busta di carta, su cui è riportato nome dell'interessato, tipo di documento, data attuale e la scadenza per la eliminazione (se non conoscibile, mettere una data presunta seguita da un punto interrogativo). Per i documenti contenenti dati particolarmente sensibili, invece del nome sulla busta si deve scrivere un codice, la data attuale e la scadenza per la eliminazione. La corrispondenza tra codice e nome dell'interessato sarà riportata in un foglio o un quaderno, posto in una busta chiusa gestita dal Responsabile o dal Titolare, e posto nell'armadio di protezione dati chiuso a chiave, presso l'ufficio del DSGA.

### **4.1.15 Conservazione di registri e altri documenti utilizzati per anni scolastici precedenti**

Molti documenti e registri sono utilizzati per un intero anno scolastico ma solo in quello. I documenti non più utilizzati negli anni seguenti (salvo ricorsi o richieste di accesso legittime) al termine dell'anno scolastico sono impacchettati a gruppi omogenei e chiusi con carta e scotch; sull'involucro viene riportato il contenuto e la scadenza per l'eliminazione. Vengono conservati in una stanza chiusa a chiave ad accesso selezionato. L'eliminazione dei documenti avviene mediante la Procedura di Protezione Dati (4.1.19).

### **4.1.16 Archiviazione nel fascicolo personale**

I documenti non archiviati nell'Armadio di Protezione dati, finché l'alunno è iscritto o il dipendente è in servizio, vengono conservati nel fascicolo personale. I dati sensibili e giudiziari vengono raccolti in busta sigillata all'interno del fascicolo personale; sulla busta, oltre al nome dell'allievo o del personale, viene riportata la lettera identificativa "S". I dati che si situano in una zona di confine tra dato particolare e dato sensibile (ad es. certificati medici generici privi di diagnosi), data la loro bassa pericolosità vengono mantenuti nel fascicolo personale, poi eliminati con la procedura di Protezione Dati(4.1.19). Il fascicolo personale è conservato in cassettiere metalliche, presso gli uffici di segreteria, chiuse a chiave negli orari non lavorativi e normalmente presidiate da almeno un Incaricato dei trattamenti (ovvero un dipendente assegnato alla segreteria).

### **4.1.17 Archiviazione nell'archivio storico**

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

### **4.1.18 Scarto periodico dei documenti**

Scarto periodico dei documenti contenenti dati personali di qualunque livello, ai sensi dell'art. 11 comma e del D.Lgs 196/2003, vanno eliminati non appena cessa lo scopo per cui sono stati raccolti. Pertanto periodicamente, di regola all'inizio di ogni anno solare per le pratiche che hanno questa cadenza, oppure all'inizio di ogni nuovo anno scolastico tutti gli archivi vengono passati al vaglio e vengono eliminati i documenti non più necessari, utilizzando la Procedura di Protezione Dati (4.1.19).

### **4.1.19 Distruzione dei documenti**

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

### **4.1.20 Appunti, bozze e copie superflue**

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

### **4.1.21 Cautele nella fase di fotocopiatura e stampa**

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

### **4.1.22 Movimentazione da parte di terzi**

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

### **4.1.23 Ingresso di persone esterne per manutenzione e pulizia dei locali**

L'accesso di dipendenti o estranei per la manutenzione o per la pulizia dei locali contenenti archivi dev'essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni devono essere effettuate in presenza di un Incaricato.

### **4.1.24 Ingresso di altre persone in segreteria**

Di norma l'ingresso in segreteria, nelle ore lavorative, è riservato a chi vi lavora, al Dirigente e ai suoi collaboratori, agli assistenti tecnici, ai Collaboratori scolastici che ne hanno motivo. Le altre componenti scolastiche e gli estranei possono accedervi solo nell'orario di apertura al pubblico stabilito dal C.d.I. Ciò viene previsto allo scopo di evitare che persone non autorizzate vedano anche involontariamente documenti riservati.

## **TRATTAMENTI DA PARTE DEI COLLABORATORI SCOLASTICI**

### **4.2.1 Partecipazione alle procedure della segreteria (Par. 4.1)**

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

### **4.2.2 Gestione di documenti scolastici**

In generale qualunque documento scolastico che contenga dati personali è sottoposto dal D.Lgs 196/2003 a una qualche forma di protezione, quindi va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va consegnato in segreteria per l'archiviazione. L'obbligo è ancora più stringente se il dato è di tipo particolare, sensibile o giudiziario. Chi avesse originale o copia di un tale documento deve custodirlo con elevatissima cura e cautela dalla visione di terzi e riconsegnarlo alla segreteria appena possibile.

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte del D.Lgs 196/2003. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola. Va comunque previamente chiesta l'autorizzazione al Dirigente o al Responsabile perché potrebbe costituire atto illegittimo. Pertanto qualsiasi registro, elaborato, elenco, libretto personale, certificato, e in generale documento scolastico che contiene dati

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

personali di qualcuno va custodito con cautela, impedendo che altri ne prendano visione, lo copino o se ne impadroniscano.

### **4.2.3 Custodia**

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

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

La Presidenza e la segreteria vanno chiusi a chiave quando non presenziati dal relativo personale. E' fatto divieto assoluto a chiunque non ne abbia ricevuto esplicita autorizzazione di accendere o utilizzare i computers della segreteria o della presidenza o che comunque contengano dati personali. Si deve intervenire immediatamente se una persona non autorizzata tenta di farlo.

Se esterni per motivi di manutenzione devono entrare nelle stanze citate o negli archivi per i quali è prevista la chiusura a chiave, vanno seguiti a vista; se questo è impossibile, vanno invitati a tornare in altro momento.

### **4.2.4 Trasporto di documenti scolastici**

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

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

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

## **4.3 TRATTAMENTI SU SUPPORTO CARTACEO DA PARTE DEI DOCENTI**

### **4.3.1 Registri**

I registri personali devono essere sempre custoditi in modo sicuro. I registri di classe devono essere consultabili solo dagli alunni della classe interessata e si deve vigilare perché non vi siano accessi non autorizzati. I docenti sono Incaricati di riporli in segreteria quando terminano le lezioni. Il registro dei verbali del consiglio di classe e qualunque altro registro di verbali, affidato per la scrittura, la firma o la consultazione, deve essere mantenuto protetto da accessi non autorizzati e riconsegnato quanto prima in segreteria.

### **4.3.2 Elaborati contenenti notizie particolari o sensibili**

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

### **4.3.3 Certificazioni mediche e informazioni sullo stato di salute degli alunni**

I dati personali in grado di rivelare lo stato di salute sono classificati "sensibili" e quindi protetti dalla visione di terzi che non sia strettamente necessaria. Quindi eventuali certificati medici vanno visionati solo se necessario e subito restituiti all'interessato affinché li consegni in segreteria. Questo vale in particolare per i certificati di esonero o limitazione presentati per educazione fisica; l'insegnante prenda nota dei limiti da osservare e faccia recapitare dall'interessato il certificato in

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

segreteria. A volte l'insegnante ottiene informazioni su particolari, anche gravi, problemi di salute dell'alunno che possono presentarsi durante le lezioni (allergie, asma grave, diabete grave, epilessia, cardiopatie gravi, ecc.) o imbarazzanti (disturbi di continenza, ecc.), messe a disposizione dai genitori o dall'interessato. Se l'informazione è orale l'insegnante è tenuto al riserbo. Se esiste qualche comunicazione scritta, trattasi di dato sensibile e va trattato con particolari cautele, chiedendo al Titolare o al DGSA come fare. Anche informazioni su particolari diete seguite dall'alunno o per motivi di salute o per motivi religiosi sono da considerare dato sensibile, pertanto va rivelato soltanto nei casi strettamente necessari ed omettendone la ragione. Nel caso di alunni portatori di handicap che incide sulla didattica, la visione e la detenzione della relativa documentazione per l'integrazione è un dato di massima sensibilità in quanto idoneo a rivelare lo stato di salute. Pertanto i documenti dovranno essere visti soltanto dai docenti e personale strettamente necessario, conservati con elevata cautela, poi consegnati in segreteria e conservati in luogo sicuro per dati sensibili.

### **4.3.4 Gestione degli elenchi degli alunni**

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

### **4.3.5 Gestione di documenti scolastici**

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

## **4.4 TRATTAMENTI SU SUPPORTO CARTACEO DA PARTE DEI MEMBRI DEGLI ORGANI COLLEGIALI (ANCHE ESTERNI ALLA SCUOLA)**

### **4.4.1 Gestione di documenti scolastici**

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

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

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

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

## **5 PROCEDURE DI PROTEZIONE PER TRATTAMENTI CON STRUMENTI ELETTRONICI**

### **5.1 ANALISI DEI RISCHI**

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;

## Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)

- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
  - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
    - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

### 5.2 INDIVIDUAZIONE DELLE RISORSE DA PROTEGGERE

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;
- software;
- apparecchiature di comunicazione;
- manufatti vari;
- servizi;
- apparecchiature per l'ambiente;
- immagine della scuola.

### 5.3 INDIVIDUAZIONE DELLE MINACCE

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse indicate al paragrafo 5.2.

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione			X
Uragano			X
Fulmine			X
Fuoco	X	X	
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere			X

## Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)

Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		
Uso illegale di software	X	X	
Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	
Intercettazione (Eavesdropping)	X		
Infiltrazione nelle comunicazioni	X		
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	

Per ulteriori dettagli delle minacce relative all'aspetto informatico vedere l'Allegato 1.

### 5.4 INDIVIDUAZIONE DELLE VULNERABILITÀ

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nel paragrafo 5.3.

**Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

<b>Infrastruttura</b>	<b>Hardware</b>	<b>Comunicazioni</b>
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione inadeguata della rete
		Connessioni a linea pubblica non protette

<b>Documenti cartacei</b>	<b>Software</b>	<b>Personale</b>
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

## **5.5 INDIVIDUAZIONE DELLE CONTROMISURE**

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico;
- contromisure di carattere procedurale;
- contromisure di carattere elettronico/informatico.

### **Contromisure di carattere fisico**

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità dell'Istituto;
- i responsabili dei trattamenti sono anche responsabili dell'area in cui si trovano i trattamenti;
- i locali ad accesso controllato sono chiusi anche se presidiati;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'Istituto;
- i locali sono provvisti di sistema di allarme e di estintore (le misure sono attive);

### **Contromisure di carattere procedurale**

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal responsabile del trattamento o da un suo delegato;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri di classe, contenenti dati comuni e particolari, durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni vengono depositati dall'insegnante dell'ultima ora di lezione in portineria e successivamente raccolti da un incaricato del trattamento e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio delle lezioni.
- il docente è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del docente che è chiuso a chiave, una chiave di riserva è mantenuta con le dovute cautele dalla scuola presso l'ufficio Didattica;
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato nell'ufficio del Titolare.

### **Contromisure di carattere elettronico/informatico**

Vedere l'allegato 2.

## **5.6 NORME PER IL PERSONALE**

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa e indicate nel paragrafo 5.2, nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete (Allegato 3).

## **5.7 INCIDENT RESPONSE E RIPRISTINO**

Vedere l'Allegato 2

## **5.8 Procedure ad ogni variazione degli Incaricati**

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

## **5.9 Scelta del software**

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

## **5.10 Accesso ai dati in assenza dell'Incaricato**

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

- 1) deve sussistere un'improrogabile necessità di accedere ai dati per ragioni di servizio;
- 2) deve essere verificata l'impossibilità o la notevole difficoltà di raggiungere l'Incaricato;
- 3) il Responsabile apre la busta chiusa riposta in luogo sicuro dov'è scritta la password. Poi la mette in una nuova busta chiusa.
- 4) chi ha aperto la busta, comunica l'accesso effettuato al dipendente assente al momento del suo rientro e lo invita a modificare immediatamente la password.

## **6 POLICY PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI**

### **6.1 Policy per l'accesso alle risorse di rete.**

Vedere allegato 3

### **6.2 Policy per l'utilizzo delle postazioni PC**

L'utilizzo delle postazioni PC da parte dei dipendenti e degli studenti della scuola è permesso ed incoraggiato per i soli scopi legati al raggiungimento degli obiettivi assegnati ad ognuno.

I computers e le infrastrutture di rete messi a disposizione dalla scuola sono considerate risorse della scuola stessa e pertanto devono essere utilizzate per scopi istituzionalmente riconosciuti.

### **6.3 Policy per il rilascio di abilitazione navigazione internet**

L'utilizzo di internet da parte dei dipendenti e degli studenti della scuola e' permesso ed incoraggiato per i soli scopi legati al raggiungimento degli obiettivi assegnati ad ognuno.

L'accesso ad Internet ed alla Intranet, così come i computers e le infrastrutture di rete sono considerate risorse della Scuola e pertanto devono essere utilizzate per scopi istituzionalmente riconosciuti.

- ✓ La scuola non e' responsabile dei contenuti delle informazioni ricevute da internet.
- ✓ E' proibito qualsiasi utilizzo che non ricada nei compiti personalmente affidati ad ognuno.
- ✓ E' proibita la trasmissione e l'accesso a qualsiasi materiale in violazione di qualsiasi legge nazionale ed internazionale. Questo include ma non si limita a: materiale coperto da copyright, materiale con contenuti osceni o materiale pornografico
- ✓ Qualsiasi tentativo di violazione della sicurezza informatica, anche attraverso internet, comporterà la perdita dei privilegi di accesso ad internet.
- ✓ E' proibito utilizzare attrezzature della scuola per acquisti on-line a titolo personale con o senza carta di credito.
- ✓ E' proibito l'utilizzo delle attrezzature della scuola per scopi ricreativi (giochi, musica, chat-line,)
- ✓ E' proibito scaricare qualsiasi tipo di software. Sara' cura dell'amministratore di sistemi mettere a disposizione sulla intranet i software freeware o shareware indispensabili.
- ✓ E' proibito l'utilizzo di qualsiasi casella di posta internet non ufficialmente rilasciata dalla scuola.
- ✓ Viene mantenuto dall'Amministratore di Sistema un registro dei collegamenti (log) con le misure tecniche ed organizzative necessarie a garantire la riservatezza di tale registro. Il registro dei collegamenti potrà essere esibito solo all'Autorità Giudiziaria, dietro esplicita richiesta, ovvero per eseguire rilevamenti di carattere statistico, generali ed impersonali.

### **6.4 Policy per il rilascio della abilitazione al servizio di posta elettronica esterna.**

Le caselle di posta elettronica assegnate dalla scuola sono di proprietà della scuola stessa.

L'utilizzo di posta elettronica e' esclusivamente per fini professionali e lavorativi legati ai compiti istituzionali della scuola.

I messaggi delle caselle di posta elettronica sono paragonabili a cartoline postali quindi nessuna garanzia di riservatezza può essere fornita dal punto di vista tecnico.

Si consiglia di non inviare con la posta elettronica messaggi con allegati di grosse dimensioni per evitare il decadimento delle prestazioni di accesso alla rete internet.

La scuola fornisce l'accesso alle caselle di posta elettronica esterna agli utenti della rete secondo gli standard definiti, compilando l'apposito modulo e sottoscrivendo ed accettando il contenuto di questo documento.

Le caselle di posta internet vengono rilasciate ai soli dirigenti, segreterie, docenti.

La creazione di ogni altra casella, deve avere oggettive e fondate motivazioni e deve avere il benessere da parte del Dirigente d'Istituto.

Il nome della casella viene assegnato dall'amministratore di sistema, seguendo gli standard in uso.

## **7 PIANO DI FORMAZIONE**

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

(la formazione è stata fatta dal DSGA)

## 7.1 Aggiornamento del piano

Il presente piano è soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 Num. 196. Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo della scuola ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo della scuola tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

## 8 CRITERI E MODALITA' DI SALVATAGGIO E DI RIPRISTINO DEI DATI

Nei moduli, ALLEGATO 2 "MISURE, INCIDENT RESPONSE, RIPRISTINO", e TABELLA 5 e 5.1 "MODALITA' DI SALVATAGGIO DEI DATI" e "MODALITA' DI RIPRISTINO DEI DATI", sono descritti i criteri e le procedure adottati per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva direttamente dall'eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che quando sono necessarie, le copie dei dati siano disponibili e le procedure efficaci.

Nella Tabella 5 sono riportate le seguenti informazioni:

Data base: contiene il codice identificativo del data base interessato al salvataggio;

Dati sensibili o giudiziari contenuti: descrive i dati sensibili o giudiziari da salvare contenuti nel data base;

Criteri individuati per il salvataggio: descrive le procedure di salvataggio in essere per il data base;

Ubicazione di conservazione delle copie: indica il luogo di conservazione delle copie;

Struttura operativa incaricata del salvataggio: Indica la struttura incaricata del salvataggio.

Nella Tabella 5.1 sono riportate le seguenti informazioni:

Server/data base: contiene l'indicazione del server e i data base ivi contenuti che verranno ripristinati;

Scheda operativa: contiene il riferimento alla scheda operativa che descrive la procedura di ripristino;

Pianificazione delle prove di ripristino: contiene l'indicazione del periodo in cui si prevede di effettuare dei test di efficacia delle procedure adottate per il salvataggio/ripristino dei dati.

## 9 PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Nel modulo **TABELLA 6 "PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI"** sono riportate le informazioni necessarie per disporre di un quadro sintetico dell'impegno formativo che si prevede di sostenere in attuazione della normativa.

Nella TABELLA 6 sono riportate le seguenti informazioni:

Corso di formazione: riporta l'identificativo del corso di formazione.

Descrizione sintetica: contiene la descrizione sintetica degli obiettivi del corso.

Classi di incarico interessate: contiene l'elenco delle classi omogenee di incarico a cui il corso è destinati e/o le tipologie di incaricati interessati.

Numero di incaricati interessati: contiene il numero di addetti interessati dal corso.

## **Documento programmatico sulla sicurezza** (ai sensi del D.L.vo n. 196 del 30/06/03)

Numero di incaricati già formati/da formare nell'anno: contiene l'indicazione del numero di addetti già formati negli anni precedenti e quelli di cui si prevede la formazione nell'anno in corso.

### **10. ELENCO ALLEGATI COSTITUENTI PARTE INTEGRANTE DI QUESTO DOCUMENTO**

- ALLEGATO 1 Minacce
- ALLEGATO 2 Misure, incident response, ripristino
- ALLEGATO 3 Regolamento per l'utilizzo della rete
- ALLEGATO 4 Utilizzo del proxy
- TABELLA 1 Elenco dei trattamenti dei dati e strutture di riferimento
- TABELLA 2 Archivi e data base elettronici
- TABELLA 2.1 Archivi e data base elettronici
- TABELLA 2.2 Archivi e data base elettronici
- TABELLA 2.3 Archivi e data base elettronici
- TABELLA 3 Elenco dei computer e degli uffici dove vengono trattati i dati
- TABELLA 3.1 Elenco dei server e degli uffici dove vengono trattati i dati
- TABELLA 4 Elenco del personale incaricato del trattamento in ogni struttura e dotazioni informatiche
- TABELLA 5 Salvataggio dei dati
- TABELLA 5.1 Modalità di ripristino dei dati
- TABELLA 6 Pianificazione degli interventi formativi