ISTITUTO DI ISTRUZIONE SUPERIORE “PIER LUIGI NERVI”
Via San Bernardino da Siena, 10 – 28100 Novara
Tel. 0321 625790 – fax 0321 629734
E mail dirigente_scolastico@itgnervi.com noit006003@itgnervi.com

REGOLAMENTO E PROCEDURE PER IL TRATTAMENTO DEI DATI

Visto l’art. 34 e la regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali D.lgs. N. 196 del 30/06/2003

Visto il Decreto Ministeriale n. 305 del 7 dicembre 2006 pubblicato in G.U. n. 11 del 15 gennaio 2007, con il quale è stato adottato il Regolamento relativo al trattamento dei dati sensibili e giudiziari nel settore dell’istruzione

Visto il Decreto legge n. 5 del 03/02/2012, “Disposizioni urgenti in materia di semplificazione e sviluppo”, che modifica l’art. 34 e l’allegato B del D.lgs. N. 196 del 30/06/2003

SCOPO

Il presente documento rappresenta una misura minima di sicurezza predisposta dall’Istituto Scolastico ISTITUTO DI ISTRUZIONE SUPERIORE “PIER LUIGI NERVI” .

Lo scopo è quello di informare circa la struttura dei dati trattati, delle persone responsabili dei trattamenti dei dati, dei rischi che incombono sui dati e delle contromisure preventive e di recupero da disastri adottate.

Il presente documento è stato redatto dal Prof. ROBERTO SACCHI in qualita’ di Legale Rappresentante dell’Istituto Scolastico ISTITUTO DI ISTRUZIONE SUPERIORE “PIER LUIGI NERVI” e, quale Titolare, provvede a firmarlo in calce.

1. TRATTAMENTO DEI DATI PERSONALI

Elenco dei trattamenti dei dati personali

L’Istituto scolastico ISTITUTO DI ISTRUZIONE SUPERIORE “PIER LUIGI NERVI” per le sue finalità istituzionali tratta direttamente o per mezzo di collaborazioni esterne i seguenti 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.

DATO ANONIMO : il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u) del DPR 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.

Tabella 1 : elenco dei trattamenti, informazioni di base

Identificativo Del trattamento	Descrizione sintetica	Natura dei dati trattati P=personale G=giudiziario S=sensibile	Struttura interna di riferimento	Struttura esterna che concorre al trattamento	Descrizione strumenti utilizzati
A01	Alunni – Dati personali trattati dai Docenti	P-S	Corpo docente	NO	Stazioni di lavoro - Cartaceo
A02	Alunni – Dati personali trattati da Assistenti Amministrativi e D.S.G.A.	P-S	Segreteria didattica-uffici segreteria	P.A	Stazioni di lavoro-cartaceo-telefono
A03	Personale dipendente –– Dati personali trattati da Assistenti Amministrativi e D.S.G.A. e revisori contabili	P-S	Segreteria	P.A.- revisori dei conti	Stazioni di lavoro-cartaceo-telefono
A04	Collaborazioni professionali – Clienti e fornitori – Dati personali trattati da Assistenti Amministrativi e D.S.G.A.	P-S	Segreteria e Ufficio Tecnico	NO	Stazioni di lavoro-cartaceo-telefono
A05	Gestione finanziaria e del bilancio—Dati personali trattati da Assistenti Amministrativi e D.S.G.A..	P-S	Segreteria	P.A.-Revisori contabili	Stazioni di lavoro-cartaceo-telefono
A06	Gestione Istituzionale e Protocollo—Dati personali trattati da Assistenti Amministrativi e D.S.G.A.	P-S	Segreteria	NO	Stazioni di lavoro-cartaceo-telefono
A07	Gestione di trattamenti da parte della componente esterna di organi collegiali o di commissioni di esame.	P-S	Organo collegiale-commissione d'esame	P.A.	Cartaceo

A08	Trattamenti di dati personali effettuati da Personale Ausiliario e Tecnico e organi sindacali	P-S	Collaboratori Scolastici, Assistenti Tecnici, RSU	Organi sindacali	Stazioni di lavoro-cartaceo-telefono
A09	Comunicazioni alle famiglie – Dati personali e sensibili trattati da Assistenti Amministrativi e Docenti	P-S	Segreteria e docenti	Famiglia	Stazioni di lavoro-Cartaceo - telefono
A10	Comunicazioni al personale – Dati personali e sensibili trattati da Assistenti Amministrativi e D.S.G.A.	P-S	Segreteria	NO	Stazioni di lavoro-cartaceo-telefono
A11	Sanitari e giudiziari – dati relativi al personale, agli studenti e alle famiglie trattati da assistenti amministrativi, D.S.G.A., docenti ed eventuali assistenti sociali incaricati dal Comune o dalle ASL, eventuali esperti o consulenti esterni	S-G	Segreteria – docenti	P.A. ed esperti	Stazioni di lavoro-cartaceo-telefono
A12	Gestione protocollo riservato – dati giudiziari di tutto il personale dipendente e degli alunni : l'accesso è consentito solo al Titolare del trattamento.	P-S-G	Titolare	NO	Stazioni di lavoro-cartaceo-telefono
A13	Assistenza tecnica hardware e software – l'accesso è consentito al tecnico esterno avente incarico specifico	P-S	NO	Ditta esterna	Stazioni di lavoro-cartaceo-telefono

Dati personali in ingresso

I documenti cartacei sono acquisiti dal Responsabile del trattamento dei dati; quelli riservati sono sempre consegnati in busta chiusa al Dirigente Scolastico. I documenti pervenuti tramite FAX o consegnati aperti vengono subito consegnati al Dirigente Scolastico.

Documenti in uscita

I documenti in uscita vengono trattati solo dal personale incaricato, protocollati e predisposti per le spedizioni in busta chiusa. I documenti che contengono dati riservati vengono messi in busta chiusa ed inseriti nel plico contenente la lettera di trasmissione nella quale è evidenziata la presenza di documentazione riservata.

Strutture e strumenti di riferimento nella trattazione dei dati personali

Tutti i dati posseduti dalla Scuola vengono trattati presso gli Uffici della sede centrale dell'Istituto, ubicata a Novara in Via San Bernardino da Siena, 10 e negli Uffici della sede associata ubicata a Novara, in Viale Liguria, 5.

Nella sede centrale è presente un server ubicato negli Uffici di segreteria, e il personale amministrativo in servizio non è a conoscenza della password per la sua accensione, ad eccezione dell'incaricato per gli interventi urgenti e inderogabili. Essa è conservata in busta chiusa a cura della DSGA, Responsabile del Trattamento dei dati. La gestione del server è affidata all'Amministratore di sistema esperto informatico, all'aggiornamento del servizio antivirus. Nel server sono installati i programmi di gestione utilizzati solo dalla Segreteria. Le copie di backup vengono effettuate quotidianamente.

Al server sono collegati n. 11 client: 3 negli Uffici di Segreteria per la gestione delle pratiche amministrative e contabili; 4 negli Uffici di Segreteria per la gestione delle pratiche didattiche e del protocollo; 1 nell'Ufficio del DSGA, per la gestione delle pratiche amministrative e 1 nell'Ufficio della collaboratrice della DSGA per le pratiche amministrative; 1 nell'Ufficio di presidenza e 1 nell'Ufficio della vicepresidenza.

L'accesso al computer e quindi ai programmi da parte del personale è consentito con password appositamente assegnata all'assistente amministrativo responsabile dell'area lavoro.

Da tutte le postazioni degli Uffici di Segreteria è possibile accedere a Internet tramite un router con collegamento ADSL; al personale amministrativo è consentita la navigazione in internet solo per visualizzare siti istituzionali e di Enti con i quali l'Istituto intrattiene rapporto di lavoro.

E' fatto divieto di visualizzare e scaricare posta elettronica da domini diversi da quelli istituzionali.

Tutti i PC sono dotati di software antivirus aggiornati direttamente sul server dalla Ditta a cui è stata affidata l'assistenza tecnica.

La Segreteria è dotata di fax per la ricezione e la trasmissione di documenti cartacei. Non sono presenti dispositivi di collegamento wireless.

Nella sede associata e nella sede centrale sono presenti computer utilizzati per la didattica.

2. DISTRIBUZIONE COMPITI E RESPONSABILITÀ

TITOLARE: Il titolare del trattamento è l'Ente e la titolarità è esercitata dal rappresentante legale; tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza

delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La sua designazione non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile è un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il Responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le ha le responsabilità indicate nella lettera di incarico.

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 dati e di consentirne l'utilizzazione. In questo contesto assume le funzioni di amministratore di sistema, ovvero del soggetto che deve sovrintendere alle risorse di rete e consentirne l'utilizzazione. L'Amministratore è un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.
Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile, che tratta i dati personali. Gli Incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

3. TITOLARE, RESPONSABILI, INCARICATI

Titolare del trattamento: Dirigente scolastico

Responsabile del trattamento dei dati: Direttore dei Servizi Generali e Amministrativi

Custode delle password: Direttore dei Servizi Generali e Amministrativi

Incaricati dell'assistenza e della manutenzione degli strumenti elettronici: gli assistenti tecnici, in virtù e nei limiti delle lettere dell'incarico conferito specificatamente

Incaricato Amministratore di sistema: Incarico conferito con specifica lettera di nomina depositata agli atti della scuola

Incaricati del trattamento dei dati: tutti i docenti, tutto il personale di segreteria, tutti i collaboratori scolastici e gli assistenti tecnici in virtù e nei limiti delle lettere dell'incarico conferito specificatamente

Possono trattare i dati eventuali soggetti interni od esterni all'Istituto Scolastico, laddove siano incaricati in modo permanente o temporaneo dello svolgimento di attività che comportano trattamento di dati personali.

4. TRATTAMENTI AFFIDATI ALL'ESTERNO

In questa sezione è riportato il quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi

Descrizione sintetica dell'attività esternalizzata	Trattamento di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Manutenzione PC e reti	Interventi di riparazione, ripristino, aggiornamento hardware e software	Ditta esterna	Indicazioni di responsabilità inserite nel contratto
Software didattici; registro elettronico	Ripristino, implementazione e aggiornamento	Infoschool Bassano del Grappa	Indicazioni di responsabilità inserite nel contratto

5. ANALISI DEI RISCHI E DELLE MINACCE

La ricognizione e l'analisi dei rischi, che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuita, in grado di recare pregiudizio ai dati personali trattati, è stata riportata nelle tabelle che seguono nelle quali gli eventi sono stati suddivisi in tre categorie:

1) Comportamenti degli operatori.
Sottrazione di credenziali di autenticazione; carenza di consapevolezza, disattenzione o incuria; comportamenti sleali o fraudolenti; errori materiali.

2) Eventi relativi agli strumenti.
Danno arrecato da virus informatici o da programmi suscettibili di recare danno; spamming o tecniche di sabotaggio; malfunzionamento, indisponibilità o usura degli strumenti; accessi esterni non autorizzati; intercettazione di informazioni in rete.

3) Eventi relativi al contesto fisico-ambientale.
Accessi non autorizzati a locali ad accesso ristretto; eventi distruttivi naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.) nonché dolosi, accidentali o dovuti ad incuria; guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc); errori umani nella gestione della sicurezza fisica.

I suddetti rischi sono stati ripartiti in classi di gravità, nella tabella seguente, tenendo conto della concreta possibilità di realizzazione, adottando la seguente scansione riferita al possibile

impatto sulla sicurezza:
Alta - Media - Bassa

Tabella 2 – Analisi dei rischi (regola 19.3 del disciplinare tecnico)

	Id	*Rischi*	*Si/No*	*Descrizione dell'impatto sulla sicurezza*
Comportamento degli operatori	**1**	**Sottrazione di credenziali di autenticazione.**	**Si**	**Alta**
	2	**Carenza di consapevolezza, disattenzione o incuria.**	**Si**	**Media**
	3	**Comportamenti sleali o fraudolenti.**	**Si**	**Bassa**
	4	**Errore materiale.**	**Si**	**Media**
Eventi relativi agli strumenti	**5**	**Azione di *virus* informatici o di programmi suscettibili di recare danno (quali spyware, adware, trojan, attivabili a seguito di collegamenti nascosti e che possono rilevare informazioni o anche password).**	**Si**	**Alta**
	6	***Spamming* (saturazione di risorse informatiche a seguito di invio di molti messaggi di posta elettronica) o tecniche di sabotaggio (password cracking e "bombe logiche": queste ultime si attivano anche a distanza di tempo e possono impedire il funzionamento del sistema).**	**Si**	**Alta**
	7	**Malfunzionamento, indisponibilità o degrado degli strumenti, dovuti a guasti, eventi naturali, disturbi elettrici e black-out, sabotaggi**	**Si**	**Media**
	8	**Accessi esterni non autorizzati.**	**Si**	**Media**
	9	**Intercettazione di informazioni in rete.**	**Si**	**Media**
Eventi relativi al contesto	**10**	**Accessi non autorizzati a locali/reparti ad accesso ristretto.**	**Si**	**Bassa**
	11	**Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc,) nonché dolosi, accidentali o dovuti ad incuria.**	**Si**	**Media**
	12	**Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.).**	**Si**	**Media**
	13	**Errori umani nella gestione della sicurezza fisica.**	**Si**	**Media**

Minacce a cui sono sottoposti i supporti di memorizzazione:

Le principali minacce sono le seguenti:

1. distruzione e/o alterazione a causa di eventi naturali
2. imperizia degli utilizzatori
3. sabotaggio
4. deterioramento nel tempo (invecchiamento dei supporti)
5. difetti di costruzione del supporto di memorizzazione che ne riducono la vita media
6. evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti

v. allegato 2

6. INDIVIDUAZIONE DELLE VULNERABILITÀ

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nell'articolo 5.

Infrastruttura	*Hardware*	*Comunicazioni*
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione inadeguata della rete
		Connessioni a linea pubblica non protette
Documenti cartacei	*Software*	*Personale*
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Mancato controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

7. INDIVIDUAZIONE DELLE CONTROMISURE

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

contromisure di carattere fisico
contromisure di carattere procedurale
contromisure di carattere elettronico/informatico

Contromisure di carattere fisico

Sono definite aree ad accesso controllato quei locali che contengono apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati sensibili e apparecchiature di telecomunicazione) e archivi informatici e/o cartacei contenenti dati personali o sensibili/giudiziari.

In particolare, il locale ove è ubicato il server, comunica solo con la Segreteria e non ha accesso alla pubblica via.

Le due sedi dell'Istituto sono protette da allarme antifurto, con sensori interni anti-intrusione.

Le sale insegnanti sono dotate di cassettiere con chiusura a chiave, ove vengono riposti i registri personali dei docenti e gli elaborati degli alunni.

Per tali aree vale quanto segue :

1. Il Responsabile nominato dal Titolare del trattamento dei dati è anche responsabile delle aree in cui si trovano le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati sensibili e apparecchiature di telecomunicazione) nonchè gli archivi informatici e/o cartacei contenenti dati personali o sensibili/giudiziari.
2. i locali sono chiusi o presidiati; le chiavi di accesso ai plessi scolastici sono affidate al Dirigente Scolastico, al DSGA, ai collaboratori scolastici.
3. l'accesso agli Archivi viene consentito solo alle persone autorizzate;
4. i locali sono provvisti di estintore e di sistema antincendio;
5. I computer, incluso il server, risultano tutti sollevati da terra, in modo da evitare eventuali perdite di dati dovute ad allagamenti; il server è collegato ad un gruppo di continuità che consente di escludere la perdita di dati derivante da sbalzi di tensione o interruzione di corrente elettrica.

Contromisure di carattere procedurale

In generale per i locali che contengono documenti riguardanti dati sensibili, cartacei e/o informatici sono definite le seguenti regole di gestione:

1. il Responsabile predispone la lista delle persone autorizzate ad accedere alle aree ad accesso controllato;
2. la lista deve essere periodicamente controllata;
3. i visitatori occasionali devono essere accompagnati;
4. gli ingressi fuori orario devono essere controllati;
5. deve essere assicurata l'esecuzione di test periodici sull'efficacia degli estintori;
6. il personale delle ditte che provvedono ad effettuare prestazioni che comportano accesso di estranei ai locali, vengono accompagnati da personale interno autorizzato.

Per il trattamento dei dati cartacei devono essere osservate le seguenti norme:

1. individuazione scritta di tutti gli incaricati del trattamento delle informazioni mediante l'elenco dei trattamenti sensibili (vedi Art.2);
2. accesso ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
3. utilizzo di archivi con accesso selezionato;
4. restituzione di atti e documenti al termine delle operazioni;
5. divieto di fotocopiare documenti senza l'autorizzazione del Titolare o del Responsabile;
6. divieto di abbandonare incustodito il proprio posto di lavoro;
7. divieto di abbandonare incustodita documentazione cartacea contenente dati personali e/o sensibili;
8. divieto assoluto di esportare documenti o copie dei medesimi all'esterno dell'Istituto Scolastico senza l'autorizzazione del Titolare o del Responsabile, tale divieto si estende anche all'esportazione telematica;
9. il materiale cartaceo utilizzato per la predisposizione di documenti in originale deve essere opportunamente distrutto in modo da renderlo inintellegibile; è fatto assoluto divieto di riciclare in qualsiasi modo materiale cartaceo contenente dati.
10. l'accesso di dipendenti o estranei per la pulizia dei locali contenenti dati personali dev'essere effettuata solo con i contenitori chiusi a chiave. Se dati personali non sono rinchiusi in un contenitore, la pulizia deve essere effettuata alla presenza di un Incaricato del trattamento di tali dati. Durante l'accesso per la pulizia tutti i computer contenenti dati sensibili o giudiziari devono essere spenti (o in modalità salvaschermo con password di ripristino) oppure deve presenziare un Incaricato del trattamento di tali dati.
11. i registri di classe, contenenti dati comuni e particolari, durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni nella sede centrale il docente dell'ultima ora deposita il registro in segreteria, dove viene conservato in apposito armadio chiuso a chiave; nella sede associata, il docente dell'ultima ora lo deposita in apposita rastrelliera in sala insegnanti, che viene chiusa a chiave.
12. il docente è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del docente che è chiuso a chiave
13. il protocollo riservato, accessibile solo al Titolare, è conservato in apposito armadio di sicurezza.

In particolare, i dati trattati su supporto cartaceo sono collocati in appositi schedari dislocati negli uffici di segreteria e muniti di chiave.

I registri dei Verbali dei Consigli di classe sono custoditi in apposito armadio chiuso a chiave nell'Ufficio di Segreteria della sede centrale e nell'Ufficio di vicepresidenza della sede associata. I registri dei Verbali degli altri Organi Collegiali sono custoditi in apposito armadio chiuso a chiave collocato nell'Ufficio del DSGA.

Contromisure di carattere elettronico/informatico

Per le norme relative al trattamento informatizzato dei dati si rimanda all'Allegato 3

Alle contromisure sopra elencate, si aggiungono le disposizioni interne per il corretto utilizzo della rete, per le quali si rimanda al Regolamento per l'utilizzo della rete (Allegato 1)

.

8. NORME PER IL PERSONALE

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete di cui all'Allegato 1.

9. PIANO DI FORMAZIONE / INFORMAZIONE

La formazione/informazione degli incaricati viene effettuata all'ingresso in servizio, al mutamento di incarico, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale e/o periodicamente in funzione della variazione degli organici della scuola. Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali.

Inoltre, essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi (hardware e software) e, nel dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile o giudiziaria.

Gli interventi formativi avvengono, oltre che attraverso specifici incontri stabiliti dal Titolare del trattamento in circostanze di necessità come sopra descritte, anche attraverso la consegna di materiale esplicativo riguardante le norme, gli adempimenti richiesti, nonché le misure minime di sicurezza che sono esplicitate nelle linee guida al trattamento dei dati allegate alle lettere di incarico.

Il personale supplente temporaneo che prenderà servizio durante il corso dell'anno scolastico verrà informato sui contenuti del presente Documento e sui doveri da esso derivanti, tramite la consegna della lettera di incarico corredata delle opportune linee guida, e la visione del Documento stesso, che viene esposto all'albo della scuola

10. REVISIONE E INTEGRAZIONE DEL REGOLAMENTO E DELLE PROCEDURE PER LA PROTEZIONE DEI DATI

Il presente documento è soggetto a revisione e integrazione ogni qualvolta si verificano le seguenti condizioni:

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

11. ATTIVITA' DI CONTROLLO E DI VALUTAZIONE

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Responsabile del trattamento, in collaborazione con il Titolare e l'Amministratore di sistema, provvede anche con verifiche casuali a controllare che le misure adottate siano effettivamente e adeguatamente applicate e che gli strumenti e i supporti siano in piena efficienza.

In sede di valutazione, il Titolare del trattamento coadiuvato dal Responsabile del trattamento e dall'Amministratore di sistema, analizza l'efficacia degli strumenti adottati al fine di rivedere se necessario l'indice di gravità dei rischi, controllando quali danni si sono avuti o quali siano possibili, la frequenza degli accadimenti registrati, le circostanze in cui si sono subiti attacchi, individuare le misure risultate inadeguate e che vanno riconsiderate.

12. 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 (assistentato materiale), è escluso, nei limiti del possibile, l'accesso dei medesimi a documentazione contenente 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 Decreto legislativo 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.

Elenco Allegati costituenti parte integrante di questo documento

Allegato 1 - Regolamento per l'utilizzo della rete
Allegato 2 - Minacce
Allegato 3 – Rilevamento, risposta all'incidente e ripristino
Allegato 4 - Videosorveglianza
Lettere di incaricato del trattamento dei dati con relative linee guida
Lettera di incarico del Responsabile del Trattamento dei dati
Lettera di incarico di Amministratore di sistema
Informative per famiglie, dipendenti e fornitori
Regolamento trattamento dati sensibili

Data _____ Firma del Titolare

_____

Al presente documento è stata attribuita data certa mediante l'inserimento in oggetto di atto deliberativo pronunciato dal Consiglio di Istituto riunito nella seduta del 27 marzo 2013, Delibera n. 26/2013