



Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO "B. R. MOTZO"
SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO
08011 - BOLOTANA - (NU)

Prot. N. 624/C23

Bolotana 31/03/2006

PRIVACY

(D.L.vo N. 196/2003)

DISPOSIZIONI MINIME SULLA SICUREZZA
E
DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali)
(D.L.vo N. 196 del 30/06/2003)

Il responsabile della sicurezza
(ing. Giuseppe Pilia)

(firma)

Premessa

Scopo di questo documento è disciplinare le modalità di trattamento dei dati personali, in formato cartaceo e elettronico e stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare, affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato dall'istituto comprensivo B. R. Motzo di Bolotana" (Nu) previsti dal D.L.vo 30/06/2003 N° 196 "Codice in materia di protezione dei dati personali". Il presente documento è stato redatto dal Dirigente Scolastico in qualità di responsabile della sicurezza, che provvede a firmarlo in calce. Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Articolo 1 - Normativa di riferimento

- D.L.vo n. 196 del 30/06/2003;
- Regolamento per l'utilizzo della rete.

Articolo 2 - Definizioni e responsabilità

Per **Amministratore di sistema** si intende 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 l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere 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.

Per **Custode delle password** si intende il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

Per **dati anonimi** si intende i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

Per **dato personale** si intende 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;

Per **dati identificativi** si intende i dati personali che permettono l'identificazione diretta dell'interessato.

Per **dato sensibile** si intende qualsiasi dato personale idoneo 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;

Per **dato giudiziario** si intende qualsiasi dato personale idoneo 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.

Per **incaricato** si intende il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

Per **interessato** si intende il soggetto al quale si riferiscono i dati personali.

Per **responsabile del trattamento** si intende il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e 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 deve essere 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 responsabilità indicate nella lettera di incarico.

Per **responsabile della sicurezza informatica** si intende il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e 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 deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

Per **titolare** si intende il titolare del trattamento che è l'**Istituzione scolastica** e la titolarità è esercitata dal rappresentante legale (**Dirigente Scolastico**), 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.

Articolo 3 - Titolare, responsabili, incaricati

- Titolare del trattamento;
- Responsabile del trattamento dei dati;
- Responsabile della sicurezza informatica;
- Amministratore della rete;
- Custode delle password;
- Incaricati del trattamento dei dati;
- Incaricato dell'assistenza e della manutenzione degli strumenti elettronici;

Articolo 4 - Analisi dei rischi

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

L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

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

- 1) **Dati anonimi**, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- 2) **Dati personali**:
 - **Dati personali semplici**, ovvero la classe di dati a rischio intermedio

- **Dati personali sensibili/giudiziari**, ovvero la classe di dati ad alto rischio;
- **Dati personali sanitari**, ovvero la classe di dati a rischio altissimo.

Articolo 5 - Individuazione delle risorse da proteggere

Le risorse da proteggere sono:

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

Articolo 6 - Individuazione delle minacce

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse indicate all'articolo 5.

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione			X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi	X		
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di acqua	X		
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere		X	X
Radiazioni elettromagnetiche			
Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria		X	
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		
Uso illegale di software	X	X	

Rischi	Deliberato	Accidentale	Ambientale
Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	
Intercettazione (Eavesdropping)	X		
Infiltrazione nelle comunicazioni	X		
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Ripudio	X		
Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	

Minacce a cui sono sottoposte le risorse hardware

Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;
- malfunzionamenti dovuti a sabotaggi, furti, intercettazioni (appareati di comunicazione).

Minacce a cui sono sottoposte le risorse connesse in rete

Le principali minacce alle risorse connesse in rete possono provenire dall'interno dell'istituto, dall'esterno o da una combinazione interno/esterno e sono relative:

- all'utilizzo della LAN/Intranet (interne);
- ai punti di contatto con il mondo esterno attraverso Internet (esterne);
- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le seguenti tecniche:

Ip spoofing

L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Packet sniffing

Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

Port scanning

Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.

Highjacking

Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione é complessa e richiede elevate capacità e rapidità d'azione.

Social engineering

Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.

Buffer overflow

Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

Spamming

Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

Password cracking

Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.

Trojan

Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsapevolmente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.

Worm

Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).

Logic bomb

Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.

Malware e mmc (malicious mobile code)

Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.

Dos (denial of service)

Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.

Ddos (distributed denial of service)

Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete. L'utilizzo di programmi di sniffing e port scanning é riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete dell'Istituto Comprensivo "B. R. Motzo" di Bolotana; tali programmi non sono in nessun caso utilizzati su reti esterne a quella dell'Istituto Comprensivo "B. R. Motzo" di Bolotana. La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.

Minacce a cui sono sottoposti i dati trattati

Le principali minacce ai dati trattati sono:

- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

Minacce a cui sono sottoposti i supporti di memorizzazione

Le principali minacce ai supporti di memorizzazione sono:

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

Articolo 7 - 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 6.

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
Infrastruttura	Hardware	Comunicazioni
		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
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
Documenti cartacei	Software	Personale

	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

Articolo 8 - 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.

Le misure di carattere elettronico/informatico (Le misure di carattere elettronico/informatico sono quelle in grado di segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, di gestire le copie di salvataggio dei dati e degli applicativi, di assicurare l'integrità dei dati, di proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi.) adottate sono:

- utilizzo di server con configurazioni di ridondanza in mirroring.
- presenza di gruppi di continuità elettrica per il server.
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità settimanale e storico di un mese;
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet entro luglio del 2006.

Articolo 9 - Principi di carattere generale

- I trattamenti di dati personali effettuati all'interno dell'Istituzione Scolastica devono avvenire secondo le modalità definite dalla normativa in vigore, con particolare riguardo a quanto disposto dal Dlgs 196/2003 e dalla normativa collegata;
- Occorre custodire e controllare i dati personali oggetto del trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dai casi consentiti o altrimenti trattati in modo illecito;
- Chiunque, all'interno di questa istituzione scolastica, tratti dati personali, è tenuto all'obbligo della dovuta riservatezza in ordine alle informazioni delle quali sia venuto a conoscenza;
- L'obbligo di mantenere la dovuta riservatezza, in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, permane anche quando sia venuto meno l'incarico stesso;
- Tutti i trattamenti dei dati personali vanno necessariamente organizzati secondo una procedura che garantisca:
 - una continua e idonea custodia dei dati oggetto del trattamento;
 - un adeguato controllo sugli accessi non autorizzati ai dati;
 - il maggior livello possibile di sicurezza in merito alla conservazione dei dati;
- Il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola. Al di fuori delle finalità strettamente istituzionali, dentro la

scuola non si possono trattare dati personali né su supporto cartaceo né su supporto elettronico;

- I dati personali oggetto dei trattamenti devono essere esatti ed aggiornati, inoltre devono essere pertinenti rispetto alle finalità del trattamento, completi e non eccedenti le finalità per le quali vengono raccolti e trattati. Ne consegue che i trattamenti dei dati vanno ridotti a quanto indispensabile rispetto alle finalità istituzionali perseguite;
- Nell'ambito delle indicazioni del presente Regolamento, particolare attenzione va prestata al trattamento di dati sensibili e giudiziari;
- L'istituto esegue verifiche periodiche sull'attualità degli incarichi affidati in merito al trattamento dei dati, nonché sull'esattezza e l'aggiornamento dei dati sensibili e giudiziari, sulla loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite.

Articolo 10 - Accesso ai luoghi in cui si effettuano i trattamenti

- L'accesso ai locali in cui si trovano le apparecchiature informatiche dell'istituzione scolastica (server di rete, computer, stampanti, ecc) utilizzati per il trattamento dei dati personali, nonché gli archivi e i registri cartacei contenenti dati personali, è controllato ed è permesso esclusivamente al personale debitamente incaricato e autorizzato;
- I locali ad accesso controllato sono chiusi anche se presidiati. Dopo l'uscita dell'ultimo incaricato/addetto al trattamento dei dati i locali sono chiusi a chiave;
- L'elenco delle persone autorizzate ad accedere ai locali di cui al presente articolo è periodicamente verificato dal responsabile del trattamento o da un suo delegato;
- Eventuali visitatori occasionali delle aree ad accesso controllato sono previamente autorizzati dal Responsabile del trattamento dei dati e accompagnati da un incaricato, che controllerà che i visitatori non accedano a dati in possesso dell'istituzione scolastica se non previamente autorizzati e incaricati;
- L'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo in seguito ad apposita convenzione e/o lettera con istruzioni che disciplinino ambiti e modalità delle operazioni effettuabili.

Articolo 11 - Raccolta, comunicazione e diffusione dei dati

- E' vietata ogni forma di diffusione e comunicazione dei dati personali a terzi soggetti, a meno che ciò non sia previsto da Legge o da Regolamento e autorizzato dal titolare del trattamento dei dati personali;
- I dati idonei a rivelare lo stato di salute non possono essere diffusi;
- E' necessario consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa (L'informativa è affissa negli Uffici di Segreteria e pubblicata sul sito web dell'Istituto www.scuolebolotana.it);
- Le comunicazioni di dati agli interessati (persone fisiche e giuridiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per iscritto dovranno essere consegnate in contenitori chiusi.

Articolo 12 - Tenuta dei registri e degli archivi cartacei

- I dati personali trattati attraverso supporto cartaceo possono essere trattati solo da personale debitamente incaricato e nel rispetto delle disposizioni contenute nelle lettere d'incarico e nel presente regolamento;

- I registri di classe, contenenti dati personali, durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni vengono depositati dall'insegnante dell'ultima ora di lezione nel locale di segreteria e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio delle lezioni;
- I certificati medici ricevuti vanno consegnati al più presto in Segreteria;
- Durante l'orario di servizio il docente è responsabile della custodia e della conservazione dei registri personali e dei registri di valutazione attraverso cui sono trattati dati personali. Fuori dall'orario di servizio il registro viene conservato nella sala docenti che è chiusa a chiave;
- E' fatto divieto di fotocopiare/scannerizzare documenti contenenti dati sensibili senza l'autorizzazione del responsabile o del titolare del trattamento;
- E' fatto divieto di esportare documenti o copie contenenti dati personali, all'esterno dell'Istituto, senza l'autorizzazione del titolare o del responsabile del trattamento; tale divieto si estende anche all'esportazione telematica;
- I dati comuni sono custoditi separati dai dati sensibili in sottofascicoli chiusi con dicitura "riservato";
- I documenti contenenti dati sensibili e giudiziari sono custoditi in armadi e/o cassette chiuse a chiave.

Articolo 13 - Trattamenti in formato elettronico – principi generali

- Le principali misure di sicurezza relative ai trattamenti di dati in formato elettronico sono indicate nel Documento Programmatico sulla Sicurezza dell'Istituto comprensivo "B. R. Motzo" di Bolotana;
- L'utilizzo dei Personal Computer e della Rete interna è permesso esclusivamente per lo svolgimento delle attività istituzionali della scuola;
- La scuola adotta procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- I computer della Segreteria sono connessi ad una rete locale autonoma, non visibile o raggiungibile da altri computer dell'istituto;
- La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Articolo 14 - Trattamenti in formato elettronico – regole operative

- E' fatto divieto, agli utilizzatori di strumenti elettronici, di lasciare incustodito, o accessibile lo strumento elettronico stesso; in particolare, in caso di allontanamento anche temporaneo dal posto di lavoro, è vietato lasciare aperto il proprio sistema operativo con la password inserita, a meno che il sistema non richieda automaticamente la password in caso di inattività prolungata;
- L'accesso ai dati trattati elettronicamente da parte degli incaricati e degli addetti esterni alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- La manutenzione degli elaboratori, che preveda o meno il trasferimento fisico presso un laboratorio di riparazioni, è autorizzata solo a condizione che il fornitore del servizio si impegni al rispetto della normativa sulla protezione dei dati personali; il fornitore si deve altresì impegnare a mantenere la dovuta riservatezza in ordine ai dati di cui sia venuto a conoscenza e a non utilizzarli fuori dai casi consentiti;

- Tutte le operazioni di manutenzione che sono effettuate all'interno dell'Istituzione Scolastica avvengono con la supervisione del Responsabile del trattamento o di un suo delegato;
- Gli hard disk non sono condivisi in rete se non in casi specifici e limitati;
- E' fatto assoluto divieto di memorizzare, sulla propria postazione di lavoro, dati di carattere personale che non siano inerenti alla funzione svolta;
- E' proibito installare qualsiasi programma da parte dell'utente o di altri operatori, a meno che non siano autorizzati dell'amministratore del sistema (se nominato) o dal Responsabile del trattamento;
- E' vietato fare uso delle funzionalità di accesso remoto del proprio computer se non espressamente autorizzati dal Responsabile del trattamento o dell'amministratore del sistema (se nominato);
- All'uso di supporti rimovibili (floppy, cd, zip) va sempre preferito l'utilizzo di internet o di un file server locale;
- Va evitato l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza;
- E' fatto divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non; La decisione di "scaricare" può essere presa solo dal responsabile del trattamento o l'amministratore del sistema (se nominato);
- Va attivata la protezione massima per gli utenti dei programmi di posta utilizzati, al fine di proteggersi dal codice html di certi messaggi e-mail, dato che alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer;
- E' fatto divieto di utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi dello Stato;
- Gli allegati di posta, se non si è certi della loro provenienza, non vanno aperti e in ogni caso vanno analizzati con un antivirus;
- E' opportuno impostare l'antivirus anche nella funzione di autoriparazione;
- Avvisare sempre l'amministratore di sistema nel caso in cui il processo di autoriparazione non vada a buon fine;
- E' opportuno conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino anomalie di funzionamento quali ad esempio modifica e sparizione di dati, irregolarità nell'utilizzo del Computer.

Articolo 15 - Disposizioni in merito alla gestione delle password

- Tutti gli incaricati del trattamento dei dati personali accedono agli strumenti elettronici usati per i trattamenti attraverso un codice identificativo personale (in seguito indicato user-id) e password personale;
- User-id e password iniziali sono assegnati dal Responsabile del trattamento o dal custode delle password (se nominato), se necessario con il supporto del responsabile del sistema informativo (se nominato), oppure con l'ausilio di una ditta esterna debitamente incaricata;
- I codici assegnati sono segreti, non possono essere assegnati né comunicati ad altri soggetti; vanno custoditi con diligenza e riservatezza;

- L'user-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome;
- La password è composta da almeno 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'Istituzione scolastica, al suo utilizzatore o al suo ufficio;
- La password deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato;
- Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima;
- Le password verranno prontamente disattivate dopo tre mesi di non utilizzo;
- In caso di necessità, il Responsabile del trattamento o l'amministratore di sistema (se nominato) è autorizzato a intervenire sui personal computer;
- L'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse che altri non autorizzati ne sono venuti a conoscenza.

Articolo 16 - 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 precedentemente indicate, nel rispetto di quanto stabilito nel presente documento.

Articolo 17 - Piano di formazione

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

Le finalità della formazione sono:

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

Il piano in relazione alla protezione dei dati personali: diritto di riservatezza e misure di sicurezza, dovrà riguardare:

1. Le finalità del T.U. in materia di protezione dei dati personali
2. Le regole di trattamento
3. La tutela dei diritti dell'interessato
4. I soggetti del trattamento: Titolare-Responsabili-Incaricati
5. Rischi che incombono sui dati
6. Le misure disponibili per prevenire eventi dannosi
7. Il sistema di tutela giurisdizionale e paragiurisdizionale a protezione del dato
8. Il ruolo del Garante per la protezione dei dati personali
9. Le sanzioni civili e penali nella violazione delle norme a protezione del dato
10. Le singole misure di sicurezza logiche, fisiche e procedurali

11. Le regole di trattamento dei dati relativi agli studenti
12. Esempi pratici e casi risolti

Il piano prevede inoltre la pubblicazione di normativa ed ordini di servizio nella bacheca della scuola.

Articolo 18 - Sanzioni

In caso di violazione delle disposizioni del presente regolamento, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dal regolamento d'istituto.

Articolo 19 - Validità

Le misure contenute negli articoli precedenti hanno validità permanente.

Il piano è comunque soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 N° 196.

Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

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

Articolo 20 - Regolamento per l'utilizzo della rete

Paragrafo 1 - Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica del Istituto Comprensivo “B. R. Motzo” di Bolotana e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire. La rete dell’Istituto Comprensivo “B. R. Motzo” di Bolotana è connessa alla rete Internet.

Paragrafo 2 - Principi generali – diritti e responsabilità

L’Istituto Comprensivo “B. R. Motzo” di Bolotana promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina. Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione. Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell’operatore. E’ pertanto proibito installare qualsiasi programma da parte dell’utente o di altri operatori, escluso l’amministratore del sistema. L’utente ha l’obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza. Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

Paragrafo 3 - Abusi e attività vietate

E' vietato ogni tipo di abuso (Si intende con abuso qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale) .

In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale dell'Istituto Comprensivo "B. R. Motzo" di Bolotana;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (User Id e password) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne a quella del Istituto Comprensivo "B. R. Motzo" di Bolotana;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distruggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica del Istituto Comprensivo "B. R. Motzo" di Bolotana per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;

- abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

Paragrafo 4 - Attività consentite

E' consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Paragrafo 5 - Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete del Istituto Comprensivo "B. R. Motzo" di Bolotana. Tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature. L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche. Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare. L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Paragrafo 6 - Modalità di accesso alla rete e agli applicativi

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente. L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi. L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete. L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus. Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password.

Paragrafo 7 - Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti dell'Istituto comprensivo "B. R. Motzo" di Bolotana.

Articolo 21 - Utilizzo del proxy

L'utilizzo del proxy riguarda le misure procedurali relative all'identificazione e all'autenticazione degli utenti, le regole di utilizzo delle risorse hardware e software, le norme comportamentali e le responsabilità di ciascuno. Rientrano in questo aspetto le norme di comportamento interno per limitare l'uso privato di e-mail o Internet, in quanto i controlli sono possibili solo a determinate condizioni e con l'accordo delle rappresentanze sindacali unitarie. Si ricorda che il D.L.vo 196/03 (Codice in materia di protezione dei dati personali) ribadisce quanto dettato dall'art. 4 dello Statuto dei Lavoratori, ovvero il "... divieto di utilizzo da parte del datore di lavoro di apparecchiature atte al controllo a distanza dell'attività del lavoratore, salvo che esigenze organizzative, produttive o di sicurezza non abbiano determinato, previo accordo con le rappresentanze sindacali, la lecita introduzione in azienda". D'altro canto la consultazione di siti web da parte del lavoratore o l'utilizzo di posta elettronica durante il normale orario di lavoro non è consentita quando tale attività non sia pertinente con le mansioni affidate, come l'art. 1024 del codice civile prevede nel principio generale di diligenza del lavoratore. Per trovare un punto di equilibrio tra i diritti del lavoratore e dell'istituto è opportuno introdurre una policy trasparente e codificata con l'apporto dei lavoratori, dando anche la possibilità al datore di lavoro di prevedere meccanismi sanzionatori, sempre che la policy sia resa accessibile a tutti i lavoratori, come previsto dall'art. 7 dello Statuto dei Lavoratori. Sempre tra le politiche di sicurezza si può fare riferimento alle responsabilità civili e penali per i danni cagionati con il trattamento dei dati personali. A titolo di esempio si possono elencare:

1. la responsabilità civile disciplinata dall'art. 2050 del Codice Civile e art. 15 D.Lgs. 196/03 "chi cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo";
2. la sanzione penale che colpisce chi, essendovi tenuto, omette di adottare le misure di sicurezza (art. 169 del D.Lgs. 196/03), pari all'arresto fino a due anni o ad ammenda da 10mila a 50mila euro, ma con estinzione del reato in caso di regolarizzazione entro 6 mesi dall'accertamento del reato e pagamento di somma determinata dal Garante.

Le informazioni e le attività eseguite sulla rete informatica e telematica dell'Istituto Comprensivo "B. R. Motzo" di Bolotana relative agli utilizzatori, sono registrate e conservate su file (registro elettronico delle attività o file di log). Tali file possono essere soggetti ad indagini, nel rispetto di quanto sancito dal D.L.vo 30 giugno 2003, n. 196. Inoltre, il responsabile per la sicurezza può accedere ai file degli utilizzatori per proteggere l'integrità dei sistemi informatici.

Il responsabile del trattamento

Il DSGA
dott. G. Onida

Il titolare del trattamento

Il Dirigente scolastico
ing. G. Pilia