



www.icrivasanlor.it

ISTITUTO COMPRESIVO
di Scuola dell'Infanzia, Primaria e Secondaria di Primo grado
di RIVA LIGURE e SAN LORENZO AL MARE
SEDE CENTRALE E UFFICI: VIA CARAVELLO, 3 - 18015 RIVA LIGURE (IM)
Tel. 0184 486384 - Fax 0184 487989 - E-mail: segreteria@icrivasanlor.it
Codice fiscale: 90057290083



M.I.U.R.

ANNO SCOLASTICO 2010/2011

D. P. S.

Documento Programmatico sulla

Sicurezza dei Dati Personali



Elaborato in base al

D.Lgs. 30 giugno 2003 n.196

**in "Materia di protezione dei dati
personali" ed al relativo
disciplinare tecnico**

**Aggiornato ai sensi del D.M.7
dicembre 2006 n.305 e della D.M. 30
novembre 2007 n 104.**

Firma del Titolare del
Trattamento _____

Firma del Responsabile del
Trattamento _____

D. P. S.
Documento Programmatico
sulla Sicurezza dei Dati Personali

ISTITUTO COMPRENSIVO DI RIVA LIGURE E S. LORENZO AL MARE
V. Caravello 3 – 18015 Riva Ligure IM
Tel. 0184 486384 – Fax 0184 487968
Codice Mecc. Imic803001 C.F. 90057290083
E-mail:imic803001@istruzione.it Sito: www.icrivasanlor.it

Prot. n. 834/A23

Riva Ligure, 23 marzo 2011

Al Personale in servizio

Istituto Comprensivo di Riva Ligure e San Lorenzo al Mare

Al Consiglio di Istituto

Al DSGA

Albo

**DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
PERSONALI
(D. L.vo 196 del 30/06/03)**

PREMESSA

L'Istituto Comprensivo di Riva Ligure e San Lorenzo al Mare con sede in Riva Ligure – Via Caravello, 3 C.F.90057290083, nella persona del suo legale rappresentante pro tempore D.S. Prof. Luciano Calzamiglia (C.F. CLZLCN51T13E290T) ha redatto il seguente Documento Programmatico per la Sicurezza ai sensi e per gli effetti dell'art. 34 comma 1, lettera g) del D. L.vo n. 196/2003 e del disciplinare tecnico allegato al medesimo sub B "Disciplinare tecnico in materia di misure minime di sicurezza", nonché della "Guida operativa per redigere il documento programmatico" pubblicata sul sito web del Garante.

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

ARTICOLO 1 – RIFERIMENTI NORMATIVI

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

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

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

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

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

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

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

ARTICOLO 2 – OBIETTIVI DEL DOCUMENTO

Il “DPS”, redatto in ottemperanza a quanto disposto dal D.L.vo 196/2003 (Codice in materia di protezione dei dati personali) mira a regolamentare e garantire la riservatezza, la sicurezza e la protezione dei dati personali in possesso dell'Istituto Comprensivo di Riva Ligure e San Lorenzo al Mare di Riva Ligure (IM), nonché a porre in atto idonee strategie per la protezione delle aree e dei locali interessati a misure di sicurezza.

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

Tali dati riguardano:

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

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

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

ARTICOLO 3 – CAMPO DI APPLICAZIONE

1. Il “DPS” definisce le politiche e gli standard di sicurezza in merito ai dati da garantire e proteggere. Tali dati si distinguono in:

- dati personali comuni (dati anagrafici o identificativi delle persone, indirizzi, recapiti telefonici, codici fiscali, dati bancari, informazioni circa la composizione familiare, la professione esercitata da un determinato soggetto, la sua formazione etc.);
- dati sensibili (dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute, appartenenza a categorie protette, portatore di handicap, stato di gravidanza , vita sessuale etc.);

- dati giudiziari (provvedimenti sul casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato o dei relativi carichi pendenti, la qualità di imputato o indagato ai sensi degli artt. 60 o 61 del Codice di Procedura Penale, avviso di garanzia, separazioni, affidamento dei figli, etc.).

Il Decreto 7 dicembre 2006 n. 305 – Regolamento recante identificazione dei dati sensibili e giudiziari trattati in attuazione degli articoli 20 e 21 del Dlgs 30 giugno 2003 n. 196, identifica nelle schede allegate (n.1-2-3-4-5-7), che ne formano parte integrante, le tipologie di dati sensibili e giudiziari e di operazioni indispensabili per la gestione del sistema dell'istruzione.

LA Direttiva ministeriale 30 novembre 2007 n. 104 reca linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'uso di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali. Il Regolamento di Istituto recepisce tali linee di indirizzo e prevede sanzioni rigorose e severe per eventuali comportamenti connessi ad un trattamento improprio di dati personali acquisiti mediante telefoni cellulari o altri dispositivi elettronici.

2. I trattamenti sono realizzati prevalentemente negli uffici di direzione e segreteria, nell' archivio della sede centrale, nelle aule scolastiche ove sono conservati, durante l'anno scolastico, i registri degli alunni di classe, il giornale dell'insegnante, l'agenda per la programmazione didattica, i documenti di valutazione e i documenti degli alunni che saranno meglio individuati nell'opportuna sezione di questo DPS.
3. I dati sono trattati con fascicoli e atti cartacei e con strumenti elettronici di elaborazione. Per i dati sensibili si garantiranno maggiori misure di riservatezza con fascicolazione a parte, con eventuale cifratura o individuando criteri per criptare i dati stessi.
4. Il Responsabile e gli Incaricati di effettuare il trattamento dei dati utilizzano i fascicoli cartacei e computer in dotazione degli uffici.
5. I computer degli uffici di segreteria e della presidenza sono collegati in rete isolata da firewall e collegati ad internet, così come ad internet sono collegati i computer della sala docenti, biblioteca e aula informatica , fuori però dalla rete protetta da firewall (DMZ).
6. Gli Incaricati che hanno accesso ad atti e documenti informatici degli uffici sono forniti di password personali e utilizzano codici identificativi. Tali password sono adeguatamente custodite in buste chiuse dal Responsabile in luogo sicuro
7. Le aule dotate di lim sono collegate ad internet per favorire la didattica. I Docenti del Consiglio di Classe tutti sono responsabili dell'accesso a interne

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

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

- Il titolare: la persona fisica e giuridica cui compete la responsabilità finale ed assume decisioni fondamentali riferite alle modalità di trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- Il responsabile: la persona fisica, dotata di particolari caratteristiche di natura morale e di competenza tecnica, con precise capacità ed affidabilità, preposta dal titolare al trattamento dei dati personali, ivi compreso il profilo della sicurezza;
- gli incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento e che materialmente provvedono al trattamento dei dati, secondo le istruzioni impartite dal titolare e dal responsabile;

- l'amministratore di sistema: il soggetto cui è conferito il compito di "sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base di dati e di consentirne l'utilizzazione". Tale figura è individuata dall' art. 1 del DPR 318/99, mentre non viene riproposta nel D.L.vo 196/2003 che pur conserva una propria funzionalità per la garanzia delle misure di sicurezza logica del sistema informatico della gestione dei dati. Pertanto si ravvisa la necessità di individuare tale figura con delega di compiti definiti.

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

Titolare del trattamento, come definito nella Premessa, è il legale rappresentante pro tempore di questa Istituzione Scolastico, D.S. Prof.Luciano Calzamiglia.

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

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

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

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

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

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

In particolare, il Titolare del trattamento individua, designa e nomina quale Rappresentante del trattamento dei dati il DSGA di questa Istituzione Scolastica, Dott.ssa CRESPI BRUNA (C.F. CRSBRN56D45C511L), persona con capacità professionali, esperienza e affidabilità, tale da fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

Il Responsabile del trattamento dei dati ha il compito di:

- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi nella rete di trattamento dei dati, nonché l'elenco delle tipologie dei trattamenti effettuati;
- Attribuire di concerto con l'Amministratore di sistema, ad ogni utente (User) o Incaricato un codice identificativo personale (User-id), e le modalità di utilizzazione del sistema informatico;
- Verificare che le misure previste dal DPS vengano adeguatamente attuate;
- Informare il Titolare nella eventualità che si siano rilevati dei rischi.

Altresì al Responsabile del trattamento dei dati è affidato il compito di assegnare le password e le modalità d'uso delle stesse agli incaricati che provvederanno personalmente alla loro gestione, e custodire le password di amministrazione , consegnate dall'Amministratore di sistema, nell'armadio blindato dell'ufficio della Presidenza.

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

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

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

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

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

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

Agli Incaricati deve essere assegnato un codice identificativo protetto da password personalizzato.

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

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

SETTORE SERVIZI DI AMMINISTRAZIONE ALUNNI E SUPPORTO ALLA DIDATTICA

N. 1 incaricato : PANIZZI Viviana (in maternità sostituita da VALLESE Franca)

FUNZIONI DIDATTICHE

OGGETTO

Sezione Alunni
Pratiche alunni e relativi adempimenti
Infortuni (anche di 1 giorno) alunni e docenti di ogni ordine e grado
Libri di testo
Qualsiasi pratica inerente la riforma
Privacy tutto quanto relativo agli alunni
Rapporti con altre scuole
Mensa alunni e docenti pratiche generali
Trasmissione fascicoli altre scuole
Elezioni alunni /genitori
Statistiche
Attività di ed.fisica (giochi st., piscina, rugby ecc.)
Elenchi alunni per visite e viaggi istruzione
Convocazioni genitori e docenti consiglio di istituto
Tenuta registro biblioteca di Istituto
Esami di Stato e relativi adempimenti con Presidente Commissione
Circolari / Posta ai plessi on line (incarico specifico)

SETTORE SERVIZI DI AMMINISTRAZIONE DEL PERSONALE

N. 2 incaricati :

GIOIA Patrizia (Personale S.S. e Ata) FUNZIONI AMM.VE

Sezione personale docente 1° grado
Personale docente e A.T.A. e relativi adempimenti
Ricerca supplenti docenti e A.T.A. e relativi contratti
Comunicazione Centro per l'impiego
Certificati di servizio
Sostituzione Docenti Secondaria per assenze giornaliere (in mancanza D.S.)
Punto edu docenti (formazione)
Tutte le statistiche relative ai docenti e 1° grado e A.T.A.
Disoccupazione e tfr
Trasmissione fascicoli altre scuole
Decreti di assegnazione docenti alle classi
Organico in collaborazione con Balestra Maria Organico di tutto l'Istituto (inserimento portale SIDI e relative statistiche e comunicazioni)
Adeguamenti carriera docenti 1° grado e A.T.A.
Trasferimenti 1° grado e A.T.A.
Istruttoria pensionamento
Comunicazione dati di sciopero a sistema di tutto il personale
Ricostruzioni carriera di tutto il personale art.7 e aggiornamenti Sissi e Argo , Inps, Inpdap In collaborazione con D.S.G.A.

SANTORO Maria , (Personale Primarie Infanzia) FUNZIONI AMM.VE

Sezione personale docente Infanzia e Primaria + protocollo
Personale docente e relativi adempimenti
Inserimento portale SIDI supplenze giornaliere
Ricerca supplenti e relativi contratti
Comunicazione Centro per l'impiego
Certificati di servizio
Punto edu docenti (formazione)
Tutte le statistiche relative ai docenti di Scuola dell'Infanzia e Primaria
Rapporti con altre scuole
Disoccupazione e tfr
Trasmissione fascicoli altre scuole
Decreti di assegnazione docenti alle classi
Adeguamenti carriera docenti Infanzia e Primaria
Trasferimenti Infanzia e Primaria
Istruttoria pensionamento
Protocollo informatico(art. 7)
Incarico specifico: tenuta archivio vivente e storico e tenuta magazzino

SETTORE SERVIZI GENERALI - ASSISTENTE AMMINISTRATIVO

N. 1 incaricato RAMBALDI Sandra

Sezione Amministrativo/contabile
Supporto Dirigente Scolastico per POF, Piano Annuale attività.
Corrispondenza Dirigente Scolastico
Corsi on line docenti ATA
Anagrafe delle prestazioni
Stampa dei modelli cud
Registrazioni ore eccedenti
Questionari monitoraggio informatico
Inventario patrimonio Stato
Pagamento fotocopie
Collaborazione con Panizzi per supporto alunni
Collaborazione con Balestra per Cud e 770
Registrazione ore eccedenti
Incarico specifico: supporto informatico inst.Sissi e supporto plessi

SETTORE SERVIZI CONTABILI FUNZIONE AMMINISTRATIVA con funzioni vicarie

N. 1 incaricato: BALESTRA Maria

OGGETTO

Sezione Amm.vo/Contabile
Predisposizione con DSGA Programma Annuale
Tenuta registri Cassa e partitari
Variazioni al Programma
Emissione mandati (acquisizione CIG CUP e DURC) e reversali
Predisposizione C.Consuntivo con DSGA
Pagamento emolumenti personale interno
Pagamento emolumenti personale esterno
Pagamento competenze esami di licenza
Pagamento indennità varie
Tenuta registro emolumenti e acc./ritenute
Versamenti ritenute ed oneri riflessi
Compilazione dei modelli cud
Predisposizione mod.770
Anagrafe tributaria
Rapporti Inps, Inpdap Tesoro
Registro conto corrente postale
Organico in collaborazione con ass.amm.Patrizia Gioia
Stipendi / compensi di tutto il personale con tutti i relativi adempimenti
Sostituzione dsga (art.7)
Coordinamento sezione staccata di San Lorenzo al Mare (incarico specifico)
Elezioni organi Collegiali triennali (incarico specifico)
Progetti Fondazione Carige e Teatro

MISURE MINIME DI SICUREZZA (ARTT.33 SS. D.Lgs 196/2003)

Compiti della struttura	Natura dei dati trattati	Trattamenti operati dalla struttura	Ubicazione fisica	Misure di sicurezza adottate	Soggetti incaricati del trattamento
UFFICIO DI PRESIDENZA	Dati docenti cartacei Dati alunni cartacei Dati informatizzati	Dati sensibili Dati giudiziari Dati personali	Stanza A 1	Cassaforte Computer personale sotto firewall no dom.	Luciano CALZAMIGLIA
SEGRETERIA DIDATTICA	Dati docenti Dati alunni Protocollo	Dati personali docenti Dati personali alunni Dati ditte	Stanza A 2	Cassaforte Computer sotto firewall e dominio Armadi chiusi	GIOIA Annunziata SANTORO Maria PANIZZI/VALLESE
SEGRETERIA AMMINISTRATIVA E CONTABILE	Dati personale Dati ditte Dati enti	Dati personali	Stanza A 3	Computer sotto firewall e dominio	CRESPI Bruna BALESTRA Maria RAMBALDI Sandra

TUTTI I COLLABORATORI SCOLASTICI:

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

RIEPILOGO:

PLESSO DI RIVA LIGURE SEC.1 GRADO	Palmieri Donato Porrato Laura Viale Roberta Scrigna Gloriana
PLESSO DI RIVA LIGURE PRIMARIA	Centorame Annamaria Lanteri Maria Grazia
PLESSO DI S.STEFANO PRIMARIA	Castriconi Anita De Paola Silvana
PLESSO DI SANLORENZO SEC.1 GRADO e PRIMARIA	Matis Natalina Verda Manuela Gogioso Carla e Guglielmetti Anna 3 giorni sett.
PLESSO DI CIVEZZA	Di Maggio Tiziana 2 giorni sett.
PLESSO DI PIETRABRUNA INFANZIA	Carli Nicoletta 3 giorni sett. Guglielmetti Anna 2 giorni sett.
PLESSO DI PIETRABRUNA PRIMARIA	Carli Nicoletta 2 giorni sett.
PLESSO DI CIPRESSA INFANZIA	Giribaldi Danila Reina Lucia
PLESSO DI CIPRESSA PRIMARIA	Biancu Caterina Mergioti Franco
PLESSO DI POMPEIANA	Di Maggio Tiziana 3 giorni sett.
Riva Santo Stefano San Lorenzo	Gatta Roberto 18 ore

AREA DOCENTI SCUOLA DELL'INFANZIA E DI SCUOLA PRIMARIA e SCUOLA SECONDARIA

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

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

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

Vengono altresì individuati i docenti che sono responsabili dei plessi per quanto riguarda la supervisione dei laboratori informatici secondo la tabella sottoesposta:

PLESSO DI RIVA LIGURE SEC.1 GRADO	Panebianco Silvia
	Coppo Emiliana
PLESSO DI RIVA LIGURE PRIMARIA	Puopolo Rosaria
PLESSO DI S:STEFANO PRIMARIA	Modena Cecilia
PLESSO DI SANLORENZO SEC.1 GRADO	Galluzzo Paola
PLESSO DI SAN LORENZO PRIMARIA	Giretto Gabriella
PLESSO DI CIVEZZA	Pastorelli Loredana
PLESSO DI PIETRABRUNA INFANZIA	Catalano Alessandra
PLESSO DI PIETRABRUNA PRIMARIA	Brunengo Marina
PLESSO DI CIPRESSA INFANZIA	Russo Maria
PLESSO DI CIPRESSA PRIMARIA	Sacco Maria Grazia
PLESSO DI POMPEIANA	D'Agostono Catia

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

L'Amministratore di Sistema sovrintende al sistema informatico e garantisce il corretto funzionamento dei sistemi informatici e delle banche-dati .

Dato l'elevato utilizzo delle strumentazioni informatiche, il Titolare del trattamento ritiene opportuno conferire la nomina di Amministratore di Sistema all'Assistente amministrativa Sig.ra Sandra RAMBALDI (con la supervisione del prof. Roberto Molinaro), in quanto persona capace, idonea, esperta nell'utilizzo dei sistemi informatici e dei relativi programmi.

L'Amministratore di sistema , compatibilmente con gli impegni dell'incarico, è tenuto ad un adeguato autoaggiornamento.

In particolare l' Amministratore di Sistema:

- controlla il corretto funzionamento del sistema informatico e di tutti gli strumenti di sicurezza adottati;
- garantisce la massima riservatezza nel trattamento dei dati;
 - supporta gli incaricati del trattamento in caso di necessità;
- informa tempestivamente il Responsabile di anomalie nel funzionamento del sistema informatico che possono pregiudicare il corretto trattamento dei dati.

- in collaborazione con il responsabile del trattamento progetta in tempo utile le eventuali ristrutturazioni del sistema;
- fa in modo che sia prevista la disattivazione dei Codici identificativi personali (User-id), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali (User-id) per oltre 6 mesi;

ARTICOLO 5 - DIRITTI DELL' INTERESSATO

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

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

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

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

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

ARTICOLO 6 - ANALISI DEI RISCHI E GRADO DEI RISCHI CHE INCOMBONO SUI DATI

- 1) Le situazioni dei rischi che incombono sui dati possono riguardare:
 - Dati su materiale cartaceo;
 - Dati su attrezzature informatiche;
 - I luoghi e i contenitori che custodiscono sia i materiali cartacei, sia le attrezzature informatiche.
- 2) I materiali cartacei a rischio sono:
 - Raccoglitori e fascicoli che raccolgono i documenti contenuti nei fascicoli del personale;
 - Schede personali degli alunni;
 - Registri (di classe, di modulo, giornale dell'insegnante, di presenza);
 - Registro dello stato del personale;
 - Decreti e certificati sulle persone;
 - Anagrafe fornitori;
 - Contratti e convenzioni;
 - Documentazione finanziaria e contabile;
 - Registro infortuni;
 - Moduli di iscrizione, istanze, etc
 - Atti affissi agli albi.
- 3) Gli eventi che possono generare danni e che comportano rischi per la sicurezza dei dati personali si distinguono sotto un triplice aspetto:
 - a. Comportamento di tutti gli operatori (docenti, amministrativi, collaboratori):
 - sottrazioni di credenziali di autenticazione;
 - Carenza di consapevolezza, disattenzione o incuria;
 - Manomissioni e comportamenti sleali o fraudolenti;
 - Errore materiale;

- b. Eventi relativi agli strumenti:
- Azione di virus informatici o di programmi suscettibili di recare danno;
 - Spamming, spybot
 - Tecniche di sabotaggio
 - Malfunzionamento, indisponibilità o degrado degli strumenti;
 - Accessi esterni non autorizzati ;
 - Intercettazioni di informazioni in rete;
 - Attacchi dall'esterno al sistema
- c. Eventi relativi al contesto fisico-ambientale:
- Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, etc.), nonché dolosi, accidentali o dovuti ad incuria;
 - Accesso di estranei o persone non titolari di incarichi e responsabilità nel trattamento dei dati;
 - Errori umani nella gestione della sicurezza fisica;
 - Accessi esterni non autorizzati;
 - Vandalismo;
 - Intercettazioni di informazioni in rete;
 - Sottrazione di strumenti contenenti dati;
 - Guasto ai sistemi complementari (impianto elettrico, gruppo di continuità, climatizzazione, etc.).

TABELLA e GRAVITA' STIMATA:

I suddetti rischi sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione presso l'istituzione scolastica, adottando la seguente scansione:

A= alto B = basso EE = molto elevato M = medio MA = medio-alto MB = medio-basso

La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

Tabella : Analisi dei rischi

EVENTO		IMPATTO SULLA SICUREZZA DEI DATI		RIF. MISURE DI AZIONE
		DESCRIZIONE	GRAVITÀ STIMATA	
COMPORTEMENTI DEGLI OPERATORI	Furto di credenziali di autenticazione	Accesso altrui non autorizzato	M/B	Vigilanza sul rispetto delle istruzioni impartite
	Carenza di consapevolezza, disattenzione o incuria	Dispersione, perdita e accesso altrui non autorizzato	M	Formazione e flusso continuo di informazione
	Comportamenti sleali o fraudolenti	Dispersione, perdita, accesso altrui e divulgazione non autorizzati	B	Vigilanza sul rispetto delle istruzioni impartite
	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

EVENTI RELATIVI AGLI STRUMENTI	Azione di virus informatici o di malware	Perdita o alterazione, anche irreversibile, di dati, di programmi	A	Adozione di idonei dispositivi di protezione
	Spamming o altre tecniche di sabotaggio	Perdita o alterazione, anche irreversibile, di dati, di programmi impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	EE	Adozione di idonei dispositivi di protezione
	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Assistenza e manutenzione; ricambio periodico , planning di ammortamento
	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Adozione di idonei dispositivi di protezione
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	M	Adozione di idonei dispositivi di protezione
EVENTI RELATIVI AL CONTESTO	Accessi non autorizzati a locali/reparti ad accesso ristretto	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati, azione di sorveglianza dei collaboratori ed incaricati del trattamento
	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori; accesso altrui non autorizzato	MB	Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	M	Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	A	Attività di controllo, assistenza e manutenzione periodica
	Errori umani nella gestione della sicurezza fisica	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

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

1. MISURE DA ADOTTARE

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

- Individuazione e nomina del responsabile del trattamento dei dati (per l'accesso ai computer e alla rete si richiede autenticazione, identificazione e password per ogni Incaricato);
- Individuazione del Responsabile di sistema per garantire tutte le misure di sicurezza predisposte per la conservazione e utilizzazione dei dati,
- Misure di prevenzione per eliminare gli eventuali incendi con adeguate modalità di gestione degli stessi (impianto elettrico a norma, estintori, etc.);
- Individuazione dei locali e contenitori (armadi, armadi di sicurezza, armadi blindati, classificatori con serrature, apparecchiature e strumenti di raccolta dei dati adeguati e sicuri, etc.);
- Regolamentazione sia per il personale che per gli esterni nell'accesso ai locali e alle attrezzature che conservano dati, archivi e documentazione,
- Attuazione di misure di protezione attiva e passiva dei locali (porte con serrature di sicurezza, archivio, sistemi di allarme ove collocati .
- Banche dati su server con mirroring su raid del server
- Periodico salvataggio dei dati del server su unità rimovibili (i-o megazip).
- Installazione di Firewall al fine di impedire intrusioni dall'esterno
- Protezione dalle macchine con password di accesso personale e di amministrazione.
- Periodica verifica della funzionalità delle macchine.

2. CRITERI DI PROTEZIONE E GESTIONE DELLE PASSWORD

La rete che tratta i dati personali e sensibili è inclusa in un dominio protetto da firewall . Per accedere al dominio, l'utente registrato, dovrà utilizzare un profilo personale identificato da un nome utente protetto

da password personale conforme alle regole di sicurezza di lunghezza minima di 7 caratteri con scadenza massima di 42 giorni entro i quali l'utente dovrà provvedere al rinnovo pena il blocco del profilo che dovrà essere riattivato dall'amministratore di sistema

il profilo personale consente agli utenti del dominio di accedere sia al programma sissi per il quale il responsabile del trattamento provvederà ad assegnare le relative aree e funzioni e consente di accedere ai documenti personali e condivisi presenti sul server.

Gli incaricati al trattamento provvedono a gestire e tutelare le proprie password autonomamente, in caso di assenza dell'incaricato, l'amministratore di sistema, sotto precisa indicazione del responsabile del trattamento provvederà a sbloccare il profilo e/o rendere disponibili i dati relativi presenti sul server.

3. CRITERI, PROCEDURE PER GARANTIRE L'INTEGRITÀ DEI DATI

Il Responsabile del trattamento, con il supporto dell' Amministratore di Sistema, stabilisce la periodicità con cui debbono essere effettuate :

- Le copie di sicurezza delle banche di dati trattati
- La verifica della funzionalità dei sistemi di sicurezza
- La verifica e funzionalità delle macchine e programmi
- L'aggiornamento del software

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

- Il tipo di supporto da utilizzare per le copie di back-up;
- Il numero di copie di back-up effettuate ogni volta;
- Verificare se i supporti utilizzati per le copie di back-up sono riutilizzati e in questo caso con quale periodicità;
- Concordare preventivamente se per effettuare le copie di back-up si utilizzino procedure automatizzate e programmate;
- Valutare la durata massima delle unità di back-up;
- Assegnare il compito periodico di effettuare le copie di back-up agli Incaricati del trattamento.

4. CUSTODIA E CONSERVAZIONE DELLE COPIE DI BACK-UP

Le copie di back-up devono essere adeguatamente conservate a cura del Responsabile del trattamento nell'armadio blindato sito in segreteria didattica.

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

- Al Titolare del trattamento
- Al Responsabile del trattamento della sicurezza dei dati
- All' Amministratore di Sistema.
- Agli Incaricati

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

5. PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita degli stessi a causa di virus informatici, il Responsabile del trattamento dei dati stabilisce, con il supporto dell' Amministratore di sistema

Il protocollo di sicurezza relativo all'aggiornamento e alla verifica dell'adeguamento del software antivirus e di tutte quelle norme atte a proteggere il sistema dalle infezioni virali.

E' consigliabile che gli Incaricati del trattamento svolgano un'attenta azione di sorveglianza della postazione di lavoro assegnata, informando tempestivamente l'Amministratore di sistema dell'eventuale insorgenza di attacco virale rilevata dall'antivirus e qualsivoglia altra anomalia, in modo da rendere possibile l'annotazione degli eventuali virus rilevati.

In caso di rilevamento virale, ove possibile, l'Amministratore, provvederà ad individuarne la fonte in modo da prevenire eventuali ulteriori contagi.

Nel caso in cui su uno si verificasse un attacco virale non impedito o non bloccato dall'antivirus, il Responsabile del trattamento, unitamente all' Amministratore di Sistema, deve provvedere a:

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

6. PROTEZIONE DELLE AREE E DEI LOCALI

a) Sicurezza di area

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

Tutte le scuole sono dotate di impianto elettrico a norma e di appositi estintori.

Si precisa inoltre che:

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

Tabella : Elenco delle banche dati collocazione

BANCA DATI INTERESSATA	TIPO DATI	TIPO DI SUPPORTO	AREA	STRUTTURA INTERESSATA
Registro infortuni	personali	Cartaceo condivisa su server	comune	Armadio segreteria didattica Server segreteria contabile
Registro protocollo riservato	Sensibili e giudiziari	cartaceo	comune	Cassaforte presidenza
Registro certificati	personali	cartaceo	comune	Armadio segreteria didattica
Registro protocollo	Personali generici	Cartaceo e informatico	comune	segreteria didattica
Archivio titolario	personali	Cartaceo, condivisa su server	comune	Armadio segreteria didattica Server segreteria contabile
Registro iscrizioni	personali	Sissi su server Cartaceo	alunni	Server segreteria contabile Armadio segreteria didattica
Registro trasferimenti	personali	Sissi su server	alunni	Server segreteria contabile
Registro diplomi	personali	cartaceo	alunni	Armadio segreteria didattica
Registro c/c postale	personali	cartaceo	alunni	Armadio segreteria didattica
Fascicoli pers.alunni	Sensibili e giudiziari	Cartaceo Sissi su server	alunni	Armadio segreteria didattica Server segreteria contabile
Fascicoli diagnosi	Sensibili	cartaceo	alunni	Cassaforte presidenza
Registri classe	personali	Cartaceo Sissi su server	alunni	Armadio di classe Server segreteria contabile
Registri pers.docenti	personali	Cartaceo Sissi su server	alunni	armadio chiuso aula docenti Server segreteria contabile
Registro verbali collegio docenti	personali	cartaceo	comune	Armadio segreteria contabile
Registro ruolo	personali	Cartaceo Sissi su server	personale	Armadio segreteria didattica Server segreteria contabile
Registro no ruolo	personali	Cartaceo Sissi su server	personale	Armadio segreteria didattica Server segreteria contabile
Registri assenze doc e ata	personali	Cartaceo Sissi su server	personale	Armadio segreteria didattica Server segreteria contabile
Fascicoli personale docenti e ata	personali	Cartaceo Sissi su server	personale	Armadio segreteria didattica Server segreteria contabile
Pratiche trasferimenti	Personale	SIDI	Personale	Segreteria didattica
Gestione graduatorie doc. e ata	Personale	SIDI	personale	Segreteria amministrativa
Pratiche giudiziarie	Dati giudiziari	cartaceo	personale	Cassaforte presidenza
Registro emolumenti	personali	**** Argo cartaceo	amministrativo	Client in segreteria amm.va Armadio segreteria amm.va
Bilancio	Personali	Argo	Amministrativo	Client in segreteria amm.va Armadio segreteria amm.va
Registro contratti	personali	Cartaceo Sissi su server	amministrativo	Armadio segreteria didattica Server segreteria contabile
Registro minute spese	personali	Cartaceo Sissi su server	amministrativo	Cassetto chiuso seg. Contabile Server segreteria contabile
Registro accantonamento ritenute	personali	Cartaceo Sissi su server	amministrativo	Cassetto chiuso seg. Contabile Server segreteria contabile
Conguaglio fiscale dipendenti	personali	Cartaceo Dati on line ministero finanze	amministrativo	Cassetto chiuso seg. Contabile Client segreteria contabile

Registro anagrafe prestazioni	personali	Cartaceo Dati on line ministero finanze	amministrativo	Cassetto chiuso seg. Contabile Client segreteria contabile
Registro verbali consiglio istituto	personali	Cartaceo condivisa su server	amministrativo	armadio seg. Contabile Server segreteria contabile
Registro RSU	personali	Cartaceo condivisa su server	amministrativo	armadio seg. Contabile Server segreteria contabile

Tabella : Le misure di sicurezza adottate

MISURA	RISCHIO CONTRASTATO	STRUTTURA INTERESSATA	EVENTUALE BANCA DATI INTERESSATA	MISURA GIÀ IN ESSERE	PERIODICITÀ E RESPONSABILITÀ DEI CONTROLLI
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile di dati, accesso altrui non autorizzato	Segreteria Presidenza cartaceo	Registro protocollo riservato, fascicoli diagnosi, pratiche giudiziarie Registro verbali collegio docenti	Cassaforte blindata, locale chiuso, accesso riservato Misure di protezione e sicurezza	Quotidiana attraverso la presenza del dirigente scolastico
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile di dati, accesso altrui non autorizzato	Segreteria didattica cartaceo	Registro infortuni Registro certificati Registro protocollo Archivio titolario Registro iscrizioni Registro diplomi Registro c/c postale Fascicoli personali alunni Registro ruolo Registro no ruolo Registro assenze Fascicolo pers.docenti e ata Registro contratti Registro emolumenti	Armadi e cassetti chiusi Locale chiuso con accesso riservato Misure di protezione e sicurezza	Quotidiana attraverso gli incaricati del trattamento
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Segreteria didattica Programma sissi su server condivisa su server	Registro infortuni Archivio titolario Registro iscrizioni Registro trasferimenti Fascicoli personali alunni Registri di classe Registri pers.docenti Registro ruolo Registro no ruolo Registro assenze Fascicolo pers.docenti e ata Registro contratti	Rete sotto dominio protetta da Firewall Mirroring raid su server Back-up periodico dei dati Antivirus Aggiornamenti periodici Credenziali di autenticazione personali e di amministrazione	Quotidiani da parte degli incaricati del trattamento trimestrali dell'amministrato re di sistema Back-up mensile Trimestrali cambi password personali e aggiornamenti periodici
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile di dati, accesso altrui non autorizzato	Servizi amministrativi cartaceo	Registro minute spese Registro accantonamento ritenute Conguaglio fiscale dipendenti Registro anagrafe prestazioni Registro verbale consiglio Registro RSU	Armadi e cassetti chiusi Locale chiuso con accesso riservato Misure di protezione e sicurezza	Quotidiana attraverso gli incaricati del trattamento

Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi amministrativi Programma sissi su server condivisa su server	Registro minute spese Registro accantonamento ritenute Registro verbale consiglio Registro RSU	Rete sotto dominio protetta da Firewall Mirroring raid su server Back-up periodico dei dati Antivirus Aggiornamenti periodici Credenziali di autenticazione personali e di amministrazione	Quotidiani da parte degli incaricati del trattamento trimestrali dell'amministratore di sistema Back-up mensile Trimestrali cambi password personali e aggiornamenti periodici
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile di dati, accesso altrui non autorizzato	Aule Cartaceo Armadio di classe Armadio chiuso aula docenti	Registri di classe Registri personali docenti	Armadi e cassetti chiusi Locale chiuso con accesso riservato Misure di protezione e sicurezza	Quotidiana attraverso gli incaricati del trattamento
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi amministrativi Programma argo su client Segreteria didattica	Registro emolumenti	Rete sotto dominio protetta da Firewall Back-up periodico dei dati Antivirus Aggiornamenti periodici Credenziali di autenticazione personali e di amministrazione	Quotidiani da parte degli incaricati del trattamento trimestrali dell'amministratore di sistema Back-up mensile Trimestrali cambi password personali e aggiornamenti periodici
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi amministrativi Client con collegamento on line MEF Segreteria contabile	Conguaglio fiscale dipendenti Registro anagrafe prestazioni	Rete sotto dominio protetta da Firewall Antivirus Aggiornamenti periodici Credenziali di autenticazione personali e di amministrazione	Quotidiani da parte degli incaricati del trattamento trimestrali dell'amministratore di sistema Back-up mensile Trimestrali cambi password personali e aggiornamenti periodici

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

- 1) Per prevenire e diminuire i danni causati da danneggiamenti, smarrimenti, inaffidabilità della base dati:
 - a) per i dati cartacei si potrà ricostruire copia da documenti e atti in possesso degli interessati (personale in genere) o di altri enti cui sono stati trasmessi (Scuole, MIUR, Ufficio Scolastico Regionale, CSA, ASL, Comune);
- 2) per i dati informatici si utilizzerà il restore dalle copie di back-up; se questo non fosse possibile si potranno ricostruire i dati danneggiati da atti e documenti cartacei. L'amministratore di sistema provvederà periodicamente alla verifica del corretto funzionamento del sistema di back up delle basi dati tramite simulazioni di ripristino.
- 3) Il Responsabile del trattamento, d'intesa con gli Incaricati di collaborare nell'Amministrazione di Sistema, ha il compito di verificare di sovente o almeno ogni sei mesi la situazione dei Sistemi operativi installati sulle apparecchiature con le quali vengono trattati i dati. La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda:
 - La sicurezza dei dati trattati
 - Il rischio di distruzione o di perdita dei dati
 - Il rischio di accesso non autorizzato o non consentito
- 4) Ad evitare danneggiamento o perdita di dati si rende estremamente importante:
 - La periodica e attenta manutenzione dei sistemi operativi utilizzati, l'aggiornamento tempestivo e la sostituzione dei sistemi operativi qualora si riscontrassero evidenti carenze nella sicurezza degli stessi.

ARTICOLO 9 – INTERVENTI FORMATIVI PER GLI INCARICATI DEL TRATTAMENTO

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno i bisogni formativi di cui necessitano gli Incaricati, specie per le innovazioni che nel campo telematico/tecnologico/informatico avvengono di continuo. E' necessario tenere il personale in tale campo continuamente informato e all'altezza dei compiti che devono espletare, per meglio conoscere i rischi che incombono sui dati, per avere una ottimale conoscenza delle misure di sicurezza e degli adeguati comportamenti da adottare, delle responsabilità circa i dati danneggiati, persi o distrutti.

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

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

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

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

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

Per gli Incaricati del trattamento un corso si rende urgente immediatamente dopo l'affidamento dei compiti e delle responsabilità e comunque entro il secondo semestre dell'anno scolastico in corso. Sarà messo a disposizione del personale il D. L vo 196/2003.

ARTICOLO 10 – NORME FINALI

Il “DPS” potrà essere integrato e aggiornato in qualunque periodo dell’anno, ma almeno entro il 31 marzo di ogni anno.

Per quanto non regolamentato nel presente DPS si applicano le norme contenute nel D.L.vo 196/2003, nel D.M.7 dicembre 2006 n.305 e nella Direttiva ministeriale 30 novembre 2007 n.104.

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

Il presente documento verrà portato all’attenzione della Giunta Esecutiva e del Consiglio di Istituto del 30/06/2011, con gli eventuali adeguamenti che potrebbero derivare dalla verifica annuale dell’assegnazione degli incarichi e delle specifiche competenze, come previsto dall’allegato B, n. 26 sul Disciplinare tecnico in materia di misure minime di sicurezza, per riferire sulla sua avvenuta redazione con data certa, per informazione ai componenti, per adozione ed assunzione di delibera, anche al fine di porre il Titolare in grado di attuare gli adeguamenti fisici, logistici, tecnologici ed informatici urgenti e necessari per le finalità previste dalla legge.

Gli allegati al presente documento ne formano parte integrante e sono così specificati:

- Informativa Ditte/Enti/Associazioni
- Informativa tutto il personale dipendente
- Informativa amministratore di sistema
- Ordine di servizio relativo a tutto il personale dipendente
- Acquisizione delle manleve

Il presente documento è aggiornato al 23.03.2011.

Titolare del trattamento dei dati
(Luciano Calzamiglia)