



ISTITUTO COMPRENSIVO STATALE
"Monsignor Saba"
Via Buscaglia, snc – 09030 ELMAS (CA)
Tel 070/2135088 – Fax 070/243511
e-mail caee08600e@istruzione.it; a.flaviani@tiscali.it;
sito web: www.scuolaelmas.it



Documento programmatico sulla sicurezza dei dati personali

*Redatto in base alle disposizioni del CODICE IN MATERIA DI
DATI PERSONALI (D.Leg.vo 196/2003) e del DISCIPLINARE
TECNICO allegato al medesimo decreto*

FINALITA' E SCOPI

Il 1 gennaio 2004 è entrato in vigore il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione di dati personali, testo unico che riordina tutta la normativa in tema di trattamento dei dati personali e di Privacy. All'Art. 2 il nuovo codice dispone che "il trattamento dei dati personali 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". Per conseguire tali finalità il codice impone all'art. 31 e ss. l'adozione di misure minime di sicurezza tra le quali, al comma 1 dell'Art. 34, è citata la tenuta di un aggiornato documento programmatico sulla sicurezza.

Il presente documento, redatto dal Dirigente Scolastico prof.ssa Annalisa Flaviani quale rappresentante della Istituto Comprensivo "Mons. Saba" Elmas che deve ritenersi titolare del trattamento di dati personali secondo quanto stabilito dall'Art. 28 del D. Lgs. 196/03, si propone quindi di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato da tutto il personale dell'Istituto.

DEFINIZIONI

Trattamento

qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

Dato personale

qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Dati identificativi

i dati personali che permettono l'identificazione diretta dell'interessato;

Dati sensibili

i 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 e la vita sessuale;

Dati giudiziari

i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Titolare

la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Responsabile

la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente,

associazione od organismo preposti dal titolare al trattamento di dati personali;

Incaricati

le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

Interessato

la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

Comunicazione

il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Diffusione

il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Dato anonimo

il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

Blocco

la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

Banca di dati

qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

Comunicazione elettronica

ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

Misure minime

il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31; b)

Strumenti elettronici

gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento; c)

Autenticazione informatica

l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

Credenziali di autenticazione

i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

Parola chiave

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

Profilo di autorizzazione

l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti

Sistema di autorizzazione

l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

ARTICOLAZIONE DEL DOCUMENTO

Conformemente a quanto prescrive il punto 19. del “disciplinare tecnico” (allegato sub b) al d.Lgs. 196/2003 e sulla base degli esempi pubblicati nel sito web del garante oltre che di documentazione messa a disposizione delle scuole da parte del sindacato nazionale Dirigenti Scolastici, il documento è articolato come di seguito riportato:

Parte I: Analisi della situazione

- 1.1 Indicazione delle sedi e descrizione dei locali in cui si effettuano i trattamenti
- 1.2 Elaboratori utilizzati per il trattamento dei dati personali
- 1.3 Ruoli e compiti delle figure previste per il trattamento e la sicurezza dei dati personali
- 1.4 struttura organizzativa funzionale al trattamento dei dati personali
- 1.5 nomine ed incarichi
- 1.6 indicazioni relative ai dati trattati
- 1.7 dati sensibili

Parte II – Misure di sicurezza adottate o da adottare

- 2.1 analisi dei rischi possibili e dei danni conseguenti
- 2.2 misure di sicurezza adottate o da adottare
- 2.3 formazione del personale
- 2.4 programma di revisione ed adeguamento

Parte I - Analisi della situazione

1.1 Indicazione delle sedi e descrizione dei locali in cui si effettuano i trattamenti

1.1.1 Sedi

Una situazione di notevole rilevanza, ai fini dell'individuazione dei rischi per la sicurezza dei dati e per la predisposizione delle misure minime, si presenta nella sede centrale della scuola nei cui locali sono ospitati gli uffici di segreteria, l'ufficio del dirigente e le classi dell'Istituto. In essa vi sono custoditi tutti i materiali cartacei nonché le strumentazioni informatiche che vengono utilizzate per l'elaborazione dei dati personali.

P01: Sede centrale – Via Buscaglia

Vengono indicati inoltre i plessi che ospitano scuole dipendenti dall'Istituto, ove i dati contenuti ed i rischi per l'integrità dei dati medesimi sono ridottissimi. In essi vengono custoditi i registri di classe che contengono i dati anagrafici ed i recapiti delle famiglie degli alunni. Gli strumenti informatici in essi presenti sono utilizzati per la didattica e nessuno di essi è autorizzato al

trattamento di dati personali.

P02: Plesso scolastico – Via Amundsen

P03: Plesso scolastico – Via Sestu

P04: Plesso scolastico – Via Don Palmas

1.1.2 Stanze

Il trattamento e la conservazione dei dati nelle sedi su menzionate avviene nelle stanze di seguito riportate:

Rif.	Plesso	Descrizione	Armadi
S1	P01	Stanza del Dirigente Scolastico	N°2 Armadi scaffale con serratura, N°1 Armadio senza serratura, scaffalature
S2	P01	Stanza del Direttore SGA	N°1 armadio (6 ante) con serratura N° 1 armadio (8 ante) con serratura
S3	P01	Ufficio Didattica e Personale	N° 1 cassaforte, N° 1 armadio (n. 10 ante) con serratura N° 1 armadio (n. 14 ante) con serratura n. 3 schedari senza serratura
S4	P01	Ufficio gestione contabilità e magazzino	N° 1 armadio (n. 10 ante) con serratura n. 1 scaffale (n. 4 ante) senza serratura
S5		Archivio di deposito	Scaffalature aperte posizionate su 5 pareti
S6		Sala Professori	n. 1 armadio aperto

Si rimanda alla parte II del documento per la specificazione delle misure di sicurezza fisica adottate.

1.2 Elaboratori utilizzati per il trattamento dei dati personali

Per il trattamento dei dati personali sono utilizzati i sistemi di elaborazione di seguito riportati:

Rif.	Stanza	Descrizione	Sistema operativo	Applicativi	Antivirus	In rete	Incaricato utilizzatore
PC1		Server	Windows Server 2003	Office Sissi Argo	Symantec Antivirus	SI	
PC2	S1	PC Client	Windows XP Professional	Office Argo	Symantec Antivirus	SI	Flaviani
PC3	S2	PC Client	Windows XP Professional	Office Sissi Argo	Symantec Antivirus	SI	Meloni

PC4	S3	PC Client	Windows Professional	XP	Office Argo	Symantec Antivirus	SI	Pecorelli
PC5	S3	PC Client	Windows Professional	XP	Office Argo	Symantec Antivirus	SI	Devino
PC6	S3	PC Client	Windows Professional	XP	Office Argo	Symantec Antivirus	SI	Lobrano
PC7	S4	PC Client	Windows Professional	XP	Office Sissi Argo	Symantec Antivirus	SI	Cannas

Si rimanda alla parte II del documento per una descrizione più approfondita del sistema informatico e per la specificazione delle misure di sicurezza informatiche adottate.

1.3 Ruoli e compiti delle figure individuabili per il trattamento e la sicurezza dei dati personali

1.3.1 Titolare del trattamento di dati personali

Il **Titolare del trattamento** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il titolare del trattamento delinea gli elementi essenziali e le strategie di fondo del trattamento dati e quindi assume il ruolo di **Responsabile della sicurezza dei dati**.

Il **Titolare del trattamento**, anche nel suo ruolo di **responsabile della sicurezza dei dati**, ha le seguenti responsabilità e funzioni:

- Delinare gli elementi essenziali del trattamento dati quali finalità, modalità, strumenti utilizzati
- Predisporre le misure di sicurezza da attuare per la protezione dei dati personali comprese le misure minime di sicurezza previste dall'allegato B
- Redigere ed aggiornare periodicamente il documento programmatico sulla sicurezza con la specificazione delle sedi e degli uffici in cui viene effettuato il trattamento dei dati, l'elenco delle banche dati oggetto di trattamento, la descrizione del sistema informatico attraverso il quale avviene il trattamento dei dati personali
- Vigilare sulla puntuale osservanza delle disposizioni e delle proprie istruzioni anche attraverso verifiche periodiche
- Definire e verificare periodicamente le modalità di accesso ai locali in cui sono conservati e trattati dati personali e le misure di protezione da adottare
- Decidere se affidare il trattamento dei dati all'esterno della struttura del titolare

Il **Titolare**, nella sua funzione di **Responsabile della sicurezza dei dati personali**, può incaricare per iscritto uno o più **Responsabili della gestione del sistema informatico** che sovrintendono alle risorse informatiche utilizzate per il trattamento dei dati

1.3.2 Responsabile del trattamento

Il **Responsabile del trattamento** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposto dal titolare al trattamento di dati personali e a cui sono affidate le seguenti responsabilità e compiti:

- Individuare, nominare ed incaricare per iscritto gli **incaricati del trattamento** per le banche dati che gli sono state affidate
- Individuare, nominare ed incaricare per iscritto uno o più **incaricati delle copie di sicurezza** delle banche dati

- Di trasmettere ai propri incaricati le disposizioni ricevute dal **Titolare** in merito al trattamento di dati personali
- Di sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali
- Di dare istruzioni adeguate alle figure da esso nominate
- Verificare periodicamente, con frequenza almeno semestrale, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli **Incaricati del trattamento**

Il Responsabile del trattamento si assume inoltre l'Incarico di custode delle copie delle credenziali con il compito di:

- Gestire e custodire le credenziali per l'accesso ai dati degli **Incaricati del trattamento**
- Predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto
- Istruire gli incaricati del trattamento sull'uso delle parole chiave e sulle caratteristiche che debbono avere

Il **Responsabile del trattamento**, se designato, 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

Il **Responsabile del trattamento** effettua il trattamento attenendosi alle istruzioni ricevute dal **Titolare del trattamento** ed impartendo istruzioni adeguate alle figure da esso nominate. Il responsabile del trattamento vigila sulla puntuale osservanza delle disposizioni e delle istruzioni impartite.

Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile del trattamento**, ne assumerà tutte le responsabilità e funzioni

1.3.3 Responsabile della gestione del sistema informatico

Il **Responsabile della gestione del sistema informatico** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende alle risorse informatiche utilizzate per il trattamento dei dati.

Il **Titolare**, nella sua funzione di **Responsabile della sicurezza dei dati personali**, può incaricare per iscritto uno o più **Responsabili della gestione del sistema informatico**, anche affidando l'incarico in *out-sourcing* a soggetti esterni.

E' compito dei **Responsabili della gestione del sistema informatico**:

- Definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale
- Effettuare l'aggiornamento dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne i difetti con cadenza almeno semestrale (installazione di Patch, Fix o System-Pack)
- Proteggere gli elaboratori dal rischio di intrusione esterna da parte di persone non autorizzate mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale
- Attivare, dietro disposizione del **Responsabile del trattamento**, le credenziali di autenticazione agli incaricati del trattamento,
- Revocare, dietro disposizione del **Responsabile del trattamento**, tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali
- Revocare, dietro disposizione del **Responsabile del trattamento**, tutte le credenziali per

- l'accesso ai dati degli incaricati al trattamento nel caso di mancato utilizzo per oltre 6 mesi
- Informare il **Responsabile della sicurezza dei dati personali** nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il **Responsabile della gestione del sistema informatico** deve definire la modalità e la periodicità di esecuzione delle copie di sicurezza oltre che le procedure di verifica delle copie fatte e di ripristino delle banche dati.

Qualora il **Responsabile della sicurezza** ritenga di non nominare alcun **Responsabile della gestione del sistema informatico**, ne assumerà tutte le responsabilità e funzioni

La nomina dei **Responsabili della gestione del sistema informatico** può essere a tempo determinato qualora esistano dei motivi che suggeriscano questa soluzione come nel caso di affidamento dell'incarico a soggetti esterni mediante sottoscrizione di contratto annuale.

1.3.4 Incaricato delle copie di sicurezza delle banche dati

Il **Responsabile del trattamento** può nominare, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati** che hanno il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle banche di dati.

Gli **Incaricati delle copie di sicurezza delle banche dati** devono:

- sovrintendere alla esecuzione periodica delle copie di sicurezza delle banche dati ad essi assegnati secondo le procedure definite dal **responsabile della gestione del sistema informatico** o, in assenza di tale figura, dal **responsabile della sicurezza**
- Assicurarsi della qualità delle copie di sicurezza effettuate
- attenersi alle disposizioni ricevute dal **Responsabile del trattamento** in merito alla conservazione delle copie delle banche dati
- Provvedere a conservare e custodire con la massima cura i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato
- Segnalare tempestivamente al **Responsabile della gestione del sistema informatico** ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati

Qualora il **Responsabile del trattamento** ritenga di non nominare alcun **Incaricati delle copie di sicurezza delle banche dati**, ne assumerà tutte le responsabilità e funzioni

1.3.5 Incaricato del trattamento dei dati personali

Il **Titolare od il Responsabile del trattamento** possono nominare uno o più **Incaricati del trattamento dei dati personali**, persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali.

Gli **incaricati del trattamento** dei dati personali nello svolgimento del loro incarico devono:

- Trattare i dati personali in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinente completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;

Nel caso in cui siano autorizzati ad utilizzare strumenti informatici, gli **incaricati del trattamento**

devono:

- Conservare con la massima segretezza le credenziali di autenticazione loro assegnate
- Definire le parole chiave secondo i criteri fissati dal **responsabile della sicurezza** in collaborazione con il **Responsabile della gestione del sistema informatico**
- Le parole chiave vanno modificate al primo utilizzo e , successivamente almeno ogni 6 mesi (almeno ogni 3 mesi per i dati sensibili)
- custodire gli strumenti elettronici a loro affidati e non devono in nessun caso allontanarsi durante una sessione di trattamento di dati personali lasciando accessibile lo strumento elettronico
- controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza

Il **Titolare o il Responsabile del trattamento** devono consegnare a ciascun **Incaricato del trattamento dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

1.4 struttura organizzativa funzionale al trattamento dati

Nella seguente tabella è riportata una sintetica descrizione delle struttura organizzativa funzionale al trattamento dei dati con i riferimenti agli incarichi conferiti, ai trattamenti operati ed alle relative responsabilità:

Struttura	Nominativi	Compiti	Trattamenti operati
Dirigente scolastico	Prof.ssa Annalisa Flaviani	Direzione generale di tutte le attività; gestione delle pratiche riservate	Tutti i dati in possesso dell'Istituto
DSGA	Roberta Meloni	Coordinamento delle attività amministrativo/contabili, con responsabilità sul trattamento di tutti i dati	Tutti i dati trattati dal personale amministrativo
Collaboratori del dirigente scolastico	Prof.ssa Silvia Minafra Dott.ssa Ginetta Melis	Supporto organizzativo al D.S., con delega di firma e sostituzione del medesimo in caso di assenza	tutti i dati trattati dai docenti
Ufficio personale	Gabriella Cannas Laura Devino Elisabetta Lobrano Pietro Pecorelli	Gestione dei dati del personale con trattamento di dati sia comuni che sensibili.	<u>dati comuni:</u> <ul style="list-style-type: none"> - dati personali - dati dei familiari - servizio prestato - curriculum studi - aggiornamento e formazione <u>Dati sensibili:</u> <ul style="list-style-type: none"> - convinzione religiosa - iscrizione a sindacati - stato di salute - situazione di handicap situazioni familiari con handicap
Ufficio didattica	Gabriella Cannas Laura Devino Elisabetta Lobrano	Gestione dei dati relativi agli alunni con trattamento di dati sia comuni che sensibili.	<u>dati comuni:</u> <ul style="list-style-type: none"> - Curricolo studi - Dati personali - Dati dei genitori - fotografia - registro esiti e idoneità <u>Dati sensibili:</u> <ul style="list-style-type: none"> - origine razziale ed etnica

	Pietro Pecorelli		<ul style="list-style-type: none"> - convinzione religiosa - stato di salute - situazione di handicap vaccinazioni
Ufficio contabilità	Gabriella Cannas Laura Devino Elisabetta Lobrano Pietro Pecorelli	Gestione dei dati per la predisposizione del bilancio e degli emolumenti del personale dipendente.	<u>dati comuni:</u> - dati personali <u>Dati sensibili:</u> iscrizione a sindacati
Ufficio affari generali	Gabriella Cannas Laura Devino Elisabetta Lobrano Pietro Pecorelli	Gestione dei dati per il protocollo e gestione dei dati relativi ai fornitori di beni e servizi	
Corpo docente	Tutti i docenti	Insegnamento, conduzione di laboratori, orientamento, partecipazione a commissioni varie ed ai lavori degli Organi Collegiali	Tutti i dati trattati dai docenti, relativamente ad alunni, genitori, anche con riferimento a notizie relative agli alunni in situazione di handicap
Collaboratori Scolastici	Tutti i Collaboratori Scolastici	Collaborazione con il personale amministrativo e docente in occasione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta e del trasferimento fra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali	Dati personali degli alunni e dei loro familiari ad esclusione di quelli sensibili ed in ogni caso di quelli non necessari allo svolgimento del compito assegnato
Organi Collegiali	Tutti i docenti Genitori rappresentanti Ata rappresentanti	Partecipazione alle attività gestionali; decisioni di tipo amministrativo, finanziario, regolamentare; pratiche disciplinari riguardanti gli alunni	Tutti i dati trattati in fase di elaborazione ed esecuzione delle delibere dei Consigli di Classe, Interclasse, intersezione, Collegio docenti, Consiglio di Istituto, della Giunta E. e dell'Organo di Garanzia della scuola

1.5 Nomine ed incarichi

L'Istituto Comprensivo "Mons. Saba" di Elmas, **Titolare del trattamento**, si impegna ad assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del **Codice del Disciplinare Tecnico** (Allegato B al D.Lgs. 196/03 del 30 giugno 2003), tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previa idonee istruzioni fornite per iscritto. Il Dirigente Scolastico prof.ssa Annalisa Flaviani in qualità di rappresentante legale dell'Istituto, delinea gli elementi essenziali del trattamento dati ed assume il ruolo di **Responsabile della sicurezza**.

Per la definizione, la gestione, la verifica ed il periodico aggiornamento delle misure di sicurezza adottate sulla rete destinata al trattamento dei dati personali il Titolare del Trattamento ha provveduto alla nomina dell'Ing. Antonio Vargiu quale **responsabile della gestione del sistema informatico**. Il Responsabile della gestione del sistema informatico sovrintende alle risorse

informatiche utilizzate per il trattamento dei dati e si assume le responsabilità in merito alle misure di sicurezza informatiche adottate per la protezione dei dati . L'individuazione del responsabile della gestione del sistema informatico è stata operata in conformità alle disposizioni contenute nel provvedimento del Garante sulla Privacy del 27/11/08 pubblicato nella G.U. n. 300 del 24/12/08 ***“misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”***

Il Titolare del trattamento determina:

1. di designare l'unità organizzativa “docenti” (comprendente anche assistenti alla didattica, tecnici e personale di sostegno) quale **incaricata** del trattamento dei dati personali degli alunni necessari allo svolgimento della funzione di istruzione ed assistenza scolastica.
2. che anche docenti esterni incaricati ufficialmente di funzioni nella scuola (esami, corsi, concorsi e attività integrative) entrino a pieno titolo in questa categoria;
3. di dare atto che ogni dipendente che cessa di far parte di questa unità organizzativa cessa automaticamente dalla funzione di Incaricato, che ogni nuovo dipendente 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 dipendenti validamente in servizio che ne fanno parte;
4. di autorizzare questa categoria di incaricati a trattare tutti i dati personali con cui entrino comunque in contatto nell'ambito dell'espletamento dell'attività di loro competenza e in particolare di poter consultare il fascicolo personale degli alunni e qualunque documento necessario per l'attività istituzionale;
5. di 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;

Opportune disposizioni in merito al trattamento dei dati personali da parte dell'unità organizzativa “Docenti” verranno impartite mediante uno specifico documento che verrà posto alla firma di tutti i componenti della suddetta unità al momento in servizio. Copia di tale determina verrà inoltre consegnata all'atto dell'assunzione in servizio, a ogni nuovo componente anche temporaneo dell'unità organizzativa in oggetto.

In base a quanto stabilito dall'**Art. 29 del Codice**, il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Responsabili di specifici trattamenti** con il compito di individuare, nominare ed incaricare per iscritto, gli **Incaricati del trattamento** dei dati personali.

L'Istituto Comprensivo “Mons. Saba” di Elmas ha assegnato il ruolo di **Responsabile di specifico trattamento** di dati personali al **Direttore SGA Sig.ra Meloni Roberta** per le seguenti banche dati:

- Contabilità pubblica e patrimonio
- fornitori
- dipendenti
- protocollo
- rapporto con enti ed imprese
- alunni

Nel suo ruolo di Responsabile di specifico trattamento il DSGA ha proceduto alle seguenti nomine:

Incaricato delle copie di sicurezza delle banche dati: Lobrano Elisabetta.

Incaricati del trattamento dei dati personali – personale amministrativo:

- Pecorelli Pietro

- Devino Maria Laura
- Lobrano Elisabetta
- Cannas Maria Gabriella

Per motivi organizzativi il personale amministrativo incaricato del trattamento è autorizzato all'inserimento, modifica, cancellazione e visualizzazione/stampa dei dati relativi a tutte le aree indipendentemente dalla struttura organizzativa cui sono assegnati. Eventuali limitazioni all'accesso a determinati dati verranno all'occorrenza determinate modificando i permessi relativi alle password assegnate a ciascun incaricato.

Incaricati del trattamento dei dati personali – collaboratori scolastici:

Il Responsabile del trattamento determina:

1. di designare l'unità organizzativa **“collaboratori scolastici”** quale **incaricata** del trattamento dei dati personali degli alunni autorizzata a trattare i dati personali in occasione della gestione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta e del trasferimento fra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali
2. di assegnare a tale unità organizzativa l'incarico di vigilare sui locali in cui avviene il trattamento di dati personali con i compiti di:
 - Impedire l'intrusione nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal Responsabile del trattamento.
 - Impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal Responsabile del Trattamento.
 - Identificare e verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici
3. di dare atto che ogni dipendente che cessa di far parte di questa unità organizzativa cessa automaticamente dalla funzione di Incaricato, che ogni nuovo dipendente 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 dipendenti validamente in servizio che ne fanno parte;

Opportune disposizioni in merito al trattamento dei dati personali da parte dell'unità organizzativa “Collaboratori Scolastici” verranno impartite mediante uno specifico documento che verrà posto alla firma di tutti i componenti della suddetta unità al momento in servizio. Copia di tale determina verrà inoltre consegnata all'atto dell'assunzione in servizio, a ogni nuovo componente anche temporaneo dell'unità organizzativa in oggetto.

1.6 Indicazioni relative ai dati trattati

In questa parte del documento vengono fornite informazioni essenziali in merito ai dati personali trattati, con riferimento alla natura ed alla classificazione; vengono anche indicati i riferimenti relativi alla classificazione, alla sistemazione ed alla custodia come riportato nella seguente tabella.

Banche dati attivate

Le banche dati attivate sono quelle di seguito riportate:

- Alunni
- Personale
- Protocollo
- Rapporti con enti ed imprese

- Fornitori
- Contabilità pubblica e patrimonio
- Registro di classe
- Registro degli insegnanti
- Registro infortuni alunni e dipendenti

Aree di attività

L'assetto organizzativo relativo al trattamento dei dati personali è definito dal piano di lavoro elaborato dal DSGA che prevede le seguenti aree di attività cui sono assegnati gli incaricati di seguito riportati:

Descrizione aree	Attività	incaricati
Area didattica	Gestione dati relativi agli alunni	Pecorelli Pietro
Area amministrativa e finanziaria	Gestione dati per elaborazione retribuzioni e bilancio	Cannas Maria Gabriella
Area gestione personale	Gestione dati relativi al personale dipendente	Devino Maria Laura Lobrano Elisabetta
Area affari generali	Gestione del protocollo, gestione archivio, rapporti con enti ed imprese, pratiche varie	Lobrano Elisabetta Devino Maria Laura

Ai docenti incaricati del trattamento dal Dirigente Scolastico sono affidati i registri personali e di classe in cui sono riportati i dati degli alunni. I docenti potranno trattare dati personali o anche sensibili degli alunni nell'ambito della propria attività, rispettando sempre l'obbligo del segreto d'ufficio già previsto dalle disposizioni vigenti in materia di istruzione scolastica.

finalità perseguita con il trattamento dei dati

- Garanzia del servizio scolastico
- Gestione del personale interno con contratto a tempo determinato e indeterminato
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da terzi fornitori

Natura dei dati trattati

La natura dei dati soggetti al trattamento da parte della scuola è la seguente:

- Documentazioni complete riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati
- Documenti prodotti dalle famiglie riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche.
- Documentazione riguardante il personale docente e non docente, con elementi di individuazione di appartenenza sindacale, stato di salute, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, allo stato di servizio, alla

- retribuzione, alle eventuali pratiche disciplinari.
- Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi
- Dati contabili e fiscali

Classificazione dei dati trattati

Nella seguente tabella sono sinteticamente riportate le informazioni essenziali sulla classificazione ed organizzazione dei documenti contenenti dati personali:

Dati	Plessi	Stanza	Armadio	Struttura di riferimento	Descrizione degli strumenti
Dati personali relativi agli alunni (registri di classe contenenti i recapiti delle famiglie e comunicazioni varie, con esclusione di ogni documentazione che possa contenere dati "sensibili"); anagrafe alunni	P01 P02 P03 P04	Aule, sala professori, stanze personale amministrativo	Armadi di legno con chiusura normale	DS, Personale docente, Assistenti Amministrativi	Documenti cartacei e informatici
dati personali sensibili relativi agli alunni (certificazioni mediche, certificazioni di deficit, diagnosi)	P01	S__	Armadi con serratura	DSGA e assistenti amministrativi	Documenti cartacei e informatici
dati sensibili relativi ai genitori degli alunni (istanze contenenti dati relativi alla situazione patrimoniale, documentazioni giudiziarie, documentazioni mediche prodotte a corredo delle domande di iscrizione o di altre domande)	P01	S__	Armadi con serratura	DSGA e assistenti amministrativi	Documenti cartacei e informatici
Dati relativi ai dipendenti	P01	S__	Armadi con serratura	DSGA ed Assistenti amministrativi	Doc. Cartacei e informatici
dati personali sensibili relativi ai dipendenti	P01	Ufficio del DSGA	Armadio del DSGA	DSGA	Doc. Cartacei
dati personali riservati, relativi ad alunni, genitori e personale dipendente, corrispondenza riservata custodita dal dirigente, compresi gli atti relativi ai provvedimenti disciplinari	P01	Ufficio del DS	Armadio del DS	DS	Doc. Cartacei
dati personali relativi ai fornitori	P01	S__	Armadi con serratura	DSGA ed Assistenti amministrativi	Doc. Cartacei e informatici
dati personali di anni precedenti, sistemati in archivio;	P01	Archivio	Armadi e scaffalature	DSGA ed Assistenti amministrativi	Doc. Cartacei

Affidamento dei dati a terzi per il trattamento:

Tutti i dati posseduti dalla scuola vengono trattati esclusivamente presso gli Uffici dell'Istituto. Nessuna altra struttura concorre al trattamento dei dati in possesso dell'Istituto. I dati verranno affidati a terzi solo nell'ambito della propria attività istituzionale e comunque nei casi previsti dalla informativa fornita agli interessati od in seguito ad esplicito consenso espresso dagli stessi.

Modalità di trattamento

La conservazione ed il trattamento dei dati avviene nel modo seguente:

Cartaceo:

I dati in possesso della scuola sono conservati in locali e armadi dotati di chiusura a chiave ai quali hanno accesso esclusivamente le persone incaricate (per la collocazione degli armadi si veda la tabella presente al punto 1.1.2). Alcuni dati personali non sensibili possono essere riposti in armadi senza serratura ospitati in locali vigilati e sotto il controllo dei collaboratori scolastici anche dopo l'orario di chiusura degli uffici.

Mediante il sistema informatico:

Il controllo degli accessi alle varie postazioni di lavoro viene effettuato mediante l'istituzione di un sistema di autenticazione che permette l'identificazione indiretta del soggetto autorizzato al trattamento dei dati tramite riconoscimento di una credenziale logica costituita da un codice identificativo associato ad una password.

1.7 Dati sensibili

Il trattamento dei dati sensibili e giudiziari è effettuato secondo quanto prevede il regolamento emanato dal Ministero della Pubblica Istruzione con Decreto n. 305 del 7 dicembre 2006 ed allegato al presente documento.

Parte II – Misure di sicurezza adottate o da adottare

2.1 analisi dei rischi possibili e dei danni conseguenti

In questa parte del documento vengono individuati i principali rischi potenzialmente pericolosi per la sicurezza dei dati a ciascuno dei quali viene attribuito un **indice di rischio (R)** determinato sulla base di due indici:

- **Gravità (G) dell'evento** (1=lieve; 2=media; 3=grave; 4=gravissima)
- **Probabilità (P) di accadimento** (1=improbabile/non sono noti episodi; 2= poco probabile/sono noti rarissimi episodi; 3= probabile/noto qualche episodio; 4= molto probabile/ricorrenti episodi)

Il prodotto **G x P** tra l'**indice di gravità dell'evento** e la **probabilità di accadimento** determina l'**indice del rischio R** dell'evento

EVENTO	IMPATTO SULLA SICUREZZA			
	Descrizione	Stima del rischio		
		G	P	R
Gestione manuale di materiali cartacei				
Accesso archivi	Consultazione da parte di non addetti, smarrimento di documenti, diffusione di notizie per violazione del segreto d'Ufficio	2	1	2
Distruzione	Distruzione accidentale di documenti	1	1	1
Furto	Sottrazione furtiva di documenti	2	1	2
Mancata chiusura	Accessibilità agli uffici in orari di chiusura	1	1	1
Visione abusiva	Possibilità di accedere ai dati di terzi, nell'occasione di una consultazione di documentazioni degli interessati	1	1	1
Mancata chiusura	Mancata chiusura di contenitori ed armadi	1	2	2
Gestione automatizzata delle informazioni				
Errata destinazione	Trasmissione errata per via telematica a terzi di documentazioni contenenti dati personali	2	1	2
Accesso abusivo	Accesso ai dati senza la necessaria autorizzazione	1	1	1
Intercettazione	Intercettazione dati in rete con possibilità di sottrazione, alterazione o distruzione degli stessi	3	1	3
Intrusione	Intrusione dall'esterno nel sistema informatico con possibilità di accesso a dati personali e di distruzione archivi	4	1	4
Virus	Danneggiamenti e distruzione di dati a causa di virus informatici	3	2	6
Uso o comunicazione non autorizzata dei dati	Uso non autorizzato dei dati da parte del personale ovvero loro comunicazione illegale	1	1	1
Guasto	Guasto tecnologico o malfunzionamenti HW e SW	2	3	6
Protezione sedi e strutture				
Intrusione	Intrusione con sottrazione e/o distruzione di dati in formato cartaceo o informatico con	2	1	2

	danneggiamento o furti di strumenti elettronici			
Allagamento	Infiltrazioni da acqua piovana	1	1	1
Incendio	Propagazione di fiamme da cortocircuiti	4	1	4
Mancanza di energia elettrica	Danneggiamento di dati a causa dell'improvviso spegnimento dei computers	1	1	1

2.2 Misure di sicurezza adottate o da adottare

In questa parte del documento vengono descritte le misure adottate per contrastare i rischi individuati a seguito dell'analisi effettuata e della valutazione degli eventi. Per misura viene inteso lo specifico intervento tecnico, informatico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, nonché per assicurare il livello minimo di protezione.

2.2.1 Protezione delle aree e dei locali

Contro i rischi di intrusione i locali sono dotati di impianto di allarme a sensori infrarossi, attivabile mediante digitazione di un codice in possesso del personale dipendente. L'attivazione di detto sistema di allarme avviene al termine dell'orario di lavoro.

Oltre a tale sistema, nelle ore di chiusura, la scuola usufruisce del servizio svolto da società che opera nel campo della vigilanza privata.

Le aree contenenti dati in supporto cartaceo (mobili ed armadi contenenti documenti) sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.

L'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Il personale amministrativo, incaricato del trattamento, ha ricevuto le opportune istruzioni per la tutela e la protezione dei dati in formato cartaceo e dei dispositivi informatici attraverso i quali avviene il trattamento dei dati personali.

L'accesso ai locali in cui avviene il trattamento e la custodia di dati personali è vigilato dai Collaboratori Scolastici cui è assegnato il compito di impedire l'intrusione da parte di persone non autorizzate e di identificare e quindi verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici.

2.2.2 Protezione dei supporti cartacei

Relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nei seguenti:

- qualsiasi documento degli studenti presentati alla scuola va inserito, quando personale, in apposite cartelline non trasparenti;
- qualsiasi documento che l'istituzione scolastica consegna agli studenti va inserito, quando riservato o contenente documentazione sensibile, in apposite buste o cartelline non trasparenti.
- Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non contiene alcun dato (praticamente il primo foglio funge da copertina).

Le copie dei telefax inviati mediante apparecchio tradizionale sono riconsegnate a colui che ha eseguito o fatto eseguire la trasmissione, avendo cura di porre quale primo foglio il rapporto di trasmissione formato A4 che viene stampato dal fax, con di seguito i fogli contenenti il messaggio.

Per ciò che concerne le trasmissioni del telefax, nella copertina del messaggio è inserita la seguente dicitura:

“Qualora questo messaggio fosse da Voi ricevuto per errore vogliate cortesemente darcene notizia a mezzo telefax od e-mail e distruggere il messaggio ricevuto erroneamente. Quanto precede ai fini del rispetto del Codice sulla tutela dei dati personali.”

La scuola è sprovvista di distruggi documenti, ma eventuali copie di documenti, di scritti, di appunti, di tabulati prova, ecc. sono distrutte personalmente dal personale amministrativo.

Documenti in ingresso: I documenti cartacei in arrivo sono sempre consegnati in busta chiusa al dirigente scolastico che li esamina, destinando al protocollo riservato quelli appartenenti alle tipologie di dati riservati o sensibili, e smistando quelli trattati dall'Ufficio di Segreteria. I documenti ricevuti tramite FAX o consegnati aperti vengono subito recapitati al dirigente scolastico.

Documenti in uscita: I documenti in uscita vengono trattati esclusivamente dal personale incaricato, protocollati e predisposti per la spedizione in busta chiusa. I documenti contenenti dati sensibili vengono posti in busta chiusa riservata ed inseriti nel plico contenente la lettera di trasmissione nella quale è evidenziata la presenza di documentazione riservata.

Gestione accesso archivi: L'accesso all'archivio è consentita al personale incaricato solo in seguito ad autorizzazione concessa dal DSGA che ha in custodia la chiave di accesso.

2.2.3 Interventi di collaboratori esterni, esperti e specialisti

Nel caso in cui l'Istituzione scolastica si dovesse avvalere, per l'attuazione di interventi previsti dall'offerta formativa o dagli interventi miranti all'integrazione dei soggetti diversamente abili, della collaborazione di terapisti, esperti e specialisti, assistenti igienico-personali, è escluso, nei limiti del possibile, l'accesso dei medesimi a documentazioni contenenti dati sensibili. In merito alla possibilità di trattamento di dati personali particolari da parte dei suddetti soggetti, è previsto che i medesimi dichiarino:

1. di essere consapevoli degli obblighi previsti dal D. L.vo 196/2003
2. di impegnarsi ad ottemperare all'obbligo di tutela dei dati personali
3. di adottare le istruzioni specifiche ricevute per la garanzia di sicurezza dei dati

2.2.4 Trattamenti con l'ausilio di sistemi informatici

Come specificato all'**Art.31 del D. Lgs. n. 196/03** i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

In primo luogo occorre osservare che i computer, incluso il server, risultano tutti sollevati da terra, in modo da evitare eventuali danneggiamenti e perdite di dati dovute ad allagamenti;

In secondo luogo si evidenzia che il server è collegato a un gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o da interruzione di corrente elettrica. Non appena si dovesse verificare la mancanza di energia elettrica si raccomanda di procedere alla rapida chiusura di qualunque sessione in corso, al salvataggio dei dati sul disco rigido e all'avvio della procedura di spegnimento del server.

Ulteriori garanzie sulla protezione delle basi dati sul server sono offerte dalla presenza di due dischi rigidi in configurazione RAID 1, configurazione che garantisce il recupero dei dati anche in presenza di un guasto su uno dei dischi. Nel caso in cui dovesse intervenire il guasto di uno dei dischi del server il **responsabile del trattamento** dovrà dare immediata comunicazione del fatto al **responsabile della gestione del sistema informatico** che dovrà procedere all'immediata

duplicazione degli archivi del disco e alle operazioni necessarie al ripristino o alla sostituzione del disco difettoso.

Gli incaricati del trattamento hanno ricevuto adeguate istruzioni in merito al trattamento dei dati con lo strumento informatico anche in relazione ai possibili rischi alla integrità ed alla riservatezza dei dati trattati.

2.2.4.1 Sistema di autenticazione ed autorizzazione

Il DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA – ALLEGATO B specifica che il trattamento di dati personali con strumenti informatici deve essere limitato al personale **incaricato al trattamento** dotato di una o più **credenziali di autenticazione** fra le seguenti:

1. un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solo dal medesimo
2. un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave
3. una caratteristica biometrica dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave

In considerazione dell'attuale dotazione informatica ed organizzazione dell'Istituto viene adottata la credenziale riportata al punto 1 con l'assegnazione a ciascun incaricato del trattamento di una o più parole chiave riservate.

Per quanto riguarda il **sistema di autorizzazione**, a ciascun **incaricato del trattamento** nominato dal DSGA sono dati i poteri di inserimento, accesso, modifica e cancellazione sui dati relativi alle proprie aree di competenza. Ai componenti dell'unità organizzativa denominata "docenti" non è fornita alcuna autorizzazione per l'accesso informatico ai dati trattati sui PC della segreteria ed è fatto divieto di archiviare dati personali e/o sensibili sui PC destinati all'attività didattica.

2.2.4.2 Misure per garantire l'integrità e la disponibilità dei dati

Il Titolare del trattamento al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita ha nominato un **incaricato delle copie di sicurezza delle banche dati** cui sono affidati i compiti di:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza
- Assicurarli della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro
- Provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato
- Segnalare tempestivamente al **responsabile della gestione del sistema informatico** ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati

Le copie di sicurezza vengono custodite nell'armadio blindato situato nella stanza del DSGA.

2.2.4.3 Protezione contro accessi abusivi, intrusioni e virus

Gli elaboratori destinati al trattamento di dati personali sono collegati in rete locale in modo da

rendere possibile:

- lo scambio fra di essi di dati e documenti
- l'accesso a risorse condivise (stampanti, unità di memorizzazione, etc.)
- l'accesso alla base dati del server
- l'accesso ad Internet

La rete di supporto al trattamento di dati personali è estesa ai locali di segreteria ed è fisicamente separata da qualunque altra presente nella scuola in modo da rendere impossibile ogni accesso ai dati da parte di qualunque computer presente nell'edificio scolastico non destinato al trattamento di dati personali.

L'accesso ad Internet avviene attraverso un'unica linea ADSL che è condivisa tra tutte le postazioni di lavoro per mezzo di un router. Tutte le postazioni di lavoro e tutti gli incaricati sono abilitati all'accesso ad Internet con le seguenti raccomandazioni:

- è meglio evitare, se possibile, l'accesso ad Internet dal server
- non utilizzare eventuali linee di comunicazione alternative che consentano l'accesso individuale della postazione e l'aggiramento del router (accesso mediante modem)
- l'accesso ad Internet e l'utilizzo della posta elettronica è consentito esclusivamente per lo svolgimento delle mansioni proprie dell'incaricato

Per proteggere il sistema informatico dall'azione dei **virus informatici** tutte le postazioni di lavoro ed il server sono dotate di antivirus aggiornato regolarmente con una frequenza almeno mensile.

Per la protezione da accessi abusivi ed intrusioni la rete è dotata di un dispositivo **firewall** che si interpone fisicamente tra il router ed il concentratore della LAN in modo da garantire che nessun traffico di rete possa avvenire con l'esterno, se non esplicitamente consentito dalla politica di protezione adottata.

2.2.4.4 Gestione, manutenzione ed assistenza

Per garantire l'efficienza del sistema informatico e l'adeguatezza delle misure di sicurezza adottate il **responsabile della sicurezza** ha proceduto alla nomina di un **responsabile della gestione del sistema informatico** che dovrà individuare, amministrare, aggiornare, e periodicamente adeguare le misure di sicurezza necessarie a proteggere i dati trattati.

Il Responsabile della gestione del sistema informatico dovrà definire un regolamento per l'impiego del sistema informatico che dovrà essere portato a conoscenza degli incaricati del trattamento.

Per tenere traccia degli interventi di assistenza e di amministrazione del sistema informatico il **responsabile della sicurezza**, deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta con la descrizione dettagliata delle operazioni eseguite che attesti la conformità a quanto stabilito al punto 25 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (allegato B).

E' fatto divieto agli incaricati, o a qualunque altra persona non autorizzata, di installare software sugli elaboratori utilizzati per il trattamento dei dati; tale software potrà essere installato solo dal **responsabile della gestione del sistema informatico** previa autorizzazione del responsabile della sicurezza o del responsabile del trattamento.

2.3 Formazione del personale

Il **titolare ed il responsabile del trattamento dei dati personali** valutano, per ogni persona cui hanno affidato un incarico o una responsabilità, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario

pianificare interventi di formazione.

La previsione di interventi formativi degli incaricati del trattamento, ha lo scopo principale di renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il responsabile del trattamento verificherà ogni anno, entro il 31 dicembre, le necessità di ulteriore formazione del personale incaricato al trattamento dei dati e di quello incaricato di effettuare periodicamente le operazioni di copia di sicurezza delle banche dati.

2.4 Programma di revisione ed adeguamento

Entro il **31 marzo di ogni anno**, il **Titolare del trattamento** predisporrà una nuova versione del Documento Programmatico sulla Sicurezza anche tenendo conto degli eventuali aggiornamenti al disciplinare tecnico (allegato B) apportati con decreto del Ministro della Giustizia di concerto con il Ministro per le Innovazioni e le Tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

L'Avvenuta redazione o l'avvenuto aggiornamento del Documento Programmatico sulla Sicurezza verrà menzionata nella Relazione accompagnatoria al bilancio d'esercizio.

Gli incaricati del trattamento sono stati debitamente informati circa il contenuto del presente documento e sono obbligati ad uniformarsi allo stesso mentre il responsabile del trattamento è obbligato a vigilare sull'osservanza delle disposizioni stesse da parte degli incaricati.

Il Dirigente Scolastico, in qualità di rappresentante legale dell'Istituto titolare del trattamento, si impegna ad adottare, nella fase di graduale attuazione degli interventi previsti dalla normativa sulla tutela della privacy, ogni possibile misura destinata a salvaguardare la sicurezza dei dati personali, siano essi contenuti nei documenti cartacei che registrati mediante strumenti elettronici. Tali misure riguarderanno gli aspetti organizzativi, logistici e procedurali miranti ad evitare con ogni mezzo qualsiasi incremento di rischi di distruzione o perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito.

Data 30.03.2009

Firma del Titolare

F.to prof.ssa Annalisa Flaviani