ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente Documento è stato redatto ai sensi del Titolo V, Capo I e II, art. 31 e seguenti, nonché di quanto previsto dal "Disciplinare Tecnico in materia di misure minime di sicurezza" di cui all'allegato B del Decreto Legislativo n. 196 del 30/06/2003 e successive modifiche, nel rispetto di quanto previsto dal *D.M.P.I. 7 dicembre 2006, n.305, "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196" e dalle autorizzazioni generali del Garante in materia di Protezione dei Dati Personali, pertinenti in base a natura giuridica dell'ente e natura dei dati trattati*

ANNO 2012

Il titolare del trattamento adotta il presente Documento entro il 31.03.12, considerando quanto già indicato nei precedenti Documenti Programmatici sulla Sicurezza

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

PREMESSA

A. Nota Informativa

Il presente documento e le misure di sicurezza in esso indicate si riferiscono a tutti i dati contenuti nel sistema informatico dell'ente titolare del trattamento, l'**Istituto Comprensivo di Scuola Elementare e Media "Rovereto Sud"**, nei limiti della propria competenza e delle proprie funzioni di gestione amministrativa, finanziaria, didattica e tecnica in osservanza da quanto previsto dalla normativa nazionale e provinciale di riferimento.

Copia del presente Documento viene messa a disposizione presso la Segreteria dell'Ente.

Con riferimento ad alcuni dati e trattamenti esiste un regime di con titolarità tra il titolare e la Provincia Autonoma di Trento.

B. Definizioni, finalità e campo d'applicazione

Ai sensi dell'allegato B del Decreto Legislativo 30 giugno 2003, n. 196, Disciplinare tecnico in materia di misure minime di sicurezza, il presente documento contiene idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- 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;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui ai successivi punti;
- 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

- 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;
- 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.

Per una migliore comprensione delle disposizioni normative, nonché dell'attività del presente titolare del trattamento, ai sensi del Decreto Legislativo citato si riportano le seguenti definizioni:

- "***TRATTAMENTO***", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "***DATO PERSONALE***", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "***DATI IDENTIFICATIVI***", i dati personali che permettono l'identificazione diretta dell'interessato;
- "***DATI SENSIBILI***", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "***DATI GIUDIZIARI***", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "***TITOLARE***", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad

altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

- "***RESPONSABILE***", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- "***INCARICATI***", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- "***INTERESSATO***", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- "***COMUNICAZIONE***", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "***DIFFUSIONE***", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "***DATO ANONIMO***", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- "***BLOCCO***", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- "***BANCA DI DATI***", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- "***GARANTE***", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
- "***COMUNICAZIONE ELETTRONICA***", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- "***CHIAMATA***", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- "***RETI DI COMUNICAZIONE ELETTRONICA***", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti

utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

- "***RETE PUBBLICA DI COMUNICAZIONI***", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- "***SERVIZIO DI COMUNICAZIONE ELETTRONICA***", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- "***ABBONATO***", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura ditali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
- "***UTENTE***", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- "***DATI RELATIVI AL TRAFFICO***", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- "***DATI RELATIVI ALL'UBICAZIONE***", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
- "***SERVIZIO A VALORE AGGIUNTO***", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- "***POSTA ELETTRONICA***", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

- "***MISURE MINIME***", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- "***STRUMENTI ELETTRONICI***", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- "***AUTENTICAZIONE INFORMATICA***", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- "***CREDENZIALI DI AUTENTICAZIONE***", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- "***PAROLA CHIAVE***", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- "***PROFILO DI AUTORIZZAZIONE***", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- "***SISTEMA DI AUTORIZZAZIONE***", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
- "***SCOPI STORICI***", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- "***SCOPI STATISTICI***", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- *"**SCOPI SCIENTIFICI***", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

C. Metodologia di redazione

Nella redazione del presente Documento Programmatico sulla Sicurezza (DPS) è stata utilizzata una metodologia che soddisfa rigorosamente il dettato normativo contenuto nel Disciplinare Tecnico in Materia di Misure Minime di Sicurezza (Allegato B) del D.lgs.. 30 giugno 2003, n. 196).

E' stato preso come riferimento il modello di DPS pubblicato sul sito Internet del Garante della Privacy. Il Documento è stato realizzato tramite la redazione di questionari specifici e attraverso l'analisi della struttura.

La metodologia adottata prevede un modello di gestione della sicurezza fondato su un continuo monitoraggio e miglioramento del sistema, definito come modello "Plan – Do – Check – Act", e prevede attività di identificazione, analisi e valutazione dei rischi, nonché di pianificazione e realizzazione di eventuali interventi finalizzati a ridurne la probabilità di un accadimento dannoso per la sicurezza dei dati.

Si tratta di un processo circolare che prevede la ripetizione, con cadenza almeno annuale, dei seguenti passaggi:

- analisi qualitativa del patrimonio informativo dell'Ente;
- individuazione dei ruoli e delle responsabilità;
- identificazione e classificazione delle informazioni e dei dati personali trattati dall'Ente;
- descrizione degli strumenti utilizzati;
- analisi dei rischi;
- verifica puntuale del rispetto dei requisiti previsti dal D. Lgs. 30 giugno 2003, n. 196, con riferimento al trattamento di dati personali;
- individuazione dei criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza;
- individuazione delle procedure per il controllo dell'accesso delle persone autorizzate ai locali interessati dalle misure di sicurezza;
- individuazione dei criteri e delle procedure per assicurare l'integrità dei dati, per la sicurezza delle trasmissioni e per la restrizione dell'accesso per via telematica;
- individuazione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- individuazione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare;
- elaborazione di un piano di verifica delle misure di sicurezza;
- elaborazione di un piano di formazione.

D. Piano di revisione

Il presente documento, redatto ed approvato dal titolare entro la data del 31 marzo 2011 è da ritenersi valido per il termine di un anno dalla sua emissione o della sua ultima revisione.
La revisione del presente documento programmatico è comunque pianificata prima del termine di legge qualora abbiano modo di verificarsi le seguenti ipotesi:

- entrata in vigore di nuove disposizioni legislative tali da comportare l'inadeguatezza, totale o parziale, del presente documento;
- adozione di rilevanti modifiche afferenti la struttura organizzativa, logica e informatica del titolare;
- apporto di sostanziali interventi sull'assetto delle preesistenti misure di sicurezza;
- su indicazione dell'amministratore di sistema per comprovate esigenze di sicurezza.

La nuova versione del documento sarà integrata con il verbale del processo di revisione.

In ogni caso l'Ente programma la successiva revisione del Documento Programmatico sulla Sicurezza entro il 31 marzo 2012.

E. Descrizione dell'assetto dell'istituto comprensivo

L'Istituto Comprensivo di Scuola Primaria e Secondaria di primo grado ROVERETO SUD è composto e dislocato fisicamente su quattro sedi:

- **La Scuola Primaria "D. Alighieri", Via Benacense n. 32, 38068 Rovereto (TN);**
- **La Scuola Primaria "F. Guella", Via Piave, Loc. Lizzana, 38068 Rovereto (TN);**
- **La Scuola Primaria "A. Rosmini", Via II Novembre n. 57, Loc. Marco, 38068 Rovereto (TN);**
- **Scuola Secondaria "F. Halbherr", Via Benacense n. 27, 38068 Rovereto (TN), presso la scuola ex-edili. La sede è in fase di ristrutturazione.**

Viene di seguito descritta analiticamente la struttura informatica allocata presso ciascuna delle sedi che compongono l'Istituto.
Ogni informazione nel merito delle misure di sicurezza adottate al fine di garantire la disponibilità e, contestualmente, prevenire la possibilità che i dati oggetto di trattamento possano essere danneggiati ovvero illegittimamente acquisiti da parte di terzi non autorizzati comporranno la ricognizione elaborata nel capitolo III del presente Documento.

La struttura informatica dell'Istituto risulta composta come di seguito:

UFFICI DI SEGRETERIA

presso la scuola elementare "D. ALIGHIERI":

rete client/server composta da
n. 1 server con sistema operativo Windows Server 2008 il cui aggiornamento avviene automaticamente;
n. 10 PC ad uso degli uffici (di cui n. 7 ad uso del personale di segreteria,
n. 1 ad uso del dirigente e n. 1 ad uso della collaboratrice-vicaria) 1 ad uso del tecnico

tutti con sistema operativo Windows Xp pro il cui aggiornamento avviene automaticamente;

presso le scuole medie "F. HALBERR":
gruppo di lavoro formato da n. 3 PC tutti con sistema operativo Windows Xp aggiornato automaticamente;

è stato prescritto di non salvare dati personali su queste postazioni

I PC degli uffici amministrativi sono interconnessi fra loro, e a loro volta alla rete Internet tramite router ADSL. Su rete con telecom

DIDATTICA

presso la scuola elementare "D. ALIGHIERI":
rete client/ server composta da
- n. 1 server con sistema operativo Windows Server 2003 aggiornato;
- n. 25 PC in aula informatica con sistema operativo Windows XP sp. 3
- n. 9 PC rispettivamente posizionati:

n. 2 in aula insegnanti connessi ad internet ed alla rete del laboratorio informatico,
n. 1 in aula multimediale,
n. 1 in aula magna,
n. 4 con lavagna multimediale ad uso delle classi
n. 1 portatile a disposizione con Sistema operativo Windows XP sp pro agg.;

I PC del laboratorio informatico sono interconnessi fra loro ed alla rete Internet mediante linea ADSL

Presso le scuole medie"F. HALBERR":
rete client / server composta da
- n. 1 server con sistema operativo Windows Server 2008;
- n. 25 PC in aula informatica, tutti con sistema operativo Windows XP Pro sp 3;
- n. 20 pc nelle diverse aule tutti con sistema operativo Windows XP Pro sp 3:

n. 3 pc in aula insegnanti, n. 2 pc in aula di sostegno, 11 pc collegati a lavagne multimediali, n. 1 pc in a biblioteca, n. 2 pc a disposizione;
n. 5 PC portatili, tutti con sistema operativo Windows XP Pro sp 3;

I PC del laboratorio informatico sono interconnessi fra loro ed alla rete Internet mediante ADSL

Presso la scuola elementare "F. GUELLA":
rete client / server composta da
- n. 1 server con sistema operativo Win Server 2003 aggiornato;
- n. 15 PC in aula informatica con sistema operativo Windows XP Pro sp. 3;
- n. 7 PC tutti con sistema operativo Windows XP Pro sp. 3 variamente distribuiti nelle classi; 1 aula ir sostegno,

n. 4 utilizzati nelle aule con le lavagne multimediali, n. 2 PC portatili a disposizione

I PC del laboratorio informatico sono interconnessi fra loro ed alla rete Internet mediante ADSL

Presso la scuola elementare "A. ROSMINI":
rete client / server composta da
- n. 1 Server con sistema operativo Windows Server 2003 aggiornato;
- n. 15 PC in aula informatica, con sistema operativo Windows XP Pro sp 3
- n. 6 PCtutti con sistema operativo Windows XP Pro sp 3, ad uso delle classi:

n. 4 pc utilizzati con lavagne multimediali, n. 1 pc in aula insegnanti, n. 1 pc in aula di sostegno.

I PC del laboratorio informatico sono connessi fra loro ed a loro volta alla rete internet tramite linea ADSL

In aula sostegno sono altresì presenti n. 2 pc fuori rete con windows 98.

CAPITOLO I

ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Nel presente capitolo si elencano, per ciascuna tipologia di trattamento, la natura dei dati trattati, di seguito esemplificata in base alla struttura/ufficio di riferimento, alla tipologia di trattamento e relativa finalità. I trattamenti effettuati tramite strumenti elettronici possono essere conservati anche su supporto cartaceo.

Elenco dei dati sensibili e giudiziari ex art. 4 lett. d) e lett. e) del D.lgs.. n. 196/2003

- *dati idonei a rivelare le origini razziali ed etniche*
- *dati idonei a rivelare le convinzioni religiose, filosofiche o di altro genere*
- *dati idonei a rivelare le opinioni politiche*
- *dati idonei a rivelare l'adesione a partiti, sindacati*
- *associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale*
- *dati idonei a rivelare lo stato di salute*
- *dati idonei a rivelare la vita sessuale*
- *dati giudiziari*

TRATTAMENTI **Finalità** **Struttura di riferimento**	**Modalità di trattamento**	**TIPI DI DATI TRATTATI** **con specifico riferimento ai dati sensibili e giudiziari ex art. 4 lett. d) e lett. e) del D.lgs.. n. 196/2003**
DIRIGENZA SCOLASTICA E PERSONALE AMMINISTRATIVO		
Rappresentanza dell'Istituto e sovrintendenza generale di tutti i servizi amministrativi, gestionali e organizzativi dell'Istituto (DIRIGENZA SCOLASTICA)	Cartacea e elettronica	Da 1 a 8
Gestione esclusiva dell'area "protocollo riservato" relativo a alunni, utenza esterna, genitori, personale amministrativo e docenti. Responsabile della catalogazione del protocollo riservato, ivi comprese le sanzioni disciplinari nei confronti del personale e degli alunni (solo DIRIGENZA SCOLASTICA)	Cartacea e elettronica	Da 1 a 8
Accoglimento e valutazione domande di ammissione all'istituto comprensivo e procedimento di iscrizione con i relativi atti e documenti allegati e connessi	Cartacea e elettronica	1, 2, 5, 6
Sovrintendenza ai servizi generali amministrativo contabili	Cartacea e elettronica	2, 3, 4, 6
Esecuzione degli atti amministrativi-contabili, di ragioneria e di economato	Cartacea e elettronica	4,5,6,8
Esecuzione delle delibere collegiali a carattere contabile e redazione di atti amministrativi scolastici e contabili	Cartacea e elettronica	1,2,4,5,6

Tenuta dell'archivio e del protocollo	Cartacea e elettronica	Da 1 a 8
Funzioni generali di segreteria	Cartacea e elettronica	2, 6,1
Attività di formazione, aggiornamento e tutorie per neoassunti	Cartacea e elettronica	2, 6
Gestione amministrativa e contabile, gestione acquisti, gestione personale per le rispettive competenze (rilevazione presenze e trasmissione dati PAT), fornitori e magazzino, trattamento contabile amministrativo e gestione logistica	Cartacea e elettronica	Da 1 a 8
Organizzazione, coordinamento, promozione di attività e verifica dei risultati rispetto a obiettivi assegnati e indirizzi impartiti dal Dirigente Scolastico	Cartacea e elettronica	1,2,6
Gestione anagrafiche fornitori e alunni, gestione rilevazione presenze	Cartacea e elettronica	1,2,6,8
Gestione e organizzazione richieste di accesso a documenti amministrativi	Cartacea e elettronica	Da 1 a 8
Adempimenti ex D.lgs.. n. 81/08	Cartacea e elettronica	Da 1 a 8
Ricevimento c.v. docenti e personale amministrativo	Cartacea e elettronica	Da 1 a 8
Documentazione gare e appalti	Cartacea e elettronica	Da 1 a 8
Gestione anagrafica studenti, organizzazione attività extrascolastiche, gestione attività iscrizione	Cartacea e elettronica	Da 1 a 8
Gestione fornitori, anagrafica consulente, incarichi, collaboratori	Cartacea e elettronica	
Gestione infortuni sul lavoro, gestione personale	Cartacea e elettronica	Da 1 a 8

Gestione servizio mensa	Cartacea e elettronica	Da 1 a 8

Categorie di interessati: docenti, personale amministrativo e collaboratori, alunni e rispettive famiglie (genitori), fornitori, consulenti

ASSISTENTE DI LABORATORIO SCOLASTICO / TECNICO INFORMATIC

Responsabile dei servizi di laboratorio e informatici, supporto e assistenza informatica	Cartacea e elettronica	1,2,5
Collaborazione con i docenti per l'esecuzione di esperimenti o per la preparazione delle lezioni	Cartacea e elettronica	1,2,5
Cura delle attrezzature tecniche e gestione tecnico organizzativa delle attività di manutenzione anche in collaborazione con consulenti o aziende esterne	Cartacea e elettronica	1,2,5
Riordino delle attrezzature e verifica dell'approvvigionamento periodico, anche in relazione con l'attività di collaborazione con gli appositi uffici inerente agli acquisti e al collaudo	Cartacea e elettronica	1,2,5

C*ategorie di interessati: docenti, personale amministrativo e collaboratori, alunni e rispettive famiglie (genitori), fornitori, consulenti*

PERSONALE DOCENTE

Gestione e organizzazione didattica e amministrativa degli alunni, comportante anche le attività connesse di sorveglianza durante l'orario scolastico e extrascolastico (nei casi espressamente definiti) sia all'interno che all'esterno dell'edificio	Cartacea	1, 2, 5, 6, 7, 8
Gestione prenotazioni e escursioni, gestione attività extrascolastiche	Cartacea e elettronica	6
gestione infortuni alunni (primo	Cartacea e elettronica	1, 2, 5, 6, 7, 8

soccorso)

Assistenza durante il servizio mensa	Cartacea e elettronica	Da 1 a 8
Gestione ora di religione	Cartacea	2, 5
Gestione documentazione di classe	Cartacea	2, 5, 6
Registri di classe Registri personali Programmazione didattica Documentazione sullo stato di salute degli alunni Corrispondenza con le famiglie	Elettronica (limitata alla gestione dei dati comuni)	

Categorie di interessati: docenti, alunni e rispettive famiglie (genitori).

PERSONALE AUSILIARIO

Assistenza e collaborazione nello svolgimento dei servizi di segreteria e di informazione a alunni, docenti e collaboratori. Assistenza e collaborazione nei servizi citati e in quelli indicati dal personale amministrativo (ivi compreso il servizio di fotocopiatura, registrazione e custodia del materiale affidato) Svolgimento attività di pulizia generale	Cartacea (anche tramite fax e fotocopiatori)	1, 2, 4, 5, 6

Categorie di interessati: docenti, personale amministrativo e collaboratori, alunni e rispettive famiglie (genitori), fornitori, consulenti

Ogni soggetto operante presso l'istituto comprensivo che, per ragioni connesse al proprio incarico, potrebbe avere modo di trattare dati personali, e' stato incaricato al trattamento dei dati ex art. 30 d.lgs.. 196/2003 con definizione dell'ambito di trattamento.
Presso la segreteria e' disponibile l'ambito di trattamento con la definizione relativa alle operazioni di trattamento consentite per ciascuna delle classi di appartenenza.

CAPITOLO II

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ IN RELAZIONE AL TRATTAMENTO DEI DATI

TITOLARE DEL TRATTAMENTO

Istituto Comprensivo ROVERETO SUD

*Ai sensi dell'art. **28 del d.lgs. n. 196/2003**, il Titolare del trattamento è individuato come segue:*

"Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza."

RESPONSABILI DELL'UFFICIO / SERVIZIO

Vedi atti di nomina a disposizione presso la Segreteria dell'Ente.

RESPONSABILI DEL TRATTAMENTO INTERNI

Vedi atti di nomina a disposizione presso la Segreteria dell'Ente.

*Ai sensi dell'art. **29 del D. Lgs. n. 196/2003**, il Responsabile del trattamento è individuato nel modo seguente*

1. Il responsabile è designato dal titolare facoltativamente.

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

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

RESPONSABILI DEL TRATTAMENTO ESTERNI:

Vedi atti di nomina a disposizione presso la Segreteria dell'Ente.

CUSTODE DELLE PASSWORD (se nominato)

Vedi atti di nomina a disposizione presso la Segreteria dell'Ente.

INCARICATI:

vedi atti di incarico a disposizione presso la segreteria dell'ente.

Ai sensi dell'art. ***30 del D. Lgs. n. 196/2003****, gli Incaricati del trattamento sono individuati nel modo seguente:*

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

AMMINISTRATORE DI SISTEMA

Si vedano gli atti di nomina a disposizione presso gli uffici di segreteria.

Per amministratore di sistema deve intendersi il soggetto cui è conferito il compito di sovrintendere alla gestione e alla manutenzione delle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

CAPITOLO III

Analisi dei rischi e misure da adottare per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali

I possibili rischi individuati sono i seguenti:

AREE E LOCALI	❑ Intrusione ❑ Ingresso non controllato o non autorizzato ❑ Incendio
INTEGRITÀ E DISPONIBILITA' DEI DATI	❑ Amministratore di sistema ❑ Danneggiamento, perdita, alterazione a causa di: • virus • mancanza di energia elettrica • avaria • allagamento • accessi non consentiti • furti o manomissioni hardware e software • non conoscenza da parte degli incaricati delle procedure informatiche, delle misure di sicurezza, dei rischi ❑ Danneggiamento, perdita, alterazione dei dati contenuti nei supporti di memorizzazione a causa di: • furti • copie abusive • incendio • allagamento • danneggiamento/alterazione dei supporti ❑ Danneggiamento, perdita, alterazione dei dati durante la trasmissione degli stessi a causa di: • intercettazione • errore di invio • mancata destinazione • avaria • intrusione di terzi non autorizzati • virus ❑ Inidoneo utilizzo degli strumenti informatici • Erroneo utilizzo rete • Erroneo utilizzo di Internet e posta elettronica

PRESIDIO DELLA SICUREZZA SULLE AREE E LOCALI

Ove non vengono introdotte distinzioni, le misure indicate, con le modalità qui registrate, sono da intendersi adottate presso tutti gli edifici dei vari plessi, e sia per il trattamento effettuato nell'ambito dell'attività di segreteria, che nell'ambito della didattica

RISCHIO INTRUSIONE:

Misure di sicurezza adottate:

- chiusura del cancello chiuso all'ingresso
- nelle ore di lezione è utilizzato un sistema di video-sorveglianza mediante collocazione di telecamera posta sul cancello d'entrata principale della sede centrale
- recinzione delle aree perimetrali
- durante l'orario lavorativo l'accesso all'ingresso principale è chiuso e sorvegliato dal personale ausiliario in servizio;
- l'accesso dei dipendenti viene regolato mediante apposito sistema di registrazione in ingresso ed uscita
- - la sorveglianza della sede centrale ove sono gli uffici amministrativi durante il periodo notturno è affidata ad un servizio privato di vigilanza
- .è presente un sistema di allarme dotato di sirena acustica e collegamento telefonico ai responsabili e ad un servizio privato di vigilanza

Evento	Probabilità	Danno	Rischio
Intrusione	1	3	3

MISURE DA ADOTTARE:
Non si ritiene necessario adottare ulteriori misure di sicurezza.

RISCHIO DI INGRESSO NON CONTROLLATO O NON AUTORIZZATO

Misure di sicurezza adottate
- al di fuori delle aree al pubblico, eventuali visitatori (es. prestatori d'opera, genitori) sono accompagnati e vigilati dal personale in servizio;
- l'accesso dei dipendenti viene controllato tramite firma sul registro (personale ATA)
- l'accesso ai locali della scuola ove sono gli uffici amministrativi al di fuori dell'orario di lavoro è ammesso solamente previa autorizzazione del dirigente; tale autorizzazione viene comunicata al personale responsabile della custodia dell'ufficio, il quale provvede ad accompagnare l'autorizzato durante la sua permanenza all'interno;
- l'accesso è comunque escluso nelle aree ove sono collocati gli archivi;
- le porte dei locali degli edifici amministrativi, ove sono collocati gli archivi in formato cartaceo ed elettronico dei dati personali, sono provviste di serrature, le cui chiavi sono in dotazione al personale autorizzato all'accesso;

le chiavi della porta di ingresso all'edificio sono in possesso del titolare, del portiere e degli addetti alle pulizie
le chiavi delle porte di ingresso alle singole stanze sono in possesso degli addetti alle pulizie

Evento	Probabilità	Danno	Rischio
Ingresso non controllato o non autorizzato	1	3	3

MISURE DA ADOTTARE:
Non si ritiene necessario adottare ulteriori misure di sicurezza.

RISCHIO DANNEGGIAMENTO PER INCENDIO:
Misure di sicurezza attualmente adottate:
- la struttura è dotata di estintori installati e revisionati a norma di legge la struttura è adeguata alle disposizioni in materia di sicurezza di cui al D.lgs.. n. 81/2008
- sono in particolare presenti rilevatori di fumo e dispositivi a pioggia, in alcuni locali
- i possibili danni provocati da furto e incendio sono comunque oggetto di copertura mediante polizza assicurativa stipulata per il furto dall'Istituto e per l'incendio dal Comune di Rovereto

Evento	Probabilità	Danno	Rischio
Incendio	1	3	3

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza.

PRESIDIO DELLA SICUREZZA SUI DATI

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE DEI DATI A CAUSA DI UN ACCESSO ABUSIVO A SISTEMA INFORMATICO O TELEMATICO, DI FRODE INFORMATICA, NONCHÉ DI DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI E DI DANNEGGIAMENTO DI SISTEMI INFORMATICI E TELEMATICI DA PARTE DELL'AMMINISTRATORE DI SISTEMA (PROVV. GARANTE 27/11/08)

Misure di sicurezza attualmente adottate:
- ✧ Gli amministratori di sistema sono stati incaricati per iscritto in modo tale da definire gli ambiti di operatività ad essi assegnati;
- ✧ la richiesta dei nominativi è stata inoltrata anche alla società Informatica Trentina S.p.a, la quale ha risposto con nota agli atti,
- ✧ gli accessi ai sistemi di elaborazione e agli archivi elettronici vengono registrati con un sistema idoneo;
- ✧ le registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità;
- ✧ le registrazioni vengono conservate per 6 mesi;
- ✧ ogni anno viene verificata l'operato degli amministratori di sistema.

Evento	Probabilità	Danno	Rischio

Comportamenti sleali o fraudolenti	1	2	2
Errore materiale	1	2	2
Distruzione dati	1	2	2

Accesso ai dati non consentito e non autorizzato	1	3	3
Sottrazione di credenziali di autenticazione	1	3	3
Danneggiamento/perdita dati per improprio utilizzo degli strumenti informatici	1	2	2

MISURE DA ADOTTARE:
Non si ritiene necessario adottare ulteriori misure di sicurezza.

RISCHIO DANNEGGIAMENTO,PERDITA, ALTERAZIONE A CAUSA DI VIRUS:

Misure di sicurezza attualmente adottate:

- Su tutti i Pc sono stati installati software antivirus il cui aggiornamento avviene giornalmente in modalità automatica da Internet (Live Update).

Evento	Probabilità	Danno	Rischio
Virus	1	3	3

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza.

RISCHIO DANNEGGIAMENTO,PERDITA, ALTERAZIONE A CAUSA DI PROGRAMMI DANNOSI O TECNICHE DI SABOTAGGIO:

Misure di sicurezza attualmente adottate:

- Su tutti i Pc sono stati installati software antivirus con antimalware il cui aggiornamento avviene giornalmente in modalità automatica da Internet (Live Update).

Evento	Probabilità	Danno	Rischio
danneggiamento	1	3	3

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza.

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE A CAUSA DI MANCANZA DI ENERGIA ELETTRICA:

Misure di sicurezza attualmente adottate:

- Presso gli uffici amministrativi c/o scuole medie: il server i computer sono collegati ad un dispositivo che assicura per circa 15 minuti la continuità della tensione elettrica fintanto che il personale possa provvedere al salvataggio dei dati in corso di elaborazione e corretto spegnimento delle macchine

Evento	Probabilità	Danno	Rischio
Perdita dati (per mancanza energia elettrica)	1	3	3

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza

RISCHIO DI DANNEGGIAMENTO PER ALLAGAMENTO

Misure di sicurezza attualmente adottate:

- Presso gli uffici amministrativi: gli uffici sono ubicati al secondo piano rialzato. Il server che reca i dati è rialzato da terra. I supporti informatici sono conservati in contenitori rialzati da terra.
- Gli archivi cartacei sono conservati in appositi armadi
- Presso i vari plessi: i PC della didattica sono tutti rialzati da terra

Evento	Probabilità	Danno	Rischio
Incendio	1	3	3

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE A CAUSA DI AVARIA DEL SISTEMA INFORMATICO O DEI SOFTWARE INSTALLATI:

Misure di sicurezza attualmente adottate:

- Sono stati stipulati contratti di assistenza Hardware e sistemistica.
- Per gli uffici di Segreteria il back up dei dati avviene tramite cassette con periodicità giornaliera.
- E' attivo un sistema RAID (da cancellare?)
- I supporti della copia di back-up sono sei e riportano le indicazioni del giorno
- La verifica dell'effettiva esecuzione del back up è effettuata dal personale appositamente incaricato.
- l'Istituto dispone di un tecnico-informatico per 18 ore settimanali che fornisce assistenza in didattica e anche in segreteria (qui interviene solo su specifica chiamata in presenza del personale di segreteria).

- I software sono aggiornati periodicamente in modalità automatica
- Per la didattica, e nei diversi plessi, il back up dei dati avviene con cadenza settimanale e effettuando copia dei dati su uno dei PC presenti nell'aula informatica a scelta del tecnico informatico che esegue l'operazione, ma comunque in modo da non permetterne l'accesso ad altri studenti / incaricati. Ove non sia possibile il salvataggio dati con le descritte modalità viene disposto il divieto di salvataggio dati personali

Evento	Probabilità	Danno	Rischio
Perdita dati causa avaria	1	3	3

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE A CAUSA DI ACCESSI NON CONSENTITI, FURTI O MANOMISSIONI HARDWARE E SOFTWARE, NON CONOSCENZA DA PARTE DEGLI INCARICATI DELLE PROCEDURE INFORMATICHE, DELLE MISURE DI SICUREZZA, DEI RISCHI:

Misure di sicurezza attualmente adottate:

- L'accesso ai dati è consentito solo tramite inserimento di codice identificativo personale e parola chiave attribuiti ad ogni utente.
- Sono stati adottati profili di autorizzazione con limitazione degli accessi in base alle mansioni assegnate.
- Il personale ha ricevuto informativa in ambito privacy mediante obbligo di consultazione delle linee guida sul sito internet.
- E' stata data diffusione al Documento programmatico per la sicurezza tramite il sito internet.
- Sono stati proposti al personale corsi sull'uso di PC e programmi
- Il server è ubicato in un ufficio, ove è sempre presente personale in servizio e altrimenti chiusa a chiave.
- Vige il divieto di installazione autonoma di software e hardware.

Evento	Probabilità	Danno	Rischio
Accesso non consentito ai dati	1	2	2
Furti - Manomissione hardware / software	1	3	3
Ignoranza delle procedure informatiche, delle misure di sicurezza e dei rischi	1	2	2

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza.

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE DEI DATI SU SUPPORTI DI MEMORIZZAZIONE A CAUSA DI FURTI, COPIE ABUSIVE, INCENDIO, ALLAGAMENTO, DANNEGGIAMENTO O ALTERAZIONE DEI SUPPORTI

Misure di sicurezza attualmente adottate:

- Per la segreteria: i supporti di memorizzazione sono conservati in cassaforte, blindata e ignifuga.
- I supporti di back up utilizzati vengono rinnovati con periodicità annuale.
- Sono state date istruzioni ed indicazioni agli incaricati relativamente alla custodia dei supporti di back up
- Per al didattica: la copia su PC diverso dal server viene effettuata in modo da non permetterne l'accesso ad altri studenti / incaricati.

Evento	Probabilità	Danno	Rischio
Furto	1	3	3
Copia abusiva	1	3	3
Incendio	1	3	3
Allagamento	1	3	3
Danneggiamento Alterazione	1	2	2

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza.

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE DI DATI DURANTE L'INVIO DEGLI STESSI PER INTERCETTAZIONE, ERRORE DI INVIO, MANCATA DESTINAZIONE, AVARIA, INTRUSIONE DI TERZI NON AUTORIZZATI, VIRUS

Misure di sicurezza attualmente adottate:

- Le trasmissioni sono protette da antivirus aggiornato giornalmente in automatico da Internet.
- Sono state attivate procedure di back up dei dati
- Per il collegamento esterno è presente un router che permette la trasmissione di dati e l'accesso a Internet tramite Informatica Trentina. Tali connessioni sono protette dai Firewall di Informatica Trentina.
- L'accesso remoto è consentito solo a personale incaricato o all'assistenza tecnica previa richiesta telefonica da parte nostra o della società incaricata, di attivazione del programma che consente l'accesso, e disattivazione del programma al termine dell'accesso, per quanto riguarda gli Uffici.

- ✧ L'accesso remoto è consentito solo a personale incaricato tramite password per gli strumenti informatici in uso alla Didattica.
- ✧ Il personale ha ricevuto formazione in ambito privacy la consegna di linee guida.

Evento	Probabilità	Danno	Rischio
Intercettazione	1	3	3
Errore di invio / mancata destinazione	1	2	2
Avaria	1	2	2
Intrusione di terzi non autorizzati	1	2	2
Virus	1	3	3

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza.

RISCHIO DI TRATTAMENTO ILLECITO, DANNEGGIAMENTO PERDITA DEI DATI A CAUSA DI SOTTRAZIONE DI CREDENZIALI DI AUTENTUÌICAZIONE, DISATTENZIONE O INCURIA, COMPORTAMENTI SLEALI O FRAUDOLENTI, ERRORE MATERIALE DA PARTE DEGLI OPERATORI.

- ✧ Sono stati adottati profili di autorizzazione con limitazione degli accessi in base alle mansioni assegnate.
- ✧ Sono state date istruzioni ed indicazioni agli incaricati relativamente alla custodia dei supporti di back up

Evento	Probabilità	Danno	Rischio
Trattamento illecito	1	3	3
Danneggiamento	1	2	2
Perdita dei dati	1	2	2

MISURE DA ADOTTARE:

Non si ritiene necessario adottare ulteriori misure di sicurezza.

PROSPETTO DI SINTESI SUL LIVELLO DI RISCHIO

In questa sezione del documento si è provveduto a riportare, coerentemente con quanto indicato alla regola 19.3 del Disciplinare tecnico all. B del Codice, i principali eventi potenzialmente dannosi per la sicurezza dei dati.

Metodologicamente si è proceduto ad individuare gli eventi che possono potenzialmente costituire dei rischi per la sicurezza dei dati, suddividendoli per rischi gravanti su:

- *operatori presenti*

- *strumenti utilizzati, sia di tipo elettronico sia di tipo non elettronico*
- *contesto fisico ed ambientale*

Per la classificazione del rischio si sono utilizzati 4 livelli secondo i criteri riportati nella tabella che segue:

Probabilità: (P)	1	Improbabile
	2	Poco Probabile
	3	Probabile
	4	Altamente probabile
Danno (D)	1	Lieve
	2	Medio
	3	Grave
	4	Gravissimo

In relazione all'indice R si identifica quale misura dovrà essere adottata per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti al fine della loro custodia e accessibilità.

In considerazione del fatto che il rischio 0 assoluto non può esistere si determina il livello di sopportazione del rischio:
Sopportazione da 1 a 4
Riduzione del rischio oltre 4

Pertanto, nel complesso, il livello di rischio si considera rispettivamente:

Livello	Descrizione del rischio
Basso	L'evento dannoso considerato può accadere solo per la concomitanza di più cause indipendenti e poco probabili
	Non sono noti episodi già verificatisi
	Il verificarsi del danno susciterebbe incredulità
	Danno rapidamente reversibile
Medio	L'evento dannoso considerato può accadere, anche se non in modo automatico o diretto
	E' noto qualche episodio in cui alla mancanza ha fatto seguito il danno
	Il verificarsi del danno ipotizzato, susciterebbe una moderata sorpresa
	Danno solo parzialmente reversibile
Alto	L'evento dannoso considerato può accadere per una solo causa non improbabile
	Si sono già verificati danni per la stessa mancanza
	Il verificarsi del danno conseguente la mancanza rilevata non susciterebbe alcuno stupore
	Danno irreversibile

In sintesi, per ogni categoria di rischio si è proceduto a valutarne la gravità così come esposto nella tabella che segue.

	Rischio	Gravità
Operatori	Sottrazione di credenziali di autenticazione	Basso
	Carenza di consapevolezza, disattenzione o incuria	Medio alto
	Comportamenti sleali o fraudolenti	Basso

	Errore materiale	Medio
	Altro evento	-
Strumenti	Azione di virus informatici o di programmi suscettibili di recare anno	Medio
	Spamming o tecniche di sabotaggio	Medio/Basso
	Malfunzionamento, indisponibilità o degrado degli strumenti	Basso
	Accessi esterni non autorizzati	Medio
	Intercettazione di informazioni in rete	medio
	Altro evento	-
Contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	Medio/alto
	Sottrazione di strumenti contenenti dati	Medio/alto
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.) nonché dolosi, accidentali o dovuti ad incuria	Basso
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Basso
	Errori umani nella gestione della sicurezza fisica	Basso
	Altro evento	-

Sintesi delle misure in essere e da adottare

Coerentemente con quanto previsto dalla regola 19.4 del Disciplinare tecnico all. B) del Codice, ed in base all'analisi dei rischi effettuata, all'interno della nostra struttura si è provveduto a mettere in atto le misure idonee a contrastare i rischi individuati.

Misura	Note
Stesura ed aggiornamento periodico, con cadenza almeno annuale, della lista degli incaricati	
Impostazione ed aggiornamento periodico, con cadenza almeno annuale, dei profili di autorizzazione	
Assegnazione di credenziali di autenticazione che rispondono ai requisiti di sicurezza e che sono modificate con i tempi e le modalità previsti dal Codice	
Upgrade a Windows xp ed aggiornamento sistema operativo	
Istruzioni in merito agli accessi agli archivi, all'effettuazione dei trattamenti, al controllo e custodia dei documenti, e alla segretezza e custodia delle credenziali di autenticazione	
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati.	
Formazione sugli aspetti principali della disciplina della privacy al momento dell'ingresso in servizio, periodica ed in occasione del cambio di mansioni o di aggiornamenti degli strumenti, delle procedure e delle norme di riferimento	
Utilizzo e aggiornamento periodico dei programmi antivirus	
Utilizzo e aggiornamento periodico di sistemi Firewall	
Manutenzione ed aggiornamento programmato degli strumenti	
Effettuazione delle copie di back up dei dati, delle impostazioni e delle applicazioni e custodia sicura dei supporti di memorizzazione	
Porte e finestre degli uffici munite di serrature	
Porte degli armadi muniti di serratura	
Sistema di rilevamento antincendio e spegnimento manuale	
Sistema di allarme antintrusione con codici	

CAPITOLO IV
Criteri di ripristino dati e relative modalita'

(Punto 19.5 e 23 del disciplinare tecnico – all. B D. Lgs 196/2003)

Responsabile interno di procedura: si veda nomina agli atti

Il Responsabile della procedura di ripristino dati avrà il compito di coordinare le operazioni di recupero sotto riportate e di mantenere i rapporti con i soggetti / aziende esterne, incaricati del recupero stesso.

Misure preventive:

- ✧ Assicurarsi dell'effettiva esecuzione di Back up di sistema su server tramite consultazione del file di Log;
- ✧ Archiviare 1 copia di back up di sistema (PROGRAMMI E DATI) in un armadio chiuso a chiave e aggiornarlo con cadenza non superiore ai sette giorni.
- ✧ Mantenere un elenco aggiornato di aziende in grado di fornire entro 5 gg dall'evento componenti hardware (server o personal computer) e assistenza sistemistica e software. (Elencare eventuali contratti di assistenza con specifiche clausole contrattuali relative ai tempi di intervento e/o sostituzione, anche provvisoria, di componenti hardware).
- ✧ Eseguire prove di ripristino dati secondo le seguenti modalità:
  - Richiedere al fornitore del sistema le procedure di ripristino dati;
  - Creare un file campione di prova;
  - Effettuare le procedure di salvataggio periodico dei dati;
  - Attuare la procedura di ripristino del file di prova dal supporto informatico utilizzato per il salvataggio;

Tempi previsti per la prova di ripristino: Entro il 31 / 12 / 2011

Se l'esito della prova di ripristino dati risultasse negativa, contattare l'assistenza tecnica per procedere alla verifica del sistema e all'individuazione delle cause del mancato ripristino.

Misure di ripristino in caso di perdita di dati e/o strumenti elettronici:

- ✧ Contattare il fornitore di componenti hardware e richiedere la fornitura entro 5 giorni della macchina server e delle ulteriori macchine danneggiate;
- ✧ Contattare il fornitore di servizi di assistenza sistemistica e concordare l'intervento per il ripristino di dati da Back up; (se non presente figura idonea alla mansione);
- ✧ Contattare il fornitore di eventuali ulteriori software per l'installazione ed il ripristino dei dati contenuti negli applicativi.

In collaborazione con i vari responsabili di settore/servizi effettuare un controllo sui dati di competenza, al fine di verificare l'effettivo avvenuto ripristino dei dati stessi.

CAPITOLO V
Piano di formazione agli incaricati del trattamento

Argomenti oggetto della formazione:

- Rischi
- Misure di Prevenzione
- Profili normativi in relazione alle mansioni
- Responsabilità che ne derivano
- Modalità di aggiornamento delle misure di sicurezza
- Modalità di corretto utilizzo degli strumenti informatici (Internet e posta elettronica)

Frequenza:

- Entrata in servizio
- Cambiamento di mansioni
- Introduzione di nuovi strumenti rilevanti rispetto al trattamento di dati personali
- Adozione di nuove misure di sicurezza, sia logiche che documentali.

Modalità di formazione:

- **Formazione tramite linee guida:**

Redazione e consegna di guida formativa. La guida formativa viene allegata al presente documento programmatico e ne costituisce parte integrante

Si è elaborato ed è stato portato a conoscenza degli incaricati un regolamento interno nel quale sono state specificate le corrette modalità di utilizzo degli strumenti informatici (internet, posta elettronica, rete, ecc.) da parte di dipendenti e collaboratori in linea con quanto suggerito dal Garante con proprio provvedimento di data 01 marzo 2007.

- **Messa a disposizione degli incaricati del Documento Programmatico sulla Sicurezza.**

CAPITOLO VI

Trattamenti esterni: criteri da adottare per garantire l'adozione delle misure minime di sicurezza

Nel contratto o nell'atto che prevede l'affido di svolgimento di attività a soggetti esterni, dovranno essere inserite alcune clausole contrattuali al fine di impegnare il soggetto esterno a garantire un adeguato trattamento dei dati personali così come previsto dal codice per la protezione dei dati personali.

Nel contratto o nell'atto che prevede l'esercizio delle attività deve essere inoltre contemplata la possibilità da parte del titolare del trattamento di effettuare verifiche sui trattamenti svolti per conto della società dal soggetto esterno.

Nell'allegato A sono definite le clausole contrattuali da inserire nel contratto a cura del titolare.

Il titolare deve tenere un elenco dei soggetti esterni ai quali vengono affidate le attività secondo lo schema sotto riportato.

In seguito alla nomina di responsabile o alla delega dell'attività, a seconda della tipologia di incarico e delle operazioni affidate allo stesso, il controllo sulle misure di sicurezza deve avvenire tramite elaborazione di una check-list redatta dal titolare e da compilarsi a cura del soggetto esterno.

La check list viene allegata (allegato B) al presente documento.

Data	Nome del soggetto esterno	Attività delegata	Tipi di dati trattati (comuni, sensibili, giudiziari)	Nominato responsabile (SI/NO)

CAPITOLO VII

Periodicità e modalità dei controlli

Il responsabile dei controlli sulle misure di sicurezza informatiche avrà il compito di provvedere, personalmente o tramite aziende specializzate, alla verifica della funzionalità e dell'efficienza delle misure di sicurezza adottate.

Dovrà essere redatto l' apposito verbale con gli esiti delle verifiche stesse la cui traccia è indicata nello schema di cui all'allegato C.

Responsabile dei controlli: dipendente incaricato della mansione

Cadenza dei controlli: annuale

CAPITOLO VIII

Misure e accorgimenti adottati dal titolare del trattamento relativamente alle attribuzioni delle funzioni di amministratore di sistema

Provvedimento garante privacy 27 novembre 2008

Gli *amministratori di sistema* sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle strutture informatiche. Per definizione normativa si tratta infatti di figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

L'eventuale attribuzione delle competenze e la specifica descrizione delle funzioni demandate dal titolare del trattamento ai propri incaricati, ai responsabili e all'*amministratore di sistema* trovano descrizione nel contesto dei capitoli III, IV, VI, VII del presente Documento programmatico sulla sicurezza e nella ulteriore documentazione agli atti (all. E).

1) INDICAZIONE DEGLI ESTREMI IDENTIFICATIVI DEI SOGGETTI NOMINATI AMMINISTRATORI DI SISTEMA:

si vedano nomine agli atti

Le funzioni assegnate all'amministratore di sistema, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, sono state attribuite previa una attenta valutazione dell'esperienza, della capacità e dell'affidabilità.

L'elenco delle funzioni, così come le specifiche modalità di adempimento dell'incarico attribuito e le procedure atte a garantire il controllo da parte del titolare sono state specificate nell'atto di nomina (all.E).

Per l'esatta rappresentazione delle funzioni e degli ambiti di operatività assegnati si rinvia dunque all'atto di nomina che compone parte integrante del presente documento.

2) MISURE ATTE A GARANTIRE LA TUTELA DELLA RISERVATEZZA DI EVENTUALI DATI AFFERENTI INFORMAZIONI DI CARATTERE PERSONALE DEI DIPENTENTI
Descrizione delle procedure adottate onde rendere noto a tutti i lavoratori l'eventuale ipotesi in cui l'amministratore di sistema possa avere accesso e trattare informazioni di natura personale loro riferite.

Comunicazione verbale

3) SERVIZI AFFIDATI IN OUTSOURCING

Il titolare, valutata la propria attività di trattamento dati e l'attuale organizzazione dello stesso, ritiene di non nominare alcun soggetto esterno.

Indicazione e descrizione delle procedure adottate:

L'esatta identificazione e le funzioni attribuite alle figure esterne per effetto di conferimento di incarichi in outsourcing sono state specificate nel contesto dei singoli atti di nomina oppure sono state oggetto di definizione nella sede del rapporto contrattuale che lega il titolare del trattamento al soggetto esterno.

Tali funzioni possono inoltre costituire una integrazione a quanto specificato nella documentazione adottata ai sensi delle prescrizioni di legge, tra cui si evidenziano:

- *eventuali atti di designazione del soggetto esterno quale responsabile del trattamento dati ex art. 29 d.lgs. 196/2003;*

- *incarico al trattamento dati nei confronti del soggetto con designazione dell'ambito di trattamento consentito in ragione della funzione attribuita.*

- *individuazione degli addetti alla gestione e alla manutenzione del sistema informatico.*

Per l'esatta rappresentazione delle funzioni e degli ambiti di operatività assegnati a tali soggetti si rinvia alla documentazione agli atti, che compone parte integrante del presente documento.
In ogni caso, il soggetto esterno sarà tenuto a conformarsi (ed eventualmente ad impostare autonomamente sulla propria struttura informatica quanto all'uopo necessario) al sistema di registrazione degli accessi sui sistemi di elaborazione e sugli archivi elettronici in modo tale da consentire e permettere l'esercizio di un corretto controllo sulle operazioni svolte.

Tali registrazioni devono avere caratteristica di completezza, inalterabilità e possibilità di verifica della loro integrità. Devono inoltre comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e essere conservate per un periodo non inferire a sei mesi.

E' compito del soggetto esterno riferire al titolare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Il titolare a sua volta comunica che le operazioni poste in essere da parte degli amministratori di sistema potranno essere monitorate mediante loro registrazione su supporti cartacei e registrazione dei file di log.

Tali dati saranno custoditi per il termine di sei mesi in modo protetto e sicuro. Le registrazioni avranno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità.

4) RAPPORTO CON LA SOCIETA' INFORMATICA TRENTINA SPA: INDICAZIONE DEGLI ESTREMI IDENTIFICATIVI DEI SOGGETTI NOMINATI AMMINISTRATORI DI SISTEMA.

L'Istituto Comprensivo, tenuto conto degli obblighi stabiliti dal Garante Privacy in materia di amministratore di sistema e preso atto di quanto indicato nella comunicazione di data 03 dicembre 2009 a firma del Dirigente del Servizio per lo sviluppo e l'innovazione del sistema Scolastico e formativo della Provincia Autonoma di Trento, dott. Paolo Rella, (protocollo numero: 8437/09/S148/DC) ha individuato i tecnici preposti da parte di Informatica Trentina S.p.a. quali incaricati addetti alle operazioni di gestione o manutenzione del sistema informatico.

Alla luce di tale particolare assetto ha formalmente invitato la società Informatica Trentina S.p.a. a riferire quanto prima l'elenco degli Amministratori di sistema da quest'ultima individuati con precisa indicazione degli ambiti di operatività consentiti a ciascun preposto.

Sarà compito della società Informatica Trentina S.p.a. comunicare al titolare gli eventuali aggiornamenti e gli estremi identificativi delle persone in futuro preposte quali amministratori di sistema.

Per l'esatta rappresentazione delle funzioni e degli ambiti di operatività, nonché per conoscere il nominativo di ciascun preposto alla funzione si rinvia alla documentazione agli atti.

5) VERIFICA DELL'ATTIVITA'

descrizione delle misure volte a garantire il controllo annuale sull'operato degli amministratori di sistema in modo da controllare la rispondenza con le misure organizzative, tecniche e di sicurezza.

Entro il 31 DICEMBRE di ogni anno, ciascun amministratore di sistema dovrà redigere una relazione da cui risulti la rispondenza o meno alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti. Nel caso si siano verificate delle anomalie, queste dovranno essere immediatamente segnalate al titolare del trattamento.

ALLEGATO A - Schema di clausole contrattuali

La società/consulente/cooperativa/altro…….
alla quale viene affidato lo svolgimento del servizio di……..
per l'espletamento del quale ha necessità di trattare i seguenti dati ……

- riconosce che i dati che tratterà nell'espletamento dell'incarico ricevuto sono dati personali e, come tali, sono soggetti all'applicazione del Codice in materia di protezione dei dati personali (decreto legislativo 196/03).

Si impegna a:

- Ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali rispettando le disposizioni previste.
- Agire in modo lecito e secondo correttezza verificando che i dati trattati siano esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali vengono raccolti e successivamente trattati.
- Adottare, verificare e rispettare le misure di sicurezza minime nonché idonee come prescritto dal titolo V della parte I del Codice in materia di protezione dei dati personali e dall'allegato disciplinare tecnico in materia di misure minime di sicurezza (allegato B).
- Verificare il costante funzionamento ed aggiornamento delle misure di sicurezza già esistenti e quelle che verranno successivamente adottate.
- Provvedere alla nomina degli incaricati del trattamento dati come previsto dall'Art. 30 del Codice in materia di protezione dei dati personali vigilando su di essi affinché siano osservate le disposizioni e le istruzioni impartite.
- Comunicare al Titolare del trattamento qualsiasi disfunzione che possa in qualche modo compromettere la sicurezza dei dati.
- Fornire informazioni in caso di richiesta da parte degli interessati, come previsto dalla parte I, titolo II (Diritti dell'interessato) del Codice in materia di protezione dei dati personali.
- Attenersi alle altre ulteriori istruzioni che possono essere inserite nel contratto stipulato con l'Ente o successivamente impartite.
- Annualmente e comunque entro il 31 dicembre di ogni anno il soggetto esterno deve provvedere a elaborare ed inviare al Titolare una relazione sulle misure di sicurezza adottate.

Il Titolare del trattamento si riserva la possibilità di effettuare verifiche sui trattamenti svolti per conto proprio dal soggetto esterno.

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

ALLEGATO B - Check list di controllo sui soggetti esterni

SOGGETTO ESTERNO:	DATA:
MISURA DI SICUREZZA	MODALITA'
TRATTAMENTI AUTOMATIZZATI	
Individuazione degli incaricati e istruzioni agli stessi	Indicare i soggetti incaricati (es: amministrativi ufficio paghe):
Credenziali di autenticazione	Tipologia di credenziali adottate . ❑Codice per l'identificazione dell'interessato (nome utente) + password (composta da almeno 8 caratteri, modificata dall'incaricato al primo utilizzo ed ogni 3/6 mesi) ❑Dispositivo di autenticazione (smart card) + eventuale password o C.I.P ❑Caratteristica biometrica (impronta digitale) + eventuale password o C.I.P.
Salvataggio dei dati	Modalità e frequenza:
Antivirus	Modalità e frequenza dell'aggiornamento:
Aggiornamento dei programmi volti alla sicurezza	Modalità e frequenza degli aggiornamenti:
Idonei strumenti contro l'accesso abusivo	Tipologia di strumento installato:
Documento programmatico sulla sicurezza	Allegare copia del documento programmatico
Adozione di idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento	Indicare le misure adottate:

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (CARTACEO***)***	
Individuazione degli incaricati e istruzioni agli stessi	Indicare i soggetti incaricati (es: amministrativi ufficio paghe):
Controllo degli accessi agli archivi/ autorizzazione all'accesso agli archivi	Modalità del controllo: Soggetti autorizzati:
Identificazione e registrazione delle persone ammesse agli archivi dopo l'orario di chiusura	Modalità dell' identificazione e registrazione:

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

ALLEGATO C - Verbale di controllo informatico sulle misure di sicurezza

MISURE DI SICUREZZA/STRUMENTO INFORMATICO	DESCRIZIONE	NOTE
Credenziali di autenticazione	☐ Password + codice identificativo personale ☐ Dispositivo di autenticazione ☐ Caratteristica biometrica	☐ Non si rilevano problemi ☐Si rilevano problemi dovuti a: -_____ -_____ -_____ _____ Consigli: _____ _____ _____ _____
Profili di autorizzazione	Assegnati a n…….incaricati	☐ Non si rilevano problemi ☐Si rilevano problemi dovuti a: -_____ -_____ -_____ _____ Consigli: _____ _____ _____ _____
antivirus	Modalità: ☐Automatica ☐Manuale Ultima data aggiornamento:_____	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ _____ Consigli: _____ _____ _____ _____
Aggiornamenti periodici dei programmi (patch)	Programma……. Aggiornato il…… Programma ……. Aggiornato il…… Programma ……. Aggiornato il……	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____

		-_____ -_____ _____ Consigli: _____ _____ _____ _____
backup	Modalità ☐Automatica ☐Manuale Data inizio utilizzo supporto: _____	☐Prova di lettura di un supporto ☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ _____ _____ _____ _____ Consigli:

gruppo di continuita'	☐Sui PC ☐Sul server	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ Consigli: _____ _____ _____
raid	Tipologia: ☐Hardware ☐Software ☐Raid 1 ☐Raid 5 ☐Altro	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ -_____ Consigli: _____ _____ _____
modem	Sconnessione: ☐Automatica ☐Manuale	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ Consigli: _____ _____ _____ _____

router	Sconnessione: ☐Automatica ☐Manuale	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ -_____ -_____ -_____ Consigli: _____ _____ _____
proxy		☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ Consigli: _____ _____ _____
firewall	☐Hardware ☐Software	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ Consigli: _____ _____ _____ _____ _____
accesso remoto alla rete	Modalità: ☐Linea diretta ☐Internet ☐Autenticazione PWD e ID ☐Controllo numero chiamante	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____

	☐Richiamata	-_____ _____ Consigli: _____ _____ _____ _____
Trattamento disgiunto dei dati sensibili da altri dati	Modalità: crittografia codifica disabilitazione del campo in base al profilo	☐ Non si rilevano problemi di funzionamento ☐Si rilevano problemi di funzionamento dovuti a: -_____ -_____ -_____ Consigli: _____ _____ _____ _____
altro (indicare)		

Data del controllo

_____

Firma

_____

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

ALLEGATO D

Guida formativa degli incaricati del trattamento

Introduzione: il Codice in materia di protezione dei dati personali

Definizioni

Regole generali

Regole ulteriori per i soggetti pubblici

Trattamento di dati in ambito sanitario

Rischi che incombono sui dati e misure di sicurezza

Responsabilità e sanzioni

Modalità per aggiornarsi sulle misure minime di sicurezza adottate

INTRODUZIONE: IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

La tutela della riservatezza, il diritto del cittadino a non subire invasioni nella propria sfera privata sono ormai entrati a far parte della nostra vita quotidiana. Siamo però immersi in una società che non può astenersi dal trattare dati personali, soprattutto al fine di fornire beni o servizi al cittadino. Le informazioni vengono raccolte, elaborate, comunicate ad altri soggetti, anche tramite reti di comunicazione elettronica. Si è quindi ravvisata la necessità di tutelare sia l'identità personale che i dati personali. Il Codice in materia di protezione dei dati personali (decreto legislativo 196/03), in vigore dal 1° gennaio 2004, rappresentando una raccolta organica e sistematica delle norme sulla privacy, è finalizzato proprio a disciplinare un settore delicato come la tutela dei diritti, delle libertà fondamentali, della dignità della persona e la protezione dei dati personali, definendo regole generali e specifiche al fine di un corretto e trasparente trattamento dei dati raccolti.

Concetto fondamentale del Codice è quindi il diritto alla protezione dei dati personali. Questo diritto viene tutelato sia con misure di tipo preventivo quali ad esempio l'informativa all'interessato o le misure di sicurezza, sia di tipo successivo quali ad esempio il controllo che può esercitare l'interessato sui propri dati o le sanzioni previste.

Il presente opuscolo mira ad informare gli incaricati sulle disposizioni previste e sui rischi che può comportare il trattamento di dati personali.

DEFINIZIONI

Il Codice in materia di protezione dei dati personali utilizza termini di cui è necessario conoscere il significato. Al fine di rendere più agevole l'utilizzazione della presente guida formativa e comprensibili le espressioni verbali utilizzate, in questa sezione si riportano i principali termini di cui si avvale il Codice.

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

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

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

Dati sensibili : i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

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

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

Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

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

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

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

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

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

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

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

Garante: l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675. (organo collegiale operante in piena autonomia e con indipendenza di giudizio e valutazione istituito al fine di assicurare la tutela dei diritti e delle libertà fondamentali nonché il rispetto della dignità dell'interessato nel trattamento di dati personali. Fra gli altri, ha il compito di controllare la conformità dei trattamenti, esaminare segnalazioni, reclami, ricorsi, adottare i provvedimenti previsti dalla normativa, promuovere la conoscenza del Codice. Ha inoltre poteri inibitori, sanzionatori e cautelari.)

REGOLE GENERALI

Il codice dispone regole generali finalizzate ad un corretto trattamento dei dati personali. In questa sezione vengono evidenziate le principali regole generali, valide per tutti i trattamenti e alcune indicazioni operative per conformare il trattamento alla normativa.

A) PRINCIPI GENERALI.

L'art. 11 specifica le regole generali alle quali devono essere adeguati tutti i trattamenti di dati. Secondo tali principi ogni trattamento deve essere lecito e corretto; la nozione di liceità comporta ontologicamente che il trattamento debba essere eseguito sia nel rispetto delle disposizioni specifiche di legge previste dalla normativa a carattere speciale sia nel rispetto dei principi generali del diritto; la correttezza si riferisce a regole di condotta non giuridiche da applicarsi al trattamento di dati personali. Inoltre i dati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi; questo significa che, prima dell'inizio del trattamento, si devono determinare le finalità per le quali i dati vengono raccolti e trattati, limitando la raccolta delle informazioni a quei dati che siano strumentali e funzionali allo scopo del trattamento, informandone l'interessato il quale potrà esercitare i propri diritti sui propri dati personali; i dati raccolti dovranno quindi essere esatti e, se necessario, aggiornati nonché pertinenti, completi e non eccedenti; risulta quindi necessario procedere ad un iniziale controllo in fase di raccolta dei dati al fine di evitare di raccogliere dati non necessari allo scopo del trattamento pur nella loro completezza al fine di avere un quadro completo dell'interessato in relazione al trattamento effettuato, seguito da periodiche verifiche al fine di aggiornare, se necessario, i dati.

Infine i dati devono essere conservati per un periodo non superiore a quello necessario allo scopo per il quale sono stati raccolti. E' quindi necessario valutare se e per quanto tempo la normativa di riferimento preveda la conservazione dei dati, tenendo presente la normativa contabile e fiscale, nonché la conservazione della documentazione per fini storici, statistici o scientifici, con particolare attenzione alla normativa archivistica.

B) INFORMATIVA DELL'INTERESSATO.

L'articolo 13 del Codice prevede altresì che l'interessato sia informato in merito all' identità del soggetto che ha intenzione di trattare i dati personali dell'interessato stesso e in merito all'utilizzo che ne verrà fatto. Scopo di questo adempimento è consentire all'interessato di poter " seguire " le informazioni a lui riferite ed eventualmente esercitare i diritti conferitigli dal Codice.

In particolare la normativa prevede che l'interessato o la persona presso cui sono raccolti i dati debba essere previamente informato oralmente o per iscritto circa:

- Finalità e modalità del trattamento cui sono destinati i dati;
- La natura obbligatoria o facoltativa del conferimento dei dati;
- Le conseguenze di un eventuale rifiuto di rispondere;
- I soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati;
- L'ambito di diffusione dei dati
- Gli estremi identificativi del titolare e del responsabile

Nel caso in cui, poi, i dati siano di tipo sensibile o giudiziario, deve essere inserito il riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento di tali dati.

Se i dati non sono raccolti direttamente presso l'interessato ma sono raccolti presso terzi, l'informativa all'interessato può essere data all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione. In questo caso devono essere comprese nell'informativa le categorie di dati trattati.
Questa disposizione non si applica se i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria, se i dati sono trattati ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria oppure su concessione del Garante.

C) ADEMPIMENTI PER GLI INCARICATI.
Per una corretta applicazione di queste norme è necessario che gli incaricati, al momento della raccolta dei dati, provvedano a tali adempimenti:

- fornire l'informativa relativa al trattamento dei dati così come predisposta dal titolare del trattamento eventualmente integrandola nelle parti di competenza;
- verificare l'esattezza, la pertinenza e la completezza dei dati trattati;
- non raccogliere più dati del necessario;
- rispettare l'obbligo di riservatezza e segretezza in relazione ai dati di cui si viene a conoscenza;
- far rispettare la " distanza di cortesia " nei rapporti di tipo front-office al fine di garantire la riservatezza e la discrezione nel trattamento e nella comunicazione dei dati.

D) DIRITTI DEGLI INTERESSATI.

L'articolo 7 del Codice conferisce all'interessato il diritto di accesso ai propri dati personali e altri diritti.

In particolare l'interessato ha diritto di:

1. Ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. Ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati

3. Ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. Opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Questi diritti possono essere esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato; alla richiesta è fornito idoneo riscontro senza ritardo.

La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Quando riguarda l'esercizio dei diritti previsti al punto 1 e 2 dell'elenco precedente, la richiesta può essere formulata anche oralmente e in tal caso deve essere annotata sinteticamente a cura dell'incaricato o del responsabile.

Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

Nel caso in cui sia effettuata una richiesta in tal senso, il responsabile o gli incaricati devono estrarre i dati e comunicarli al richiedente. I dati possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare.

Al fine di agevolare questi diritti viene predisposta una modulistica che sarà fornita allegata alla presente guida formativa.

REGOLE ULTERIORI PER I SOGGETTI PUBBLICI

Il codice prevede delle disposizioni specifiche alle quali devono attenersi i soggetti pubblici nel trattare dati personali. In questa sezione vengono evidenziate le principali regole specifiche per il settore pubblico, valide per tutti i trattamenti e alcune indicazioni operative per conformare il trattamento alla normativa.

A) REGOLE PER IL TRATTAMENTO DI DATI COMUNI DA PARTE DI SOGGETTI PUBBLICI

Il trattamento dei dati personali da parte di soggetti pubblici è consentito soltanto al fine dello svolgimento delle funzioni istituzionali, osservando i presupposti e i limiti stabiliti dal Codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.
Inoltre è espressamente previsto che i soggetti pubblici **siano esonerati dal richiedere il consenso dell'interessato.**

Per quanto riguarda i dati diversi da quelli sensibili o giudiziari, che per semplificare vengono convenzionalmente definiti "comuni**", in base all'art. 19, i soggetti pubblici possono legittimamente procedere al trattamento anche se non è espressamente previsto da leggi o regolamenti.**
Diverse invece sono le disposizioni in tema di comunicazione **di dati. Infatti, se la comunicazione avviene nei confronti di un altro soggetto pubblico, essa è ammessa solo quando è prevista da una norma di legge o regolamento. In subordine la comunicazione è ammessa anche in mancanza di norma di legge o regolamento, ma quando questa sia comunque necessaria per lo svolgimento di funzioni istituzionali. In tal caso la legge obbliga ad una preventiva comunicazione di tale attività al Garante.**

Se la comunicazione avviene invece nei confronti di soggetti privati o enti pubblici economici, essa è ammessa unicamente se prevista da norma di legge o regolamento.

Anche la diffusione **dei dati è ammessa** solamente se prevista da norma di legge o regolamento.

B) ADEMPIMENTI PER GLI INCARICATI

Per osservare tale norma è necessario che gli incaricati provvedano ai seguenti adempimenti:

- verificare se i trattamenti eseguiti sono svolti per le finalità istituzionali dell'Ente

- verificare, ogni volta che ci si ritrova nella necessità di dover comunicare dati all'esterno dell'Ente, le disposizioni di legge che consentono tali operazioni.

C) REGOLE PER IL TRATTAMENTO DI DATI SENSIBILI DA PARTE DI SOGGETTI PUBBLICI

Per quanto riguarda i **dati sensibili** invece, il soggetto pubblico può procedere al trattamento solo se autorizzato da **espressa** disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, il tipo di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Nel caso in cui non sia presente una tale disposizione di legge il codice prevede che il Garante, su richiesta, possa procedere all'individuazione delle attività che perseguono finalità di rilevante interesse pubblico, autorizzando così, con proprio provvedimento, il trattamento.
A seguito del provvedimento del Garante o nel caso in cui la legge, individuate le finalità di rilevante interesse pubblico, non proceda a determinare i tipi di dati e le operazioni eseguibili, dovrà essere il soggetto pubblico stesso ad individuare tali elementi. Tale individuazione dovrà essere fatta con atto di natura regolamentare, adottato in conformità al parere espresso dal Garante.

D) REGOLE PER IL TRATTAMENTO DI DATI GIUDIZIARI DA PARTE DI SOGGETTI PUBBLICI

Similarmente, anche per i dati giudiziari, il trattamento è consentito unicamente se autorizzato da espressa disposizione di legge o autorizzazione del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.
Anche in questo caso, se non vengono determinati i tipi di dati e le operazioni eseguibili, si applica quanto indicato in merito al regolamento per i dati sensibili.

E) ADEMPIMENTI PER GLI INCARICATI
Il codice prevede ulteriori principi che si applicano ai trattamento di **dati sensibili o giudiziari.** In relazione a tali tipologie di dati devono essere quindi messe in atto le seguenti procedure:

- conformare il trattamento secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato;

- devono esser trattati solo i dati 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;
- i dati dovranno essere, di regola, raccolti presso l'interessato;
- periodicamente dovranno essere verificate l'esattezza, l'aggiornamento, la pertinenza, la completezza, la non eccedenza e l'indispensabilità dei dati rispetto alle finalità perseguite nei singoli casi. I dati che, a seguito delle verifiche risultano eccedenti, 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;
- particolare attenzione si deve porre al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale. Tali dati devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo;
- i dati idonei a rivelare lo stato di salute non posso essere **diffusi**.

.**RISCHI CHE INCOMBONO SUI DATI E MISURE DI SICUREZZA**

Il codice prevede l'adozione di misure di sicurezza idonee e preventive in modo tale da ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, tenendo conto del progresso tecnico, della natura dei dati trattati e delle specificità dei trattamenti.

Il titolare del trattamento deve quindi, anche attraverso la collaborazione del responsabile, se nominato, e degli incaricati provvedere a mettere in atto tutte le misure di sicurezza a protezione dei dati personali trattati.

In particolare il codice individua alcune misure di sicurezza, definite " minime ", volte ad assicurare un livello minimo di protezione dei dati personali.

In questa sezione vengono evidenziati i principali rischi che possono incombere sui dati e le misure di sicurezza adottate a disposizione degli incaricati. La puntuale applicazione e il corretto utilizzo di tali misure da parte degli incaricati sono condizione essenziale per una sicurezza dei dati. Le misure di sicurezza esposte in questa sezione nonché ulteriori misure di sicurezza che non sono nella disponibilità degli incaricati in quanto automatiche, adottate o da adottarsi sono descritte in dettaglio nel documento programmatico sulla sicurezza, a disposizione di chiunque ne faccia richiesta al titolare o al responsabile del trattamento.

TRATTAMENTI CON STRUMENTI ELETTRONICI

Protezione dei dati da accessi non consentiti o trattamenti non autorizzati:

Ogni utente del sistema informatico è dotato di **credenziali di autenticazione** consistenti in un **codice per l'identificazione dell'incaricato** (nome utente) e una **password** oppure in un **dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato** oppure in una **caratteristica biometrica dell'incaricato, eventualmente associati ad un codice identificativo o ad una password,** in modo tale che solo gli incaricati dotati di tali credenziali di autenticazione possano accedere a uno specifico trattamento o insieme di trattamenti attraverso il superamento di un'idonea procedura di identificazione. Questa misura di sicurezza protegge i dati da accessi non autorizzati. E' obbligatorio che la password che compone le credenziali di autenticazione sia mantenuta segreta dalla persona a cui è assegnata. Infatti una divulgazione a terzi di tale password comprometterebbe la sicurezza dei dati permettendo un accesso abusivo ad essi da parte di persone non autorizzate.
Altre misure di sicurezza riguardano l'obbligo di modifica della password da parte dell'utente del sistema informatico al primo utilizzo e successivamente ogni tre mesi(nel caso di trattamento di dati sensibili o giudiziari) o sei mesi in caso di trattamento di dati comuni, la lunghezza della password e il divieto di utilizzare riferimenti agevolmente riconducibili all'incaricato. Tale obbligo ha la funzione di proteggere sia i dati personali trattati (un soggetto estraneo che si introduca nel sistema potrebbe modificare o cancellare i dati contenuti), sia l'incaricato stesso che utilizza la password (in caso di accesso ai dati tramite la password dell'utente, il sistema registra l'accesso attribuendolo all'utente stesso). L'associazione di una password non facilmente riconducibile all'incaricato (ad esempio è vietato indicare il proprio nome o cognome, quello dei familiari o la data di nascita e tantomeno utilizzare il nome utente), unita ad una lunghezza adeguata e il suo cambiamento in tempi ragionevolmente brevi permette di contrastare accessi abusivi al sistema informatico o eventuali tentativi di scoprire o sottrarre, anche con modalità informatiche, la password utilizzata.
Nel caso in cui, ora o in futuro, siano utilizzati come credenziali di autenticazione al posto di codice identificativo (nome utente) e password, dispositivi di autenticazione (ad esempio smart card) eventualmente associate ad una password, fermo restando quanto già indicato per la password, è necessario che la persone in possesso di tali dispositivi di autenticazione si preoccupino di conservarli con cura, non cedendoli a terzi né lasciandoli a disposizione di

terzi. (ad esempio non lasciare questi dispositivi a disposizione di chiunque sulla scrivania o posto di lavoro).

La collaborazione degli utenti del sistema informatico è richiesta anche in relazione alla custodia degli strumenti elettronici. In particolare è misura minima di sicurezza provvedere a non permettere che terzi non autorizzati utilizzino gli strumenti informatici in assenza dell'incaricato. A tal fine è obbligatorio che al termine dell'orario lavorativo il PC in dotazione venga spento. E' inoltre previsto che, in caso di assenza temporanea dalla propria postazione (ad esempio nelle pause pranzo, o in caso di allontanamento in genere) si provveda a bloccare la possibilità di utilizzo. A tal fine sono possibili varie soluzioni quali spegnere il PC o chiudere la porta a chiave.

La soluzione più immediata e facilmente adottabile rimane comunque quella di bloccare il PC. (ctrl + alt + canc – blocca computer). In tal modo solo inserendo la password di accesso sarà possibile accedere ai dati ripartendo esattamente dal punto lasciato in sospeso. Altra soluzione possibile è attivare la procedura di screen saver con password: in caso di non utilizzo del sistema, a cadenza prestabilita, si attiverà lo screen saver obbligando l'utente all'inserimento della password.

E' possibile che talora sia necessario accedere ai dati in assenza dell'incaricato. Questo può avvenire in caso di manutenzione del sistema, di sicurezza o di continuità operativa. Se tali operazioni di accesso ai dati o agli strumenti possono avvenire solo con l'utilizzo della password dell'incaricato, è necessario che ogni incaricato, al primo utilizzo della password e successivamente ad ogni cambio, comunichi la sua password in busta chiusa al custode delle password il cui nome sarà comunicato da parte del titolare stesso. Tale comunicazione è necessaria solo nel caso in cui sia necessario conoscere, da parte del titolare e nei casi indicati, la password dell'incaricato. Nel caso in cui il titolare del trattamento possa comunque accedere ai dati senza conoscere tale password (ad esempio tramite la password di amministratore di sistema o resettando la password dell'incaricato o qualora agli stessi dati accedano più persone, evitando quindi la paralisi lavorativa in caso di assenza dell'incaricato) tale procedura non è necessaria.

Protezione dei dati da attacchi di virus o programmi intrusivi

Il titolare del trattamento ha provveduto a installare programmi antivirus e anti programmi pericolosi e ad aggiornarli periodicamente.

E' comunque necessaria anche in questo caso la collaborazione degli incaricati e in particolare:

Se l'aggiornamento dell'antivirus non è previsto in modalità automatica ma è necessario effettuarlo manualmente a cura di ogni singolo incaricato, tale aggiornamento deve avvenire almeno una volta in settimana.

La maggior parte dei virus vengono diffusi tramite la posta elettronica e Internet; di conseguenza è necessario attenersi alle seguenti ulteriori istruzioni:

- non aprire e- mail che contengano un'estensione doppia;
- prima di aprire una e – mail, in particolare se non richiesta o nel caso in cui si ritenga quantomeno insolita, verificare il mittente ed eventualmente non aprire allegati o collegarsi a siti internet contenuti nel testo della e – mail;
- prima di utilizzare floppy o CD di qualsiasi provenienza, procedere con un controllo da parte dell'antivirus;

Protezione dei dati da distruzione o perdita, anche accidentale

Il titolare del trattamento ha provveduto a installare un sistema di salvataggio centralizzato e automatico dei dati. Il salvataggio viene eseguito a cadenza stabilita e comunque non superiore a sette giorni, da personale appositamente incaricato.

Gli incaricati dovranno però anche in questo caso concorrere e mettere in atto tutte le procedure affinché la misura di sicurezza non risulti inefficace a causa di attività non corrette.

In particolare è necessario che gli incaricati provvedano a salvare tutti i dati sul server evitando di mantenerli in locale sui singoli PC.

E' talora comunque possibile che, a causa del sistema informatico utilizzato o dei programmi installati, i dati siano elaborati in locale sul singolo PC. In tal caso è necessario segnalare la situazione all'amministratore di sistema o al responsabile del trattamento o al titolare il quale provvederà ad attuare le procedure automatiche o manuali al fine di inviare periodicamente i dati sul server in modo tale da procedere al loro salvataggio automatico. Nel caso in cui non sia possibile prevedere l'invio degli archivi sul server, sarà cura dei singoli incaricati provvedere al salvataggio di tali dati. Di regola comunque è opportuno che il salvataggio non avvenga tramite floppy ma tramite masterizzazione su CD. Tale salvataggio dovrà essere eseguito con cadenza almeno settimanale. Naturalmente i supporti sui quali saranno eseguiti i salvataggi dovranno essere conservati in modo appropriato. E' necessario quindi che siano conservati in contenitori chiusi a chiave e protetti (armadi, cassetti,ecc.) o consegnati al soggetto preposto al back up centralizzato.

Protezione dei dati contenuti nei supporti rimovibili

Anche l'utilizzo di supporti rimovibili (floppy, CD, cassette, ecc…) deve essere conforme alle norme di sicurezza previste. In particolare, nel caso tali supporti siano riutilizzati, anche da altri incaricati, e in essi siano contenuti dati sensibili o giudiziari, primo del loro riutilizzo, devono esser cancellate tutte le informazioni contenute, in modo tale da non consentire in alcun modo la conoscenza da parte di terzi di tali dati. Si raccomanda quindi:

nel caso in cui sia necessario conservare i supporti informatici contenenti dati sensibili o giudiziari, la conservazione deve avvenire in contenitori chiusi a chiave.

Nel caso in cui i supporti informatici siano riutilizzati, anche da altri incaricati, deve essere eseguita la formattazione totale del supporto.

Nel caso in cui, per motivi tecnici, non possa essere eseguita la formattazione, il supporto deve essere distrutto.

Nonostante questa misura minima sia riferita ai dati sensibili o giudiziari, è buona norma applicare questa procedura a tutti i supporti utilizzati, indipendentemente dal tipo di dato registrato.

Attenzione al trattamento dei dati dovrà avvenire anche in caso di utilizzo di altri strumenti per i quali sono disposte queste ulteriori istruzioni:

Fax.:

Verificare la correttezza del numero telefonico relativo al fax dell'utente e porre attenzione alla digitazione del numero telefonico;

provvedere a stampare sul retro del fax inviato il report di stampa verificando l'esattezza delle pagine inviate e la correttezza dell'invio;

Nel caso in cui siano inviati documenti contenenti dati sensibili o giudiziari provvedere, se possibile, a inviare il documento in due fasi, dividendo il dato identificativo dagli altri dati o, in alternativa, chiamando il destinatario per informarlo dell'arrivo del fax in modo tale che quest'ultimo possa provvedere alla tempestiva raccolta del documento stesso ed eventualmente comunicare al mittente eventuali errori di trasmissione o leggibilità del documento ricevuto.

Fotocopiatrici:

non dimenticare sotto il coperchio della fotocopiatrice il documento da duplicare;

nel caso in cui il documento contenga dati sensibili o giudiziari provvedere personalmente all'effettuazione della fotocopia e non consegnarlo ad altri soggetti per l'esecuzione del compito.

Scanner:

verificare la correttezza dell'esecuzione, la leggibilità del documento od eventuali errori di acquisizione del testo.

TRATTAMENTI CON STRUMENTI NON ELETTRONICI

Protezione dei dati dal rischio di accessi non consentiti agli atti e ai documenti cartacei

Anche gli atti e i documenti cartacei contenenti dati personali devono essere sottoposti a misure di sicurezza.
In particolare è necessario che tutti i documenti siano conservati negli apposti armadi, cassettiere, raccoglitori o archivi in genere. E' necessario inoltre che al termine dell'orario lavorativo le scrivanie siano prive di documenti, fascicoli, faldoni contenenti dati personali. Ogni incaricato è responsabile della protezione fisica dei documenti a lui affidati. Particolare attenzione dovrà essere destinata a eventuali stampe dei tabulati prodotti dall'esecuzione di programmi informatici. Le stampe dovranno quindi essere immediatamente raccolte e conservate da parte di chi ha eseguito i comandi di stampa, in particolare se la stampante è condivisa con altri uffici/servizi ed è situata in altri locali. Le stesse procedure dovranno essere attuate per l'utilizzo di fax o fotocopiatrici.
Ulteriore attenzione dovrà essere rivolta alla distruzione dei documenti, ad esempio strappando i documenti prima di cestinarli, o utilizzando i tritadocumenti in particolar modo per atti contenenti dati sensibili o giudiziari o particolarmente riservati.
Ulteriore attenzione dovrà essere rivolta ai documenti contenenti dati sensibili o giudiziari con particolare attenzione alla documentazione sanitaria contenuta nelle schede sanitarie e/o nei piani di assistenza individualizzati quando vengono consultati per l'assistenza giornaliera agli ospiti. A tal fine è necessario che tali documenti, quando sono al di fuori dei loro archivi durante l'utilizzo quotidiano, siano tenuti sotto il controllo e la custodia degli incaricati, mentre al termine dell'impiego quotidiano, devono essere riposti in armadi, cassetti, archivi o contenitori chiusi a chiave. Non devono assolutamente essere lasciati sulle scrivanie o postazioni di lavoro a disposizione di chiunque entri nell'ufficio/locale/reparto. In caso di ingresso nel locale/ufficio/reparto di persone estranee è buona norma fare in modo di impedire l'accesso a tali documenti, ad esempio conservandoli temporaneamente in un cassetto o in una teca, sempre comunque sotto il controllo dell'incaricato.
Si ricorda inoltre di provvedere alla separazione dei dati idonei a rivelare stato di salute e vita sessuale da altri dati non necessari alle finalità del trattamento. Ad esempio, i certificati medici possono essere mantenuti nel faldone contenente la documentazione dell'interessato, ma separandoli dagli altri documenti, ad esempio utilizzando una busta chiusa.

UTILIZZO DI ALTRI STRUMENTI

E' possibile che, per il trattamento di dati personali, vengano utilizzati anche altri strumenti quali ad esempio telecamere, macchine fotografiche, cellulari con integrata fotocamere, ecc….

Anche per l'utilizzo di tali strumenti è necessario attuare misure di sicurezza.

In particolare il rischio più probabile è quello di perdere o dimenticare nei luoghi visitati lo strumento.

E' quindi opportuno, se lo strumento è predisposto, inserire un PIN per proteggere i dati inseriti. Tale PIN può essere condiviso con altre persone autorizzate a tali trattamenti o consegnato al custode delle password o al titolare.

Una volta effettuate le foto o le riprese, le stesse dovranno essere riversate sul sistema informatico se si utilizzano modelli elettronici e dovranno essere cancellate le immagini dalla memoria dello strumento. Se invece vengono utilizzati modelli non elettronici, le foto sviluppate o le videocassette devono essere conservate con le stesse modalità indicate nella sezione dedicata ai trattamenti con strumenti cartacei.

VIDEOSORVEGLIANZA

In caso di installazione di sistemi di videosorveglianza, gli addetti alla visione delle immagini, nonché alla loro registrazione, se prevista, dovranno utilizzare tali strumenti unicamente per le funzioni di controllo degli accessi e/o delle zone in cui il titolare ha rilevato vi siano rischi specifici e di conseguenza installato le telecamere. Non potrà essere concessa la visone delle immagini a persone non autorizzate. I monitor dovranno esser spenti o dovranno essere attivate le chiusure dei locali ove sono posti, quando gli incaricati non sono presenti. Nel caso in cui sia predisposto un sistema di registrazione delle immagini, eventuali supporti audiovisivi rimovibili (come ad esempio le cassette VHS), dovranno essere custoditi in contenitore chiuso a chiave (armadio, cassetto) e i dati dovranno essere cancellati dopo al massimo 24 ore (fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.). Nel caso in cui le immagini siano registrate su supporto informatico si provvederà, ove possibile, alla cancellazione automatica delle immagini entro tale termine. Se ciò non fosse possibile, saranno date specifiche istruzioni agli incaricati in merito alle modalità di cancellazione.

RESPONSABILITA' E SANZIONI

Il codice della Privacy prevede sanzioni amministrative e penali, oltre al risarcimento del danno ai fini civilistici.

In questa sezione saranno indicate le principali sanzioni previste dal Codice le quali coinvolgono, oltre il titolare e il responsabile, anche gli incaricati

OMESSA O INIDONEA INFORMATIVA ALL'INTERESSATO (art. 161)

La violazione dell'obbligo di fornire un'idonea informativa sul trattamento dei dati comuni comporta una sanzione amministrativa da tremila a diciottomila euro. Nel caso di dati trattamenti di sensibili o giudiziari la sanzione può essere aumentata fino a trentamila euro con un minimo di cinquemila euro.

OMESSA ADOZIONE DI MISURE MINIME DI SICUREZZA (art. 169)

La mancata adozione delle misure minime di sicurezza è sanzionata penalmente con l'arresto sino a due anni o con l'ammenda da diecimila a cinquantamila euro. E' previsto il cosiddetto " ravvedimento operoso". All'autore del reato, all'atto dell'accertamento, è impartita una prescrizione e fissato un termine per la regolarizzazione. L'adempimento della prescrizione e il pagamento di una somma pari a un quarto del massimo dell'ammenda stabilita per la contravvenzione, estinguono il reato.

All'adozione delle misure minime di sicurezza è tenuto il titolare. Tuttavia, il disciplinare tecnico nel quale sono previsti i modi di adozione di tali misure, prevede che le modalità tecniche siano adottate a cura del titolare, del responsabile e dell'incaricato. La responsabilità quindi di mantenere in attuazione le misure di sicurezza adottate dal titolare e a disposizione degli incaricati ricade anche su questi ultimi.

TRATTAMENTO ILLECITO DI DATI (art. 167)

" Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni."

Come si evince dall'articolo la responsabilità del fatto illecito è ascritta a **" chiunque ",** ciò significa che si dovrà, in caso di trattamento illecito, verificare il soggetto che lo ha commesso, non esentando dalla sanzione né il titolare, né il responsabile ma nemmeno l'incaricato.

Il codice prevede inoltre responsabilità civile per il risarcimento del danno.

L'articolo 15 prevede che " chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11."
Questo significa che innanzitutto si viene ritenuti responsabili del danno se non si riesce a dimostrare di aver adottato ogni possibile misura idonea ad evitare il danno stesso. Inoltre, poiché l'articolo 11 (vedi sezione regole generali) è uno degli articoli più significativi del Codice in merito alla correttezza del trattamento, viene prevista la possibilità di richiesta di risarcimento del danno non patrimoniale anche in caso di violazione di quest'articolo.

VEDI ANCHE d.l. 207 /30.12.2008 ALLEGATO IN CALCE "Nuovo profilo sanzionatorio".

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

MODALITÀ PER AGGIORNARSI SULLE MISURE MINIME DI SICUREZZA ADOTTATE

Il Codice prevede che il disciplinare tecnico (allegato B) relativo alle misure minime di sicurezza, sia aggiornato periodicamente in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Eventuali ulteriori misure minime di sicurezza o modalità operative che il titolare del trattamento dovrà adottare in seguito all'aggiornamento di tale disciplinare tecnico e la cui adozione comporti un coinvolgimento degli incaricati del trattamento ai fini della realizzazione pratica, saranno comunicate direttamente agli incaricati, anche per mezzo del responsabile del trattamento, tramite circolari o posta elettronica.

Informazioni su altre misure di sicurezza minime adottate dal titolare ma che non comportano la collaborazione degli incaricati ai fini dell'attuazione, possono essere richieste al titolare, al responsabile del trattamento o al responsabile del sistema informatico, se nominati.

Rimangono comunque a disposizione degli incaricati il documento programmatico sulla sicurezza nonché i successivi aggiornamenti.

Allegato:

modulo per l'esercizio dei diritti dell'interessato.

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

ALLEGATO E - Esercizio del diritto di accesso ai dati personali e altri diritti ai sensi dell'art. 7 del Codice in materia di protezione dei dati personali

Il sottoscritto ... nato a ... il ... residente a .... con la presente istanza, presentata ai sensi dell'art. 7 del Codice in materia di protezione dei dati personali chiede:

- ❒ di avere conferma dell'esistenza di propri dati personali e di ottenerne la comunicazione in forma intelligibile;
- ❒ di conoscere l'origine dei dati medesimi;
- ❒ di conoscere le finalità, le modalità del trattamento, nonché la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- ❒ di conoscere gli estremi identificativi del titolare, dei responsabili (se designati) e del rappresentante designato ai sensi dell'articolo 5, comma 2 (se designato)
- ❒ di conoscere i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati
- ❒ l'aggiornamento *(indicare quali aggiornamenti sono richiesti)* la rettificazione *(indicare quali rettifiche sono richieste)* o l'integrazione dei propri dati personali *(indicare quali integrazioni sono richieste e qual è l'interesse a richiederle)*

- ❒ la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge *(indicare la violazione commessa*) compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati
- ❒ L'attestazione che le operazioni descritte nei due punti precedenti sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati in precedenza comunicati o diffusi ad eccezione del caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
- ❒ di opporsi al trattamento dei dati personali che mi riguardano per i seguenti legittimi motivi…….

- ❒ per opporsi al trattamento dei dati svolto per fini di informazione commerciale o di invio di materiale pubblicitario

FIRMA dell'interessato
(cioè del soggetto cui si riferiscono i dati richiesti)

Data_____ _____

D.l. 207 del 30.12.2008 G.U. 31.12.2008 n. 304

NUOVO PROFILO SANZIONATORIO

Art. 44

1. All'elenco n. 1, paragrafo 2, allegato alla legge 24 dicembre 2007, n. 244, le parole: «Decreto legislativo 30 giugno 2003, n. 196, articolo 166» sono soppresse.

2. All'articolo 161, comma 1, del decreto legislativo 30 giugno 2003, n. 196, le parole da: «tremila euro a diciottomila euro» fino alla fine del comma sono sostituite dalle seguenti: «da seimila euro a trentaseimila euro».

3. L'articolo 162 del decreto legislativo 30 giugno 2003, n. 196, è così modificato:

a) al comma 1, le parole: «da cinquemila euro a trentamila euro» sono sostituite dalle seguenti: «da diecimila euro a sessantamila euro»;

b) al comma 2, le parole: «da cinquecento euro a tremila euro» sono sostituite dalle seguenti: «da mille euro a seimila euro»;

c) dopo il comma 2, sono aggiunti, in fine, i seguenti:

«2-bis. In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 o delle disposizioni indicate nell'articolo 167 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da ventimila euro a centoventimila euro. Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta.

2-ter. In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro.».

4. All'articolo 162-bis, comma 1, del decreto legislativo 30 giugno 2003, n. 196, le parole: «, che può essere aumentata» fino alla fine del comma sono soppresse.

5. All'articolo 163, comma 1, del decreto legislativo 30 giugno 2003, n. 196, le parole: «da diecimila euro a sessantamila euro» sono sostituite dalle seguenti: «da ventimila euro a centoventimila euro» e le parole: «e con la sanzione amministrativa accessoria» fino alla fine del comma sono soppresse.

6. All'articolo 164, comma 1, del decreto legislativo 30 giugno 2003, n. 196, le parole: «da quattromila euro a ventiquattromila euro» sono sostituite dalle seguenti: «da diecimila euro a sessantamila euro».

7. Dopo l'articolo 164 del decreto legislativo 30 giugno 2003, n. 196, è inserito il seguente:

«Art. 164-bis (Casi di minore gravità e ipotesi aggravate). 1. Se taluna delle violazioni di cui agli articoli 161, 162, 163 e 164 è di minore gravità, avuto altresì riguardo alla natura anche

economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.

2. In caso di più violazioni di un'unica o di più disposizioni di cui al presente Capo, a eccezione di quelle previste dagli articoli 162, comma 2, 162-bis e 164, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da cinquantamila euro a trecentomila euro. Non è ammesso il pagamento in misura ridotta.

3. In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al presente Capo sono applicati in misura pari al doppio.

4. Le sanzioni di cui al presente Capo possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.».

8. All'articolo 165, comma 1, del decreto legislativo 30 giugno 2003, n. 196, le parole: «161, 162 e 164» sono sostituite dalle seguenti: «del presente Capo» ed è aggiunto, in fine, il seguente periodo: «La pubblicazione ha luogo a cura e spese del contravventore.».

9. L'articolo 169 del decreto legislativo 30 giugno 2003, n. 196, è così modificato:

a) nel comma 1, sono soppresse le parole da: «o con l'ammenda da» fino alla fine del comma;

b) nel comma 2, le parole: «quarto del massimo dell'ammenda stabilita per la contravvenzione» sono sostituite dalle seguenti: «quarto del massimo della sanzione stabilita per la violazione amministrativa».

10. All'articolo 62, comma 1, del decreto legislativo 6 settembre 2005, n. 206, le parole: «da euro cinquecentosedici a euro cinquemilacentosessantacinque» sono sostituite da: «da tremila euro a diciottomila euro».

11. Agli oneri derivanti dal comma 1, pari a euro 299.000 a decorrere dal 2009, si provvede mediante corrispondente riduzione dell'autorizzazione di spesa di cui al decreto legislativo 30 giugno 2003, n. 196, come determinata dalla tabella C della legge 22 dicembre 2008, n. 203 (legge finanziaria 2009), in favore del Garante per la protezione dei dati personali, a decorrere dall'esercizio 2009.

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

ALLEGATO F- modello di regolamento disciplinare regole per l'uso di Internet e della posta elettronica

Questo regolamento è adottato ai sensi del provvedimento generale del 1° marzo 2007 "**Linee guida del Garante per posta elettronica e Internet**" (G.U. n. 58 del 10 marzo 2007).

- le regole di seguito elencate hanno carattere vincolante -

PREMESSO CHE

Il datore di lavoro, quale titolare del trattamento dati, deve definire le modalità d'uso degli strumenti informatici aziendali (internet e posta elettronica) tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali: si devono infatti prevenire usi arbitrari degli strumenti informatici aziendali e la lesione della riservatezza dei lavoratori.

Si pone il divieto per il datore di lavoro di controllare arbitrariamente e sistematicamente i siti web visitati dai lavoratori, perché da essi si possono trarre informazioni anche sensibili sui dipendenti. Non gli è nemmeno concesso controllare arbitrariamente i messaggi di posta elettronica, i quali possono avere contenuti a carattere privato.

È fatto inoltre divieto di lettura e registrazione sistematica delle e-mail così come di monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori.

SI STABILISCONO LE SEGUENTI REGOLE

1) UTILIZZO DEL PERSONAL COMPUTER;
2) UTILIZZO DI PC PORTATILI;
3) UTILIZZO DI SUPPORTI MAGNETICI;
4) UTILIZZO DELLA RETE AZIENDALE;
5) UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI;

1) UTILIZZO DEL PERSONAL COMPUTER

Onde evitare il pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, salvo espressa autorizzazione da parte del titolare ovvero del responsabile, è vietato installare programmi provenienti dall'esterno.

Non è consentito utilizzare strumenti software e/o hardware atti a interpretare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.

Non è consentito modificare le configurazioni impostate sul proprio PC.
Non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come per esempio i modem).
Sui PC dotati di scheda audio e/o di lettore cd non è consentito l'ascolto di programmi, file audio o musicali, se non a fini prettamente lavorativi.

L'utente è responsabile per il proprio account e per l'uso che ne viene fatto. Di conseguenza l'utente è tenuto a tutelare il proprio account da accessi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.

I comportamenti generali riportati di seguito contribuiscono a garantire la sicurezza dell'accesso:

utilizzare una password di 8 caratteri, la quale non deve avere riferimenti riconducibili all'incaricato;
utilizzare la password con riservatezza;
modificare regolarmente la password (ogni 3-6 mesi);
non mettere a disposizione e non comunicare la password a terzi;
non trasmettere la password utilizzando la rete.

2) UTILIZZO DI EVENTUALI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno in caso di allontanamento, devono essere custoditi in un luogo protetto.

II portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.

Nel caso di accesso alla rete tramite RAS (Remote Access Server)/Accesso Remoto utilizzare l'accesso in forma esclusivamente personale ed utilizzare la password in modo rigoroso.

Disconnettersi dal sistema RAS al termine della sessione di lavoro.

Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.

Non utilizzare abbonamenti Internet privati per collegamenti alla rete.

3) UTILIZZO DI SUPPORTI MAGNETICI

Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo.

4) UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
il titolare del trattamento si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente regolamento.

5) UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Posta elettronica:

La casella di posta assegnata all'utente è uno strumento di lavoro; pertanto le persone assegnatarie di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.
Evitare che la diffusione incontrollata di "catene di sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.

Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (zip, rar, jpg).

Nel caso in cui si debba inviare un documento all'esterno è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat. pdf).

L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali; prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Potrebbero venir resi disponibili anche indirizzi condivisi tra più lavoratori, rendendo così chiara la natura non privata della corrispondenza.

Sono poi previsti, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi.

Il datore mette infine il dipendente in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e ad inoltrare al Titolare quelli ritenuti rilevanti per l'ufficio, in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.

Rete Internet:

II PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa.

È vietato compiere attività che appesantiscano il traffico o i servizi sulla rete, come pure compiere attività che possano causare disturbi al sistema senza valutarne adeguatamente le conseguenze.

E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

Non possono essere utilizzati modem privati per il collegamento alla rete.

E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato.

E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati) e di bacheche elettroniche, nonchè la registrazione in guest books anche utilizzando pseudonimi (o nicknames).

Il Titolare si riserva di individuare i siti considerati correlati con la prestazione lavorativa e di inserire filtri che prevengano determinate operazioni (quali l'accesso a siti inseriti in una sorta di black list o il download di file musicali o multimediali).

La non osservanza delle prescrizioni comporterà l'applicazione delle sanzioni disciplinari in seguito specificate.

SANZIONI DISCIPLINARI:

L'accesso ad Internet e l'uso della posta elettronica rappresentano una prerogativa che richiede da parte di tutti gli utenti un comportamento responsabile.

Si invitano quindi i dipendenti ed i collaboratori ad osservare le misure preventive sopra esposte: in base ai principi di pertinenza e non eccedenza, qualora queste non fossero sufficienti ad evitare comportamenti anomali, gli eventuali controlli saranno effettuati con gradualità.

In prima battuta si procederà con verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole.

Successivamente, ripetendosi l'anomalia, si passerà ai controlli su base individuale, nonché all'irrogazione delle sanzioni disciplinari previste dall'art. 7 dello Statuto dei Lavoratori.
Il datore di lavoro adotterà un provvedimento disciplinare nei confronti del lavoratore, dopo avergli contestato per iscritto l'addebito ed avendolo sentito a sua difesa.
I provvedimenti disciplinari saranno applicati dopo che siano trascorsi cinque giorni dalla contestazione del fatto che vi ha dato causa: entro tale termine il lavoratore destinatario potrà presentare le proprie giustificazioni in maniera sia scritta che verbale.
Il lavoratore potrà farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato.
La sanzione che verrà irrogata sarà proporzionata all'infrazione e potrà consistere in un biasimo scritto, in una multa, nella sospensione dal servizio e dalla retribuzione o addirittura nel licenziamento.

Per ogni chiarimento sarà possibile rivolgersi al Titolare, nella persona di…….

IL TITOLARE DEL TRATTAMENTO……

ISTITUTO COMPRENSIVO ROVERETO SUD
Via Benacense 32,
38068 Rovereto (TN)

ALLEGATO G - Modello atto nomina ad amministratore di sistema

(Provvedimento del Garante per la protezione dei dati personali di data 27 novembre 2008, GU 24 dicembre 2008)

Premesso

- che il Garante Privacy ha emanato il provvedimento generale di data 27 novembre 2008 (Bollettino del n. 99/novembre 2008) in materia di amministratori di sistema;
- che con tale provvedimento è stata chiaramente espressa la necessità di promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare;
- che l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti;
- che in base al punto 4.1. del citato provvedimento l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- che anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

Dopo una valutazione ed una verifica sui criteri soggettivi prescritti, Lei risulta avere i requisiti soggettivi di esperienza, capacità ed affidabilità tali da garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dati personali ivi compreso il relativo profilo della sicurezza.

Pertanto, con la presente, il sottoscritto……., in qualità di legale rappresentante della…… con sede…….. titolare del trattamento dati ex d.lgs. 196/2003, La designa quale

AMMINISTRATORE DI SISTEMA

Lei dovrà rispettare i principi generali così come sancito dal Codice in materia di protezione dei dati personali (d.lgs.. 30 giugno 2003 n. 196) nonché è tenuto a svolgere le seguenti funzioni:

- ☐ controllare, anche tramite verifiche periodiche, il funzionamento della rete e del sistema informatico installato;
- ☐ installare e/o predisporre per l'installazione dei programmi operativi, gestionali e applicativi necessari all'attività dell'ente;
- ☐ provvedere alla ordinaria manutenzione della rete, del sistema informatico e dei programmi utilizzati;
- ☐ provvedere all'installazione ovvero all'aggiornamento dei programmi antivirus e verificarne l'efficacia con cadenza almeno settimanale;
- ☐ se il sistema lo permette, provvedere all'attivazione della procedura per l'autonoma sostituzione delle parole chiave da parte degli incaricati del trattamento. Tale procedura dovrà essere comunicata agli incaricati stessi;
- ☐ attribuire a ciascun incaricato un codice identificativo personale avendo cura di evitare che un medesimo codice sia assegnato, neppure in tempi diversi, a persone diverse;
- ☐ provvedere alla disattivazione delle credenziali in caso di perdita da parte del soggetto incaricato della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo per un periodo superiore a sei mesi (ad esempio per prolungata malattia, maternità, spostamento dell'incaricato ad altre mansioni);
- ☐ eseguire ovvero sovraintendere alle procedure impostate per garantire il back-up periodico dei dati, e custodire i supporti di memorizzazione in maniera appropriata, come indicato nel documento programmatico sulla sicurezza;
- ☐ collaborare con il titolare alla predisposizione del documento programmatico sulla sicurezza;
- ☐ su indicazione del titolare o del Responsabile, se nominato, provvedere all'attivazione di limitazioni all'accesso a dati, programmi o strumenti utilizzati;
- ☐ installare e aggiornare altre misure di sicurezza ritenute necessarie, dietro preventiva autorizzazione del titolare o del responsabile, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non

autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

☐ conformare il sistema informatico ad eventuali altre norme emanate in tema di sicurezza dei dati;

☐ comunicare al titolare o al responsabile eventuali problemi o malfunzionamenti del sistema informatico;

☐ riferire al titolare, a cadenza periodica e almeno annualmente, le attività svolte;

☐ impostare un sistema di registrazione degli accessi realizzati sui sistemi di elaborazione e sugli archivi elettronici (mediante access log) che permetta l'esercizio di un corretto controllo da parte del titolare sulle operazioni svolte. Le registrazioni devono avere caratteristica di completezza, inalterabilità e possibilità di verifica della loro integrità. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate, a cura dell'amministratore di sistema per un periodo non inferire a sei mesi.

In caso di necessità può richiedere un intervento tecnico da parte di soggetti esterni avente per oggetto la manutenzione, la gestione o l'aggiornamento del software o del sistema informatico. In tal caso dovrà sovraintendere alle operazioni svolte da parte degli incaricati esterni in modo tale da presidiare il rispetto delle norme in materia di protezione dei dati personali.

Per la corretta effettuazioni di talune operazione Lei potrà avvalersi dell'aiuto di aziende esterne specializzate, qualora lo ritenga necessario. In tal caso dovrà far riferimento all'elenco di aziende previste dal titolare, che possono essere indicate nel Documento Programmatico sulla Sicurezza.

In ogni caso dovrà sovrintendere all'attività degli incaricati della manutenzione redigendo, nei limiti degli incarichi conferiti, un documento sintetico che descriva le operazioni svolte. Tale documento può essere richiesto all'azienda che ha effettuato l'intervento.

Entro il 31 dicembre di ogni anno dovrà redigere una relazione da cui risulti la rispondenza o meno alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti. Nel caso si siano verificate delle anomalie, queste dovranno essere immediatamente segnalate al titolare del trattamento ed indicate in tale ultimo documento, che verrà allegato al Documento Programmatico sulla Sicurezza.

luogo e data

Il titolare del trattamento L'amministratore di sistema