ISTITUTO COMPRENSIVO MONDOVI' 2
Via Matteotti, 9 12084 MONDOVI' (Cn)
Tel 0174 43144 Fax n.0174 553935
e-mail: cnee03700g@istruzione.it PEC: cnic85900a@pec.istruzione.it
http: www.icmondovi2.gov.it C.F.: 93055460047

DOCUMENTO PROGRAMMATICO DI SICUREZZA

IN MATERIA DI PROTEZIONE DI DATI PERSONALI

MISURE MINIME

ADEGUAMENTO AL RINNOVO LABORATORI

16 febbraio 2012

Scopo di questo documento è stabilire le misure di sicurezza da adottare affinché siano rispettati gli obblighi in materia, previsti dalla normativa vigente D.Lgs.n.196/2003 recante il Codice in materia di protezione di dati personali, segnatamente gli artt. 34 ss., nonché l'allegato B del suddetto D.Lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza.

La sicurezza, come protezione e trattamento dei dati personali, non deve essere ridotta ad una serie di adempimenti formali, bensì divenire consapevolezza della necessità di mettere in atto comportamenti corretti come dovere dell'Amministrazione per garantire il diritto di ognuno alla protezione dei propri dati. In quanto "cultura della sicurezza" richiede formazione.

Tale piano persegue l'obiettivo di minimizzare

I principi cardine del sistema di tutela dei dati, art. 1-4 del Codice della Privacy, possono essere così sintetizzati:

1. diritto di ognuno alla protezione dei propri dati personali;
2. garanzia del trattamenti dei dati personali nel rispetto delle libertà fondamentali dell'individuo e della sua dignità;
3. necessità del trattamento. I dati personali sono beni giuridici meritevoli di tutela per il cui trattamento ed utilizzo sono posti limiti e cautele specifiche;
4. liceità e correttezza del trattamento (applicazione concreta del principio di buona fede). I dati sono trattati per finalità istituzionali e per scopi leciti ed espliciti. Debbono essere trattati secondo i principi di pertinenza, completezza e non ridondanza in rapporto alle finalità del trattamento;
5. correttezza dei dati che implica aggiornamento continuo, revisione e correzioni anche su richiesta dell'interessato;
6. pertinenza, completezza e non ridondanza dei dati in rapporto;
7. conservazione e durata per il tempo necessario al raggiungimento delle finalità del trattamento.

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Al fine di perseguire le finalità istituzionali, l'Istituzione scolastica tratta dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori e utilizzatori esterni della scuola.

I trattamenti sono effettuati, anche mediante strumenti elettronici, per le seguenti finalità:

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

Fonte dei dati:

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

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

I dati oggetto di trattamento sono:

- PERSONALI: qualunque informazione riferibile, anche indirettamente, a persona fisica, giuridica, ente o associazione;
- 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;
- GIUDIZIARI: i dati personali idonei a rivelare provvedimenti, come da DPR n°313/2002 (art.3, comma1 a-o, r-u), in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI.

L'istituzione scolastica nel suo complesso è titolare del trattamento dei dati personali; la titolarità è esercitata dal Dirigente Scolastico, rappresentante legale dell'Istituto, e tra i compiti non delegabili è compresa 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 relativa alla sicurezza.

Si designa Responsabile del trattamento, ai sensi dell'art.29 del D.Lgs. n.196 del 2003, il D.G.S.A. Patrizia DHO in considerazione dell'esperienza, capacità ed affidabilità dimostrate che garantiscono garanzia di applicazione delle disposizioni in materia di trattamento.

Il suddetto Responsabile del trattamento riceve adeguate istruzioni riguardo:

a) l'individuazione ed adozione delle misure di sicurezza da applicare nell'ambito dell'istituzione scolastica, al fine di salvaguardare la riservatezza, l'integrità, la completezza e la disponibilità dei dati trattati;

b) l'esigenza di provvedere, mediante atto scritto, all'individuazione delle unità legittimate al trattamento ai sensi dell'art.30 del D.Lgs. n.196 del 2003, che operano sotto la diretta autorità del responsabile,

attenendosi alle istruzioni impartite, fermo restando l'obbligo gravante sul responsabile di vigilare sul rispetto delle misure di sicurezza adottate;

c) l' esigenza di verificare che gli obblighi di informativa di trattamento dei dati siano stati assolti correttamente, ovvero che sia stato conseguito il consenso degli interessati;

f) l'obbligo di osservare e far osservare il divieto di diffusione impropria dei dati trattati;

g) la custodia delle copie di credenziali di autenticazione mediante parola chiave, aggiornate periodicamente (ogni 6 mesi).

Il Responsabile del trattamento provvede ad individuare e a nominare gli incaricati, i quali devono attenersi alle consegne ricevute dal responsabile, autorizzandoli al trattamento dei dati in riferimento all' espletamento delle funzioni istituzionali ad essi rispettivamente assegnate.

Gli incaricati sono stati formalmente formati ed istruiti in merito alla circostanza che:

a) il trattamento e la conservazione dei dati deve avvenire esclusivamente in modo lecito e proporzionato alle funzioni istituzionali, nel rispetto del dovere di garantire il diritto di ciascuno alla tutela dei propri dati;

b) la raccolta, registrazione ed elaborazione dei dati, mediante strumento informatico o cartaceo, deve essere limitata alle finalità istituzionali;

c) è compito dell'incaricato la correzione e/o l'aggiornamento dei dati posseduti, l'esame della loro pertinenza rispetto alle funzioni.

L'ambito dei trattamenti autorizzati ai singoli incaricati è suscettibile di aggiornamento periodico.

A tutti gli incaricati destinati al trattamento di dati mediante strumento elettronico vengono conferite credenziali di autenticazioni (art.34, comma l, lett.) mediante parola chiave, conformi alle caratteristiche indicate in apposito paragrafo. E' stato designato *l'incaricato della custodia delle copie di credenziali di autenticazione* nonché della *funzione di verifica del loro aggiornamento periodico ovvero della corretta utilizzazione.*

Le suddette credenziali sono disattivate automaticamente dal gestore della rete periodicamente, ovvero in tutti i casi di mancata utilizzazione per almeno 6 mesi.

Concorrono al trattamento anche due strutture esterne all'istituzione scolastica, *incaricate mediante regolare contratto*.

Della ditta incaricata del trattamento dei dati personali per il registro elettronico è stato nominato un responsabile con il quale è stata stipulata apposita convenzione.

Al fine di meglio precisare la ripartizione delle funzioni si rinvia alla tabella seguente:

Struttura	Responsabile	Incaricato	Trattamenti operati dalla struttura	Compiti della struttura
Ufficio della Direzione e del DSGA	DHO P.	BASSO M. ROLANDO F. MICHELOTTI E. TOSETTI C.	Trattamenti strumentali allo svolgimento dei compiti istituzionali: gestione della corrispondenza e delle comunicazioni da e per gli uffici; protocollo generale con conseguente registrazione della posta.	Acquisizione caricamento dei dati, consultazione, stampa, comunicazione a terzi,manutenzione tecnica dei programmi utilizzati nel trattamento,gestione tecnica operativa della base dati (controllo,salvataggi, e ripristini, ecc.)
Ufficio personale	Soggetto qualificato come Responsabile Patrizia DHO	BASSO M. ROLANDO F. MICHELOTTI E. F.ROLANDO *C. TOSETTI	Trattamenti strumentali allo svolgimento dei compiti istituzionali, in materia di selezione ed amministrazione del personale: contratti, assenze giustificate, espletamento funzioni politiche o sindacali; aspetti economici e previdenziali; raccolta di curricula, condizioni sanitarie ed economiche. *Trattamento dati Invalsi (unica autorizzata per lo scarico)	Come sopra
Servizi Amministrativi	Soggetto qualificato come Responsabile Patrizia DHO	C. TOSETTI E.MICHELOTTI	Trattamenti strumentali allo svolgimento dei compiti di gestione amministrativa (tenuta dei dati connessi all'espletamento di procedimenti amministrativi, attività contrattuale, gestione di beni, procedure di bilancio	Come sopra
Servizi inerenti l'Offerta formativa	Soggetto qualificato come Responsabile Patrizia DHO	Tutti gli Insegnanti	Trattamenti strumentali alla predisposizione e concreta erogazione dell'offerta formativa (raccolta delle domande di iscrizione; condizioni sanitarie ed economiche dei destinatari dell'offerta formativa, documentazione concernente opzioni per insegnamenti facoltativi, dati inerenti profili sanitari o relativi al nucleo famigliare dei destinatari dell'offerta formativa, per il riconoscimento di attività di sostegno in ragione di situazioni di disagio, sociale, economico o famigliare, registri relativi alle presenze presso l'istituzione scolastica)	Come sopra

Servizi strumentali agli organi collegiali	Soggetto qualificato come Responsabile Patrizia DHO	E. MICHELOTTI C. TOSETTI	Trattamenti strumentali alle attività degli organi collegiali ed attività connesse ai rapporti con organi pubblici (composizione degli organi collegiali rappresentativi della comunità servita dall' offerta formativa, convocazione degli organi, raccolta delle delibere, raccolta degli atti concertati con altre istituzioni pubbliche)	Come sopra
Servizi strumentali, affidati all'esterno, concernenti l'assistenza e la manutenzione degli strumenti elettronici (elaboratori e programmi	Personale individuato dalla Società incaricata --- ----------	Personale individuato dalla Società incaricata --- ----------	Trattamenti strumentali (interventi di carattere tecnico aventi ad oggetto gli strumenti elettronici, effettuati anche al di fuori dei locali di pertinenza dei singoli istituti scolastici; funzionalità software gestione registro elettronico)	Come sopra

3 AMBITO DEI TRATTAMENTI.

Attesa la dislocazione dell'istituzione scolastica in più edifici, si precisano le modalità del trattamento dei dati nei vari uffici e sedi, mediante strumenti elettronici, secondo le modalità precisate nella tabella sottostante.

Tabella 2 Elenco dei trattamenti: informazione di base

Struttura deputata al trattamento	**Natura dei dati trattati** **Sensibili** **Giudiziari**		**Struttura di riferimento**	**Altre strutture(**anche esterne) **che concorrono al trattamento**	**Descrizione degli strumenti utilizzati**
Segreteria Dirigente Scolastico	S	G		Ditta esterna per esigenze di manutenzione, e\o gestione ,riparazione dei P.C. interni,client e\o Server	Stazioni PC, server + server esterno
Ufficio personale	S	G			Stazioni PC, server + server esterno
Servizi Amministrativi	S	G			Stazioni PC, server + server esterno
Servizi inerenti l'Offerta formativa	S	-			Stazioni PC, server + server esterno
Servizi Strumentali agli organi collegiali	S	-			Stazioni PC, server + server esterno

Il trattamento dei dati avviene attraverso modalità diverse: strumenti elettronici, interni (P.C.) ovvero collegati in rete fra loro, e/o mediante collegamenti alla rete intranet e/o alla rete internet. Con riferimento alla gestione dei dati mediante rete ministeriale l'Istituzione scolastica declina ogni responsabilità, operando come semplice utente, non essendo in grado di intervenire sulla gestione delle informazioni ivi contenute e gestite.

Con riferimento all'ubicazione fisica dei supporti di memorizzazione delle copie di sicurezza, l'Istituzione scolastica, tenendo conto dell'analisi di cui al punto 5, ha ritenuto di provvedere alla custodia presso l'Ufficio di Segreteria, riservando l'accesso a tali supporti al D.G.S.A. Patrizia DHO, al Dirigente Scolastico e al personale degli Uffici al fine di garantire la sostituzione ogni due giorni del supporto.

La tabella seguente riassume il quadro dei trattamenti secondo modalità e tipologia, precisando l'ubicazione dei supporti di memorizzazione.

Tabella 3. Elenco dei trattamenti:descrizione degli strumenti utilizzati

IDENTIFICATIVO DEL TRATTAMENTO	EVENTUALI BANCHE DATI DI SUPPORTO	UBICAZIONE FISICA DEI SUPPORTI DI MEMORIZZAZIONE E COPIE DI SICUREZZA	TIPOLOGIA DEI DISPOSITIVI DI ACCESSO	TIPOLOGIA DI INTERCONNESSIONE
Segreteria Dirigente Scolastico	Ruoli del personale in formato elettronico	Locale Segreteria al Piano terreno nell'Istituzione scolastica	PC	Rete locale, Intranet, Internet
Ufficio personale	Ruoli del personale in formato elettronico; Archivio del personale (N.B. le tabelle realizzate con excel recano l'indicazione delle assenze per festività religiose non cattoliche e/o condanne penali, appartenenza di uno o più dipendenti a categorie protette con handicap, etc.)	Come sopra	PC Supporto cartaceo	Rete locale, Intranet, Internet
Servizi Amministrativi	Archivio delle imprese fornitrici di servizi e/o prestazioni. L'archivio contenuto negli elaboratori sottoposti a revisione o manutenzione da parte di tecnici, anche esterni, incaricati degli interventi (sia in caso di trasporto dell'elaboratore all'esterno dell'Ente,presso i locali della ditta,sia in caso d'intervento sul posto,cioè nei locali dell'Istituzione Scolastica)	*Come sopra*	PC Supporto cartaceo	Rete locale, Intranet, Internet
Servizi inerenti l'offerta formativa	Destinatari dell'offerta formativa con caratterizzazione religiosa, economica,sociale,sanitaria (cf."modello di previsione h")	*Come sopra*	PC collegato a Server interno ed a Server esterno	Rete locale, Internet
Servizi strumentali agli organi collegiali	Membri degli organi collegiali	*Come sopra*	PC collegato a Server interno ed a Server esterno PC collegato a Server interno	Rete locale, Internet

4. ANALISI DEI RISCHI INCOMBENTI SUI DATI.

Gli archivi a supporto cartaceo, e solo in parte quelli su supporto informatico, sono sottoposti a rischio fisico ovvero degrado, furto, danneggiamento, smarrimento, atti di vandalismo, incuria, perdita totale o parziale per eventi naturali.

Gli archivi di norma sono conservati in armadi con chiave custodita da personale preposto e/o posizionati in aree ad accesso controllato. Tali aree sono sotto la responsabilità dell'Istituto, il locale deve essere chiuso e le chiavi custodite dal responsabile, l'accesso è consentito solo agli autorizzati.

Altre misure minime di sicurezza sono:

- accesso ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
- utilizzo di archivi con accesso selezionato: DSGA, Dirigente, gli amministrativi, n. 2 collaboratori;
- restituzione di atti e documenti al termine delle operazioni

Il DSGA provvede ad incaricare n. 1 assistente amministrativo responsabile dell'archivio.

Nell'istituto è funzionante un sistema di antifurto periodicamente controllato .Per quanto riguarda gli archivi informatici la valutazione ha evidenziato rischi fisici e logici che vengono accorpati in:

1) Comportamenti degli operatori.

Sottrazione di credenziali di autenticazione; comportamenti imperiti, imprudenti o negligenti dei soggetti legittimati al trattamento dei dati; comportamenti dolosi dei soggetti legittimati; errori materiali.

2) Eventi relativi agli strumenti.

- Danno arrecato da virus informatici e/o da hackers, mediante interventi precedenti all'aggiornamento degli strumenti di contrasto attivati (software e firewall);
- Spamming o tecniche di sabotaggio;
- Malfunzionamento, indisponibilità o usura fisica degli strumenti;
- Accessi abusivi negli strumenti elettronici;
- Intercettazione dei dati in occasione di trasmissione in rete.

3) Eventi relativi al contesto fisico-ambientale.

- Distruzione o perdita di dati in conseguenza di eventi incontrollabili o astrattamente preventivabili;
- Guasti a sistemi complementari, quale la mancata erogazione di energia elettrica;
- Furto o danneggiamento degli strumenti elettronici di trattamento dei dati;
- Accesso non autorizzato da parte di terzi interni o esterni all'istituzione scolastica -
- mediante uso abusivo di credenziali di autenticazione;
- Errori umani nell'attivazione degli strumenti di protezione.

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. Accanto all'adozione di misure tecnologiche sono definiti ruoli, compiti e responsabilità di tutti e di ciascuno.

Tabella 4 Analisi dei rischi

EVENTO		IMPATTO SULLA SICUREZZA DEI DATI		RIF. MISURE DI AZIONE
		DESCRIZIONE	GRAVITÀ STIMATA	
COMPORTAMENTI DEGLI OPERATORI	Furto di credenziali di autenticazione	Accesso altrui non autorizzato	**MB**	Vigilanza sul rispetto delle istruzioni impartite Accesso alla cassaforte controllato
	Carenza di consapevolezza, disattenzione o incuria	Dispersione, perdita e accesso altrui non autorizzato	**MB**	Formazione e flusso continuo di informazione
	Comportamenti sleali o fraudolenti	Dispersione, perdita e accesso altrui non autorizzato	**B**	Vigilanza sul rispetto delle istruzioni impartite
	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	**M**	Formazione e Vigilanza sul rispetto delle istruzioni impartite e flusso continuo di informazione
EVENTI RELATIVI AGLI STRUMENTI	Azione di virus informatici o di codici malefici; Spamming o altre tecniche di sabotaggio	Perdita o alterazione, di dati, di programmi e di elaboratori;	**M**	Adozione di idonei dispositivi di protezione (software di congelamento pc, antivirus); salvataggio dati mediante back up giornaliero su più dispositivi.
	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**MA**	Assistenza e manutenzione continua degli elaboratori e dei programmi; programma di ricambio pluriennale (compatibilmente con le risorse economiche); back up giornaliero.

EVENTI RELATIVI AGLI STRUMENTI	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	**A**	Adozione di idonei dispositivi di protezione Antivirus, Firewall e credenziali di autenticazione ; allarme antifurto; salvataggio dati mediante back up giornaliero
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	**MA**	Adozione di idonei dispositivi di protezione Antivirus, , Firewall e credenziali di autenticazione
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;; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**M**	Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati
	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.)	Come sopra	**A**	Attività di controllo, assistenza e manutenzione periodica
	Errori umani nella gestione della sicurezza fisica	Come sopra	**M**	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

Il programma antivirus è aggiornato periodicamente su tutte le postazioni contenenti dati.

Tutti i Personal computer installati presso i locali della segreteria hanno la possibilità di attivare una password. Essendo il rapporto PC/posti di lavoro pari a 1 tutti gli utenti devono attivare una password che renda esclusivo l'uso del personal computer al singolo operatore.

Le password di amministratore di tutti i server sono inserite e modificate periodicamente dalla funzione strumentale informatica e sono conservate in cassaforte. Le password in caso di manutenzione straordinaria possono essere affidate dal responsabile al sistemista addetto alla manutenzione e deve essere prontamente sostituita dal responsabile al termine delle operazioni di manutenzione.

1) <u>Approfondimento sulle password</u>

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.

Le regole di seguito elencate sono vincolanti per tutti i posti di lavoro tramite i quali si può accedere alla rete e alla banche dati contenenti dati sensibili.

Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo.

Devono essere rispettate le seguenti regole per la definizione/gestione delle password:

- la lunghezza minima delle password è di 8 caratteri
- deve contenere almeno un carattere alfabetico ed uno numerico
- non deve contenere più di due caratteri identici consecutivi
- non deve essere simile alla password precedente
- non deve contenere l'user-id come parte della password
- deve essere cambiata almeno ogni 6 mesi
- non deve essere comunicata ad altri utenti

Dove la tecnologia lo permette tali regole sono rese obbligatorie dai software altrimenti è responsabilità dell'utente rispettarle

2) <u>Protezione degli archivi informatici contenenti dati sensibili e giudiziari</u>

Gli elaboratori che ospitano archivi con dati sensibili devono sottostare alle seguenti regole

- obbligo di password
- autorizzazione scritta per l'accesso agli incaricati ed agli addetti alla manutenzione
- supervisione dell'incaricato del trattamento e tutte le operazioni di manutenzione
- antivirus costantemente aggiornato
- piano di backup proceduralizzato concordato con i responsabili del trattamento e del sistema informatico
- conservazione in luogo sicuro delle copie di backup
- obbligo di screen server con password

- divieto di installazione, sui personal computer, di archivi di carattere personale dell'utente
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza autorizzazione scritta da parte del responsabile del trattamento dati
- divieto di installazione accessi remoti di qualsiasi tipo mediante modem e linee telefoniche

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

5. SALVATAGGIO DEI DATI

Tutti gli utenti del sistema informativo, opportunamente istruiti sono responsabili delle operazioni di salvataggio dei propri dati. Il sistema è predisposto per effettuare quotidianamente il back up e, ogni due giorni, l'incaricato provvede alla sostituzione e conservazione delle cassette.

Le cassette sono conservate in cassaforte allocata in locale protetto da porta ignifuga. La chiave della cassaforte e dell'ufficio sono disponibili solo al DSGA e al Dirigente o suo delegato.

6. GESTIONE DEL SITO WEB

La redazione editoriale della scuola gestisce le pagine del sito garantendo che il contenuto sia accurato e appropriato, aggiornato costantemente. Il sito assolverà alle linee guida sulle pubblicazioni della scuola. La scuola detiene i diritti d'autore dei documenti propri e di quanto prodotto dagli studenti. In caso di pubblicazioni di documenti, video, immagini, musiche non proprie sono precisate fonti e /o autori. Sul sito della scuola non vengono diffuse immagini in cui gli alunni siano riconoscibili. Eventuali utilizzi di immagini sui siti ministeriali saranno preventivamente oggetto di consenso scritto dei genitori.

7. FORMAZIONE

Il buon funzionamento di un piano di sicurezza si realizza attraverso il coinvolgimento di tutto il personale della scuola creando la cultura necessaria a garantire e preservare integrità e riservatezza dell'intero patrimonio informativo con particolare attenzione ai dati sensibili.

Pertanto l'istituto ha promosso, all'interno, formazione sulla base dei bisogni riscontrati, circolazione di informazione anche attraverso la distribuzione di materiale, supporto attraverso la nomina di un referente al sistema informatico e stimola a partecipare a iniziative formative esterne.

8. REGOLAMENTO DI ISTITUTO

Nel documento sono inserite le disposizioni sull'accesso ai laboratori e all'utilizzo delle apparecchiature informatiche come norme di comportamento.

9. VINCOLI CONTRATTUALMENTE ASSUNTI DAL FORNITORE ESTERNO AI FINI DELLA SICUREZZA DEI DATI

L'Istituzione scolastica ha affidato all'esterno, nei termini risultanti dalla sopraindicata tabella, i trattamenti di dati personali sensibili o giudiziari, effettuato con strumenti elettronici, previa assunzione da parte dell'affidatario – nell'ambito dello stesso contratto con cui viene realizzato l'affidamento o con atto aggiuntivo – degli impegni derivanti dalle seguenti dichiarazioni:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche ricevute per il trattamento dei dati personali e di integrarle nelle procedure già in essere;
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di avvertire (allertare) immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Gli allegati al presente documento ne formano parte integrante.

Il presente documento è aggiornato al. 16 febbraio 2012

IL TITOLARE DEL TRATTAMENTO _____

IL RESPONSABILE DEL TRATTAMENTO _____

ALLEGATO A

REGOLE ULTERIORI PER I SOGGETTI PUBBLICI
(Principi applicabili al trattamento di dati sensibili e giudiziari)
Art. 22 D.L.vo n.196/2003

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.
2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.
3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.
4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.
5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al
fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da
quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.
6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.
8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.
9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.
7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.
8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.
9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.
10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psicoattitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.
11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.
12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

(Artt. da 33 a 36 del codice)

ALLEGATO B

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati
personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615- ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di

cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle
disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito
dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di
autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il
controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.