



ISTITUTO PROFESSIONALE DI STATO
PER I SERVIZI COMMERCIALI, TURISTICI E SOCIALI
"PAOLO BOSELLI"

Il Documento Programmatico sulla Sicurezza

ai sensi del D.L.vo 30/06/2003 n. 196 "Codice in materia di protezione dei dati personali"

***misure di sicurezza nel trattamento dei dati personali e
piano operativo per l'adozione delle misure minime di sicurezza***

Il presente documento si compone di n. 51 pagine (inclusa la presente)

Torino, 28 febbraio '07

Prot. n. 1588/A1

Il Direttore S.G.A.
(Paolo ASTUTI)

Il Dirigente Scolastico
(Prof. Giorgio MACCAGNO)

Prologo

Costituzione Italiana

- Art.1 *L'Italia è una Repubblica fondata sul lavoro.*
- Art.4 *La Repubblica riconosce a tutti i cittadini il diritto al lavoro e promuove le condizioni che rendono effettivo questo diritto.
Ogni cittadino ha il dovere di svolgere secondo le proprie possibilità e scelte un'attività.....*
- Art.32 *La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti.*
- Art.35 *La Repubblica tutela il lavoro in tutte le sue applicazioni. Cura l'affermazione e l'elevazione professionale dei lavoratori. Promuove e favorisce gli accordi e le organizzazioni internazionali intesi ad affermare e regolare i diritti del lavoro.*
- Art.38 *I lavoratori hanno diritto che siano provveduti e assicurati mezzi adeguati alle loro esigenze di vita in caso di infortunio, malattia.....*

Codice Civile

- Art. 2087 ***Tutela delle condizioni di lavoro: L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie per tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.***
- Art.2050 *Responsabilità per l'esercizio di attività pericolose: Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura, o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.*
- Art.1176 *Diligenza nell'adempimento: Nell'adempimento delle obbligazioni inerenti l'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata.*

Codice Penale

- Art. 437 *Rimozione o omissione dolosa di cautele contro infortuni sul lavoro: Chiunque omette di collocare impianti, apparecchi o segnali destinati a prevenire disastri o infortuni sul lavoro, ovvero rimuove o li danneggia è punito con*
- Art.451 *Omissione colposa di cautele o difese contro disastri o infortuni sul lavoro: Chiunque, per colpa, omette di collaborare ovvero rimuove o rende inservibili apparecchi o altri mezzi destinati all'estinzione di un incendio, o al salvataggio o al soccorso contro disastri o infortuni sul lavoro è punito*

Premessa

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato dall'istituto "Paolo Boselli", previsti dal D.L.vo 30/06/2003 n. 196 "Codice in materia di protezione dei dati personali".

Il piano prevede un'azione di formazione continua per tutti i dipendenti finalizzata a promuovere la cultura della sicurezza, indispensabile a garantire l'integrità e la riservatezza delle informazioni, siano esse conservate su supporti cartacei o informatici.

In particolare tale piano persegue l'obiettivo di:

- minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati sensibili;
- minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni sensibili;
- minimizzare la probabilità che i trattamenti dei dati sensibili siano modificati senza autorizzazione.

Il presente Documento Programmatico sulla Sicurezza viene divulgato a tutti gli studenti e a tutti i dipendenti della Scuola attraverso la pubblicazione sul sito internet www.istitutoboselli.it

Il presente documento è redatto dal Dirigente Scolastico Prof. Giorgio Maccagno in qualità di titolare del trattamento dei dati coadiuvato dal Direttore S.G.A. Sig. Paolo Astuti in qualità di gestore del sistema informatico, che provvedono a firmarlo in calce.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile, e comunque entro il 31 marzo di ogni anno.

Articolo 1

Normativa di riferimento e ambito di utilizzo

- Legge 675/1996;
- D.P.R. 318/1999
- Legge 325/2000;
- D.L.vo n. 196 del 30/06/2003;
- Regolamento per l'utilizzo della rete.
- [D.M. n. 305 del 7.12.2006](#), Regolamento concernente l'*"identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal MPI, in attuazione dell'art. 20 e 21 del decreto legislativo 30.6.2003 n. 96 (il «Codice in materia di protezione dei dati personali»)"*.

Il presente documento si applica a tutte le sedi dell'istituto "Paolo Boselli" site a Torino in:

- Via Montecuccoli n. 12 (di seguito denominata TO1);
- Strada Altessano n. 52/3 (di seguito denominata TO2);
- Via Luini n. 123 (di seguito denominata TO3);
- Via Montecuccoli n.12 – corsi serali (di seguito denominata TO4)

Articolo 2

Definizioni e Responsabilità

DATI IDENTIFICATIVI:

i dati personali che permettono l'identificazione diretta dell'interessato.

DATI PERSONALI:

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 ANONIMI:

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

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.

INTERESSATO:

il soggetto al quale si riferiscono i dati personali.

TITOLARE DEL TRATTAMENTO DEI DATI:

il titolare del trattamento è l'istituto scolastico e la titolarità è esercitata dal Dirigente Scolastico Prof. Giorgio Maccagno. Tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

RESPONSABILE DEL TRATTAMENTO DEI DATI:

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

Responsabili del trattamento dei dati dell'Istituto "Paolo Boselli" sono:

- **Direttore S.G.A. Sig. Paolo ASTUTI**

e per le sedi:

- **TO1 prof.ssa Paola MEZZANO;**
- **TO2 prof.ssa Maria Cristina GUIDONI;**
- **TO3 prof.ssa Maria Luisa DOGLIANI;**
- **TO4 prof. Salvatore DAMIANO**

INCARICATO AL TRATTAMENTO DEI DATI:

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

Gli Incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive ricevute dal responsabile del trattamento dei dati;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati sensibili e non.

Incaricati del trattamento dei dati dell'Istituto "Paolo Boselli" sono:

- **tutti gli insegnanti;**
- **tutti gli assistenti amministrativi;**
- **tutti gli assistenti tecnici;**
- **tutti i collaboratori scolastici.**

AMMINISTRATORE DEL SISTEMA INFORMATICO:

il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema informatico dell'Istituto "Paolo Boselli" e di consentirne l'utilizzazione.

L'amministratore del Sistema Informatico dell'Istituto "Paolo Boselli" è:

- **il Dirigente Scolastico Prof. Giorgio Maccagno.**

GESTORE DEL SISTEMA INFORMATICO:

il soggetto delegato dall'amministratore del sistema alla gestione della rete. La designazione di un responsabile è facoltativa e non esonera da responsabilità l'amministratore del sistema, il quale impartisce precise istruzioni per il buon andamento del sistema informatico. Il gestore è fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Conosce le vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

Il gestore del sistema informatico ha le seguenti responsabilità:

- sovrintende al funzionamento della rete;
- sovrintende al funzionamento del portale boselli;

- collabora con i responsabili del trattamento dei dati;
- monitora lo stato dei sistemi, con particolare attenzione alla sicurezza;
- informa il Titolare del Trattamento dei dati sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.
- effettua le copie di backup e di restore del database ARGO.
- provvede ad effettuare gli aggiornamenti degli applicativi ARGO sia sul server sia sui personal computer degli uffici.
- collabora con la Commissione New Technologies.

Nello svolgimento delle funzioni, qualora sia necessario, il gestore può avvalersi di personale tecnico per lo svolgimento di attività informatiche che richiedono complesse conoscenze e capacità.

Gestori del Sistema Informatico dell'Istituto "Paolo Boselli" sono:

- **Il Direttore S.G.A Sig. Paolo ASTUTI;**
- **Il Prof. Pietro EYDOUX**

CUSTODE DELLE PASSWORD:

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

Custode delle password dell'Istituto "Paolo Boselli" è:

- **il Dirigente Scolastico Prof. Giorgio Maccagno con delega al Direttore S.G.A. Paolo Astuti.**

IL SISTEMA INFORMATICO

Il Sistema Informatico dell'Istituto "Paolo Boselli" è costituito da una rete in VPN che collega le tre sedi site a Torino in:

- Via Montecuccoli 12
- Strada Altessano 52/3
- Via Luini 123

per un totale di 252 postazioni costituiti da personal computer Intel Pentium di varie potenze e capacità elaborative con sistemi operativi Windows XP e da 5 Server di cui 4 HP PROLIANT ML 150 G.

PERSONALE A.T.A. - ASSISTENTE TECNICO Domenico Bellantone (art. 7 CCNL)

- Adempimenti connessi alla redazione e all'attuazione del Documento Programmatico della Sicurezza.
- Collaborazione con il Direttore S.G.A. per la gestione organizzativa dell'area informatica.

PERSONALE A.T.A. - ASSISTENTI TECNICI (incarichi specifici M.P.I. e Fondo Istituto)

- incarico specifico "UFFICI SEDE TO1" al Sig. Malafronte – quota M.P.I.
L'individuazione dell'incarico specifico, con conseguente assunzione di responsabilità, nasce con l'obiettivo della **manutenzione e gestione ordinaria e straordinaria** dei computer degli uffici / presidenza / vicepresidenza al fine di garantire maggiore efficienza ed efficacia.

- incarico specifico “SEDE TO2” - alla Sig.ra Crusi - quota M.P.I.
L’individuazione dell’incarico specifico, con conseguente assunzione di responsabilità, nasce con l’obiettivo della **manutenzione e gestione straordinaria** della rete informatica, di tutti i personal computer, le attrezzature elettroniche e informatiche della sede TO2
- incarico specifico “SEDE TO3” - alla Sig.ra Camuso - quota M.P.I.
L’individuazione dell’incarico specifico, con conseguente assunzione di responsabilità, nasce con l’obiettivo della **manutenzione e gestione straordinaria** della rete informatica, di tutti i personal computer, le attrezzature elettroniche e informatiche della sede TO3
- incarico specifico “SEDE TO1” - alla Sig.ra Manti - quota fondo
L’individuazione dell’incarico specifico, con conseguente assunzione di responsabilità, nasce con l’obiettivo della **manutenzione e gestione straordinaria** della rete informatica, di tutti i personal computer, le attrezzature elettroniche e informatiche della sede TO1
- incarico specifico “SEDE TO4” – Sigg.ri Perrone e De Nittis - quota fondo
L’individuazione dell’incarico specifico, con conseguente assunzione di responsabilità, nasce con l’obiettivo della **manutenzione e gestione straordinaria** della rete informatica, di tutti i personal computer, le attrezzature elettroniche e informatiche della sede TO4

Obiettivo:

L’individuazione dell’incarico specifico, con conseguente assunzione di responsabilità, nasce con l’obiettivo di gestire l’area informatica, compresa la gestione della Rete Interna e del Portale di Istituto

Fasi:

- Collaborare con la presidenza nel controllo ed implementazione dei materiali relativi alle diverse sezioni in cui si articola il portale dell’istituto
- Gestire i diversi server garantendone la piena funzionalità
- Gestire il network per la FAD
- Collaborare con la presidenza nella stesura delle caratteristiche tecniche relative alle attrezzature informatiche ai fini delle operazioni di acquisto

Modalità operative:

tutta l’attività deve essere svolta nel rispetto delle norme sulla trasparenza (legge 241/90), privacy (d.lgs. 196/2003);

gestione portale: raccordarsi con le funzioni strumentali e il DSGA per l’aggiornamento periodico delle informazioni da pubblicare sul sito previa verifica dei contenuti da parte della presidenza

gestione server: verifica periodica della funzionalità della rete interna garantendone la funzionalità

supporto tecnico: collabora con la presidenza nella ricerca di nuove soluzioni informatiche per l’aggiornamento delle attrezzature dell’istituto, per la richiesta di preventivi e per la gestione della manutenzione e dell’aggiornamento tecnico della rete e dell’hardware

CREDENZIALI

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (LOGIN) associato a una parola chiave riservata conosciuta solamente dal medesimo (PASSWORD).

INTERNET

Il collegamento ad INTERNET è controllato dal sistema LOGIN/PASSWORD. Ogni dipendente ed ogni studente dell'Istituto "Paolo Boselli" è dotato di login e password personale. In prima istanza la password è assegnata automaticamente dal sistema che deve essere cambiata, dall'utente, al primo accesso

POLICY

La rete INTERNET della Scuola non può essere usata per:

- giocare in borsa
- visitare siti pornografici
- inserire nella "rete" dati sensibili e/o dati personali
- eseguire tentativi di Port Scanning / Brute Force / Denial of Service
- scaricare e diffondere programmi
- scaricare e diffondere file P2P (winmx, kazaa, emule, ecc....)
- divieto di uso a scopo diverso da quello lavorativo
- tutti i testi in entrata e in uscita possono essere resi pubblici in qualsiasi momento in quanto può essere necessario da parte del titolare del trattamento dei dati, dall'amministratore del sistema informatico, dal responsabile del trattamento dei dati, dai gestori del sistema informatico poter accedere ai computer della scuola per il buon funzionamento del sistema informatico.

SANZIONI

Chiunque (personale docente, A.T.A. e allievi) utilizzi internet non rispettando la POLICY, incorrerà in sanzioni disciplinari decise dal C.d.C. e nella sanzione amministrativa pecuniaria di **100,00 €** (cento/00 euro). Saranno i responsabili al trattamento dei dati e i gestori del sistema informatico a procedere a quanto sopra previsto. (delibera del Consiglio di Istituto n. 244 del 28 novembre 2006).

SITO WEB WWW.ISTITUTOBOSELLI.IT E CASELLA DI POSTA ELETTRONICA

Nel sito www.istitutoboselli.it sono inserite le circolari, gli avvisi, le comunicazioni riguardanti il personale Docente e A.T.A..

E' obbligo di ognuno verificare giornalmente la presenza di nuove informazioni.

Tutto il personale sarà dotato di una casella di posta individuale ed inserito in mail-list raggruppate per tipologia di qualifica e/o ufficio; verranno poi assegnati i compiti individuali di controllo della posta inviata con valore di comunicazione, mentre sarà compito di ognuno verificare la presenza di nuove comunicazioni sulla propria casella individuale ed utilizzarla anche per eventuali risposte. Verranno programmati momenti di formazione e addestramento al fine di raggiungere l'obiettivo sopra accennato.

Articolo 3 **Titolare, Responsabili, Incaricati**

- **Titolare del trattamento:** Dirigente Scolastico Prof. Giorgio Maccagno;
- **Responsabile del trattamento dei dati:** Direttore S.G.A. Sig. Paolo Astuti;
- **Responsabile del trattamento dei dati sede TO1:** Prof.ssa Paola Mezzano;
- **Responsabile del trattamento dei dati sede TO2:** Prof.ssa Maria Cristina Guidoni;
- **Responsabile del trattamento dei dati sede TO3:** Prof.ssa Maria Luisa Dogliani;
- **Responsabile del trattamento dei dati sede TO4:** Prof. Salvatore Damiano;
- **Amministratore di sistema:** Dirigente Scolastico Prof. Giorgio Maccagno;
- **Gestori del sistema informatico:** Direttore S.G.A. Sig. Paolo Astuti, Prof. Pietro EYDOUX;
- **Custode delle password:** Dirigente Scolastico Prof. Giorgio Maccagno con delega al Direttore S.G.A. Sig. Paolo Astuti;
- **Incaricati del trattamento dei dati:** tutti gli insegnanti, gli assistenti amministrativi, gli assistenti tecnici e i collaboratori scolastici;
- **Incaricato della consulenza e assistenza tecnica del sistema informatico dell'istituto "Paolo Boselli"** ditta ALBEDO s.r.l. Via Giulia di Barolo 12 10121 Torino

Articolo 4 **Analisi dei rischi**

I rischi a cui sono sottoposti gli archivi presenti nella scuola si possono suddividere in:

- rischio fisico
- rischio logico

Alla prima tipologia appartengono tutti gli archivi a supporto cartaceo e in parte quelli su supporto informatico. Alla seconda tipologia appartengono quelli che utilizzano elaboratori elettronici ed in specie quelli connessi in rete, sia locale che geografica.

RISCHIO FISICO

Il furto o il danneggiamento degli archivi, la diffusione o distruzione non autorizzata di informazioni personali e l'interruzione dei processi informatici possono esporre l'istituto "Paolo Boselli" al rischio di violare la legge 675/96.

archivi cartacei

Gli archivi cartacei sono conservati nel piano seminterrato in armadi e in locale chiuso a chiave ed appositamente predisposto e dotato di impianto antincendio.

I rischi fisici a cui sono sottoposti sono i seguenti:

- Accesso agli uffici e agli archivi di persone esterne alla Scuola;
- Smarrimento per incuria da parte del personale;
- Furto;
- Visura e/o copiatura da parte di personale non autorizzato;
- Perdita parziale o totale a causa di incendi o allagamenti;
- Perdita parziale o totale per il degrado naturale del supporto (invecchiamento);
- Atti di vandalismo

archivi informatici

Gli archivi informatizzati risiedono su n. 4 server HP PROLIANT ML 150 G e i rischi fisici a cui sono soggetti sono i seguenti:

- Distruzione fisica del server per eventi esterni allo stesso quali incendi, allagamenti, sbalzi di corrente;
- Guasti hardware del server tali da impedire il recupero degli archivi che si trovano sugli hard disk;
- Furto del server e/o dei supporti di backup dei dati;
- Perdita di dati dovuta a imperizia del personale addetto;
- Accesso ai server da parte di personale non autorizzato;
- Interruzione dei servizi di connessione fisica alla rete (linee telefoniche, router, modem, switch, hub);
- Atti di vandalismo.

misure di sicurezza relative agli accessi fisici

Sono definite aree ad accesso controllato quei locali che contengono apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati sensibili) e archivi informatici e/o cartacei contenenti dati sensibili; tali aree devono essere all'interno di aree sotto la responsabilità dell'Istituto "Paolo Boselli".

Il locale deve poter essere chiuso con chiave e l'accesso deve essere consentito solo alle persone autorizzate.

RISCHIO LOGICO

Il rischio logico si riferisce all'utilizzo di computer per la gestione degli archivi sia di dati comuni che sensibili.

I rischi di questo tipo si possono così sintetizzare:

- rischio interno all'organizzazione relativo all'utilizzo della LAN/Intranet;
- accesso alle banche dati da parte di personale esterno alla Scuola;
- accesso alle informazioni da parte di personale non autorizzato attraverso i punti di contatto con il mondo esterno (INTERNET);
- rischio esterno dovuto ad intrusioni nel sistema da parte di hacker;
- rischio interno/esterno di scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser;
- rischio interno dovuto a intrusioni da parte di personale docente, ATA e studenti.

Rischi interni ed esterni tipici dei servizi di rete che possono essere così riassunti:

- IP spoofing - Packet sniffing - Port scanning - Highjacking - Social engineering - Buffer overflow - Spamming - Password cracking - Trojan - Worm - Logic bomb - Malware e MMC (Malicious Mobile Code) - DoS (Denial of Service) – DDOS (Distributed Denial of Service)

Art. 5

Individuazione delle minacce

Minacce a cui sono sottoposte le risorse hardware

Le principali minacce alle risorse hardware sono:

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

Minacce a cui sono sottoposte le risorse connesse in rete

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

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

Minacce a cui sono sottoposti i dati trattati

Le principali minacce ai dati trattati sono:

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

Minacce a cui sono sottoposti i supporti di memorizzazione

Le principali minacce ai supporti di memorizzazione sono:

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

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

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione	X	X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi		X	
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di acqua		X	
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		

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

Art. 6 Individuazione delle vulnerabilità

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce sopraindicate.

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette

Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione inadeguata della rete
		Connessioni a linea pubblica non protette

Documenti cartacei	Software	Personale
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

Art. 7**Individuazione delle contromisure adottate**

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

- 1. contromisure di carattere fisico;**
- 2. contromisure di carattere procedurale;**
- 3. contromisure di carattere informatico.**

1) Contromisure di carattere fisico

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità dell'istituto "Paolo Boselli";
- i responsabili dei trattamenti sono anche responsabili dell'area in cui si trovano i trattamenti;
- i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura dei collaboratori scolastici addetti alla reception;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'istituto "Paolo Boselli";
- i locali sono provvisti di estintore (tra breve saranno dotati di allarmi e di antifurto);
- sono programmati interventi atti a dotare i locali ad accesso controllato di porte blindate, armadi ignifughi, impianti elettrici dedicati, sistemi di condizionamento, apparecchiature di continuità elettrica (sono avviati i lavori di ristrutturazione totale di tutti gli impianti elettrici, idrici e di messa a norma e sicurezza dell'istituto di Via Montecuccoli 12 - sede degli archivi sia informatici sia cartacei).

2) Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal responsabile del trattamento o da un suo delegato;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri di classe, contenenti dati comuni e particolari (certificati medici esibiti dagli alunni a giustificazione delle assenze), durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni vengono consegnati dall'insegnante dell'ultima ora di lezione al collaboratore scolastico incaricato

al trattamento dei dati e successivamente conservati, per la loro custodia, in apposito armadio dotato di serratura nella stanza individuata come segreteria di sede.

- il docente è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del docente che è chiuso a chiave. Una chiave di riserva è mantenuta con le dovute cautele dalla scuola (presso l'ufficio del Direttore S.G.A.);
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato presso la cassaforte nell'ufficio del Direttore S.G.A.

Inoltre per il trattamento dei soli dati cartacei sono adottate le seguenti disposizioni:

- si accede ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
- si utilizzano archivi con accesso selezionato;
- atti e documenti devono essere restituiti al termine delle operazioni;
- è fatto divieto di fare fotocopie e/o fare scansioni di documenti senza l'autorizzazione del responsabile del trattamento;
- è fatto divieto di esportare documenti o copie dei medesimi all'esterno dell'Istituto senza l'autorizzazione del responsabile del trattamento, tale divieto si estende anche all'esportazione telematica;
- il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti deve essere ridotto in minuti frammenti.

3) Contromisure di carattere informatico

Le misure di carattere informatico adottate sono:

- utilizzo di 5 server di cui 4 HP PROLIANT ML 150 G con configurazioni di mirroring;
- presenza di gruppi di continuità elettrica per i 3 server ubicati uno in ciascuna sede;
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows XP;
- definizione delle regole per la gestione di strumenti informatici;
- definizione delle regole di comportamento per minimizzare i rischi da virus;
- separazione logica della rete locale delle segreterie da quella dei laboratori didattici per mezzo di login/password.

Sicurezza base dati utenti

La base dati utenti viene mantenuta sicura e ridondante perché i 3 server, che gestiscono il dominio active directory, installati uno in ogni sede, sono in mirroring tra loro (l'installazione è stata effettuata a regola d'arte previa l'esecuzione di una serie di prove sperimentali a conferma del regolare funzionamento dei dispositivi applicati, delle copie di salvataggio e delle misure minime di sicurezza previste dal Disciplinare Tecnico del Testo Unico in materia di trattamento di dati personali di cui al D.Lgs. n.196/2003) sia perché è installato da febbraio 2007 una unità di backup HP STORAGEWORKS DAT 72 al posto del precedente modello HP SURESTORE DAT 24 che effettua la copia giornaliera di backup del database utenti.

Firewall

La intranet dell'Istituto si sviluppa sia su reti esclusivamente private che su reti pubbliche. In ogni punto di interconnessione tra reti pubbliche e private è stato posizionato un firewall che separa la rete privata da quella pubblica. I firewall si preoccupano di instradare attraverso la rete privata virtuale (VPN) realizzata da uno dei due fornitori di connettività (Fastweb per l'esattezza) tutto il traffico da e per le altre sedi, di instradare attraverso la connessione a larga banda di un altro fornitore (Albedo) il traffico verso la rete pubblica Internet e di impedire accessi alle reti interne da parte di soggetti non autorizzati. I firewall hanno anche il compito di impedire ad eventuali Worm o Trojan eventualmente insidiatisi sulle reti interne di scatenare attacchi verso il mondo esterno (Internet) o di attivare connessioni attraverso le quali eventuali

hacker possano introdursi nella rete stessa con particolare attenzione ai protocolli utilizzati dalle reti Microsoft (porte 137,138,139 e 445 su protocolli tcp ed udp). Il tutto è realizzato attraverso regole implementate sul sistema operativo libero "LINUX". Lo stesso sistema operativo viene mantenuto aggiornato in modo da scongiurare la possibilità dell'utilizzo di exploit di sistema per l'intrusione da parte della ditta Albedo s.r.l. che presta consulenza e assistenza tecnica. Vengono mantenuti inoltre log di tutte le attività non consentite e di quelle sospette onde poter documentare, se mai se ne avesse la necessità, eventuali attacchi subiti o traffico illecito rilevato. Nel rispetto delle regole della privacy, eventuali log mantenuti riguardanti il traffico analizzato e l'inoltro della posta elettronica, saranno resi disponibili esclusivamente all'autorità giudiziaria per eventuali controlli. L'accesso ai sistemi operativi dei firewall dall'esterno è consentito solo ed esclusivamente attraverso canali sicuri (ssh o https) e con l'utilizzo di credenziali. Le password di accesso sono conservate in busta chiusa presso la sede dell'istituto controfirmata dal sottoscritto e dal titolare del trattamento dei dati e/o dal gestore del sistema informatico.

I firewall implementati e configurati sono ubicati in:

- Via Montecuccoli, 12 sede TO1 – TO4
- Strada Altessano 52/3 sede TO2
- Via Luini 123 sede TO3

Unità di backup

L'HP STORAGEWORKS DAT 72, installato da febbraio 2007 al posto del precedente modello HP SURESTORE DAT 24, è installato nel server della sede di Via Montecuccoli 12 Torino, effettua giornalmente il backup dei dati sensibili (database di ARGO) e della struttura di active directory (database di tutti gli utenti e/o oggetti presenti nel sistema). Sarà cura del Gestore del Sistema Informatico la sostituzione e la conservazione giornaliera delle cassette di backup. Tale procedura si rende indispensabile per garantire il recupero dei dati in caso di disaster recovery. Il fronte temporale coperto è la settimana con conservazione aggiuntiva di una cassetta per ogni mese per la durata annuale.

Sistema antivirus/antispyware

Nella rete informatica dell'istituto è stato installato il software **McAfee VirusScan SMB Ed. 8.0** i un sistema antivirus/antispyware server/client installato su tutti i pc e server presenti nella rete informatica con sistema di autoaggiornamento centralizzato non disinseribile dagli utenti e in grado di prevenire attacchi di virus informatici. Detto software controlla anche le caselle di posta elettronica ed i file di attach. L'aggiornamento del software antivirus viene effettuato direttamente dalla casa fornitrice attraverso internet.

L'utilizzo di software antivirus non è sufficiente da solo a garantire e prevenire attacchi.

Secondo l'esperienza comune, un virus è riconducibile a un codice eseguibile in grado di generare copie di se stesso e di introdursi in file di dati e nel codice di altri programmi.

L'introduzione di un virus può essere causata da un'operazione diretta quale il trasferimento di un file, la lettura di un e-mail, l'installazione di un'applicazione da un supporto esterno (floppy, CD, DVD, zip) o attraverso internet o con un'azione indiretta tra cui l'apertura di un file in formato Word o Excel contenente un macro virus o la visualizzazione di una pagina Web contenente un applet o un componente Activex.

La raccomandazione è quella di lavorare, in particolare quando connessi ad internet (navigare, scaricare e-mail ecc.), come utente generico, in questo modo eventuali danni provocati da virus saranno limitati ai file a cui l'utente ha il permesso di accesso; lavorare invece come utente privilegiato, ovvero come amministratore, abbassa il livello di sicurezza intrinseca del sistema e permette, potenzialmente, ai virus di causare seri danni.

Archivi su supporto cartaceo

Le misure minime di sicurezza adottate per questo tipo di archivi sono così riassumibili.

- Individuazione di tutti gli incaricati del trattamento delle informazioni.
- Accesso ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
- Utilizzo di archivi con accesso selezionato;
- Restituzione di atti e documenti al termine delle operazioni.
- Utilizzo di armadi con controllo degli accessi agli archivi da parte del responsabile del trattamento dati.

Archivi su supporto informatico.

Le misure minime di sicurezza adottate per questo tipo di archivi si riferiscono a dati sensibili e non. Si ritiene che le misure adottate, molte delle quali in uso da anni, tendano a dare la massima copertura sui rischi a prescindere dalla tipologia dei dati.

Sicurezza fisica dei computer

I server dove sono presenti il database ARGO e l'active directory di tutti gli utenti ed il web server della scuola sono situati nell'ufficio del Direttore S.G.A. ad accesso controllato e in appositi armadi chiusi a chiave.

Difesa da accessi non autorizzati da rete geografica

La connettività internet è fornita tramite la rete FASTWEB/ALBEDO, di apposito software antivirus McAfee e di firewall atti ad evitare l'accesso alla rete da parte di utenti non autorizzati.

Utilizzo del software gestionale ARGO

Tutti gli utenti del software gestionale ARGO accedono al sistema informativo per mezzo di login e password personale. La password iniziale è assegnata dal Direttore S.G.A. che assegna inoltre le aree di competenza (p.es. alunni, bilancio, stipendi, magazzino, inventario, conti correnti, protocollo, carriera,...) e i relativi diritti (lettura, scrittura).

Login e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

La password ha le seguenti caratteristiche:

- Originale
- Composta da almeno sei caratteri
- Evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili

L'elenco delle password è conservato in cassaforte.

Le password di amministratore o root di sistema di tutti i server sono inserite e modificate periodicamente dall'amministratore del sistema informatico in accordo con la ditta che presta consulenza e assistenza tecnica; sono conservate in busta chiusa nella cassaforte.

La password di root in caso di manutenzione straordinaria può essere affidata dal dall'amministratore del sistema informatico al tecnico addetto alla manutenzione. In tal caso questa deve essere prontamente sostituita dall'amministratore del sistema al termine delle operazioni di manutenzione a cui lo stesso deve sovrintendere.

Al momento della generazione della user-id all'utente viene assegnata una propria cartella in cui salvare i propri archivi.

Regole di utilizzo delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato user-id) e password personale.

User-id e password iniziali sono assegnati dall'amministratore del sistema.

User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

L'user-id è costituita dalla prima lettera del nome seguito dal cognome per intero. In caso di omonimia si procede con le successive lettere del nome.

Scegliere una password con le seguenti caratteristiche:

1. originale
2. composta da almeno sei caratteri
3. evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
4. non deve contenere lo user-id come parte della password;
5. la password è segreta e non deve essere comunicata ad altri;
6. la password va custodita con diligenza e riservatezza;
7. l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.
8. la password assegnata inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo.

La password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.

Ogni sei mesi ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.

Le password di amministratore di tutti i PC e dei firewall che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.

In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.

La password è un elemento fondamentale per la sicurezza delle informazioni.

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

Il personale di Segreteria depositerà, in busta chiusa nella cassaforte, l'user id e la password.

Gli insegnanti e gli studenti non hanno obbligo di depositare la loro password personale.

Le credenziali di autenticazione non utilizzate da almeno tre mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali sono disattivate anche in caso di perdita di qualità che consente all'utente l'accesso ad INTERNET.

Protezione degli archivi informatici

I server che ospitano gli archivi con dati sensibili utilizzano le seguenti regole:

- obbligo di password di BIOS;
- autorizzazione scritta per l'accesso agli incaricati ed agli addetti alla manutenzione;
- gli hard disk non devono essere condivisi in rete;
- supervisione dell'incaricato del trattamento a tutte le operazioni di manutenzione che devono essere effettuate on-site;

- antivirus costantemente aggiornato; backup proceduralizzato concordato con i responsabili del trattamento e del sistema informatico;
- conservazione in cassaforte delle copie di backup;
- distruzione fisica dei floppy disk non utilizzati che contenevano copie parziali o totali degli archivi;
- obbligo di uso di screen saver con password;
- divieto di installazione, sui PC, di archivi con dati sensibili di carattere personale dell'utente;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer che contengono archivi con dati sensibili accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.
- Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
- La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.
- Al gestore del sistema informatico Direttore S.G.A. Paolo Astuti competono tutte le operazioni connesse al salvataggio giornaliero, settimanale, mensile e annuale dei dati del database ARGO
- Le operazioni di Restore sono affidate alla Ditta Albedo s.r.l. che presta consulenza e assistenza tecnica con la supervisione del gestore del sistema informatico Direttore S.G.A. Paolo Astuti

Cassaforte

Nel locale del Direttore S.G.A. Paolo Astuti si trova la cassaforte. In essa sono conservati, oltre ad altri documenti, le copie delle password, degli user id e dei backup dei dati.

Le chiavi della cassaforte sono custodite dal Dirigente Scolastico e dal Direttore S.G.A.

Riutilizzo dei supporti di memorizzazione

I supporti di memorizzazione di dati sensibili (hard disk, floppy disk, CD-ROM, dat, ecc.) sono soggetti alle seguenti misure di sicurezza:

- I floppy disk, CD-ROM, DAT non più utilizzati devono essere distrutti fisicamente mediante rottura delle parti principali e taglio delle superfici magnetiche (FD, DAT) alla presenza dell'incaricato del trattamento;
- Gli hard disk non più utilizzabili devono essere distrutti meccanicamente alla presenza dell'incaricato del trattamento;
- Gli hard disk ancora idonei all'uso, come nel caso di sostituzioni o dismissioni di personal computer, dovranno essere formattati a basso livello alla presenza dell'incaricato del trattamento che dovrà accertare la reale cancellazione di tutti i dati con la collaborazione del Gestore del Sistema Informatico o di un suo delegato.

Art. 9 Piano di formazione

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

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;

- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

Sono stati effettuati e sono già programmati, nel corso dell'a.s., corsi di formazione per tutto il personale dipendente

Il piano prevede inoltre la pubblicazione di normativa ed ordini di servizio in apposita bacheca situata all'albo di ogni sede.

Tra gli aspetti salienti della disamina degli interventi formativi degli incaricati del trattamento il Dirigente Scolastico ha ritenuto necessario ed indispensabile prevedere un adeguato e dettagliato piano di formazione del personale ATA quale incaricato del trattamento dei dati personali e del corpo docente.

Tale intervento formativo è stato predisposto ed applicato sotto la diretta vigilanza e il coordinamento del Responsabile del Trattamento.

Deve tenersi ben presente una chiara distinzione tra:

A) AGGIORNAMENTO PERIODICO

B) AGGIORNAMENTO SPECIFICO

Per il quale l'aggiornamento periodico deve essere adempiuto sotto la diretta vigilanza del Responsabile del Trattamento con cadenza almeno annuale e quello specifico, viceversa, tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuove banche dati oppure utilizzi nuovi strumenti informatici e/o nuove e diverse procedure.

Muovendo da questa considerazione ne discende che se l'incaricato viene assegnato a nuove mansioni o se viene trasferito da un settore ad un altro deve essere effettuato un nuovo e specifico aggiornamento mediante un programma individuale che deve essere impartito dal Responsabile in relazione alla nuova e specifica attività di trattamento svolta.

Art. 10 Incidente informatico

Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni. Tutti gli incaricati del trattamento dei dati sono pregati di avvisare tempestivamente il gestore del sistema informatico e i responsabili del trattamento dei dati nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso del login/password;
- modifica e sparizione di dati;
- cattive prestazioni del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente devono essere considerate le seguenti priorità:

- evitare danni diretti alle persone;
- proteggere l'informazione;
- evitare danni economici;

Garantita l'incolumità fisica alle persone si può procedere a:

- isolare il sistema compromesso dalla rete;
- spegnere correttamente il sistema;
- documentare tutte le operazioni.

Una volta spento il sistema oggetto dell'incidente non deve più essere riaccessato.

La successiva fase di indagine e di ripristino del sistema deve essere condotta da personale esperto di incident response.

Il Dirigente Scolastico, il Direttore S.G.A., i responsabili del trattamento valuteranno se coinvolgere esperti e/o autorità competenti.

E' indispensabile che, per un'eventuale indagine, venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino affrettato del sistema potrebbe alterare le prove dell'incidente.

Art. 11

Piano di attività annuale in tema di sicurezza

Al fine di aumentare i livelli di sicurezza nella protezione del patrimonio informatico della scuola è prevista la realizzazione nell'anno solare 2007 dei seguenti obiettivi:

- A) sistemazione in idonei locali degli archivi cartacei contenenti dati sensibili e le copie di backup, iniziato già dal 2005
- B) sostituzione dei computer e/o dei sistemi operativi obsoleti.

Art. 12

Aggiornamento del piano

Il presente piano è soggetto a revisione annuale con scadenza entro il 31 marzo di ogni anno; resta comunque valido fino a pubblicazione della successiva revisione.

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

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

Art. 13

Norme per il personale

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

Art. 14

Misure di sicurezza suppletive relative al trattamento di particolari dati sensibili.

Il presente paragrafo evidenzia le ulteriori misure in caso di trattamento di dati sensibili o giudiziari richieste dal disciplinare tecnico del D.Lgs. n. 196/2003 ed in particolare dal punto 19.8. per i dati personali idonei a rivelare lo stato di salute. Vengono, pertanto, individuati dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Una breve parentesi è necessaria per comprendere nel dettaglio gli adempimenti da effettuarsi ed in particolare un riferimento al punto 20 del disciplinare tecnico secondo quale "I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale,

mediante l'utilizzo di idonei strumenti elettronici" ed il successivo punto 21 che stabilisce, inoltre, che "sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti", oltre ancora il punto 22 secondo il quale "i supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili".

Per quanto riportato nel detto disciplinare il punto 23 prescrive che "sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Per quanto sopra riportato non v'è dubbio che la protezione crittografica dei dati cui si riferisce lo stesso Testo Unico in materia di trattamento di dati personali rappresenti un prezioso strumento di tutela e di sicurezza contro i rischi di accesso ai dati personali.

Deve porsi particolare attenzione al trattamento dei dati sensibili poiché debbono essere archiviati nel sistema informatico centrale con estrema sicurezza perché l'accesso alla consultazione e/o alla modificazione dei dati sensibili sarà sempre condizionato dal rispetto della procedura di identificazione degli incaricati ed in definitiva dei seguenti criteri in base ai quali:

- A. L'incaricato deve essere precisamente individuato ed autenticato;
- B. L'incaricato può trattare i dati sensibili solo con un appropriato profilo di autorizzazione;
- C. L'incaricato deve essere in possesso della chiave di lettura o cifratura.

Per quanto detto e per le menzionate procedure gestionali dei dati sensibili deve evidenziarsi in definitiva che i dati sensibili debbono essere nettamente separati e gestiti autonomamente ed indipendentemente da ogni incaricato unicamente in base al proprio profilo di autorizzazione e per quel che attiene i dati personali degli alunni riportati sui registri didattici prevedere che, al termine dell'ultima lezione del giorno, l'insegnante abbia cura di consegnare il registro di classe (contenente i certificati medici esibiti dagli alunni a giustificazione delle assenze) al collaboratore scolastico incaricato, al termine delle attività didattiche giornaliere, per la sua custodia in apposito armadio dotato di serratura nella stanza individuata come segreteria di sede.

Elenco Allegati costituenti parte integrante di questo documento

- Allegato 1 - elenco trattamenti dei dati
- Allegato 2 - regolamento per l'utilizzo del sistema informatico
- Allegato 3 - lettere di incarico per i responsabili del trattamento dei dati
- Allegato 4 - lettera di incarico per gli incaricati al trattamento dei dati
- Allegato 5 - lettera di incarico per il custode delle password
- Allegato 6 - lettera di incarico per i gestori del sistema informatico
- Allegato 7 - elenco personal computer

Il presente Documento Programmatico sulla Sicurezza viene divulgato a tutti gli studenti e a tutti i dipendenti della Scuola attraverso la pubblicazione sul sito internet www.istitutoboselli.it

Torino, 28 febbraio 2007

Il Direttore S.G.A.
(Paolo ASTUTI)

Il Dirigente Scolastico
(Prof. Giorgio MACCAGNO)

Nota: Fonti di documentazione

Il modello di documento programmatico sulla sicurezza è stato predisposto consultando le seguenti fonti:

- <http://www.garanteprivacy.it>
- <http://www.osservatoriotecnologico.net>
- “Sicurezza informatica” ECDL IT Administrator – Modulo 5 Testo di riferimento per la certificazione EUCIP - McGraw Hill ISBN 88-3864333-4 Tabelle Minacce e vulnerabilità Cap. 1
- Il regolamento per l'utilizzo della rete è stato derivato dal documento proposto alla Giornata di studio CISEL 0203G286 – CISEL Centro Studi per gli Enti Locali – Maggioli
- [D.M. n. 305 del 7.12.2006](#), Regolamento concernente l'*"identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal MPI, in attuazione dell'art. 20 e 21 del decreto legislativo 30.6.2003 n. 96 (il «Codice in materia di protezione dei dati personali»)"*.

ALLEGATO 1

Elenco trattamenti dei dati

Tabella 1 - Elenco dei trattamenti dei dati

BANCA DATI ALUNNI

FONTI NORMATIVA

Normativa vigente

FINALITA' DEL TRATTAMENTO

Istruzione ed assistenza scolastica

MODALITA' DI TRATTAMENTO (INFORMATIZZATA)

Elaborazione di dati per via telefonica o telematica, Raccolta e diffusione di dati via cavo o satellite, Raccolta dati tramite schede o coupon, Registrazione ed elaborazione su supporto cartaceo, Registrazione ed elaborazione su supporto magnetico, Impiego di supporti audiovisivi, Organizzazione degli archivi in forma prevalentemente automatizzata, Raccolta di dati presso registri, elenchi atti o documenti pubblici

MODALITA' DI TRATTAMENTO (NON INFORMATIZZATA)

Raccolta dati tramite schede o coupon, Registrazione ed elaborazione su supporto cartaceo, Organizzazione degli archivi in forma prevalentemente non automatizzata, Raccolta di dati presso registri, elenchi atti o documenti pubblici

NATURA DEI DATI

Origini razziali ed etniche, Convinzioni religiose; adesione ad organizzazione a carattere religioso, Adesione a sindacati o organizzazione a carattere sindacale, Stato di salute, Informazioni concernenti taluni provvedimenti giudiziari, Codice fiscale ed altri numeri di identificazione personale (carte sanitarie), Nominativo indirizzo o altri elementi di identificazione personale (nome, Cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, n° di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; n° carta di identità, passaporto, patente di guida; n° di posizione previdenziale o assistenziale; targa automobilistica; dati fisici: altezza, peso ecc.), Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al nucleo familiare), Lavoro (occupazione attuale, precedente; informazione sul reclutamento, sul tirocinio o sulla formazione professionale; informazione sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione; curriculum vitae o lavorativo, competenze professionali,; retribuzioni assegni, integrazioni salariali o trattenute; beni aziendali in possesso del dipendente; dati sulla gestione e sulla valutazione delle attività lavorative; cariche pubbliche rivestite), Attività economiche, commerciali, finanziarie e assicurative (dati contabili, ordini, buoni di spedizione, fatture; articoli, prodotti, servizi; contratti accordi transazioni; identificativi finanziari; redditi beni patrimoniali, investimenti, passività, solvibilità; prestiti, mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi; dati assicurativi e previdenziali), Istruzione e cultura (curriculum di studi e accademico; pubblicazioni di articoli, monografie, relazioni, materiale audiovisivo; titolo di studio)

COMUNICAZIONE E DIFFUSIONE

Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze di polizia, Uffici giudiziari, Enti locali, Associazioni di enti locali, Enti pubblici non economici, Camere di commercio, industria, artigianato ed agricoltura, Altre amministrazioni pubbliche, Enti pubblici economici, Ordini e collegi professionali, Datori di lavoro, Organismi per il collegamento occupazionale, Associazione di imprenditori e di imprese, Organizzazioni sindacali e patronati, Istituzione di formazione professionale, Consulenti e liberi professionisti anche in forma associata, Banche ed istituti di credito, Imprese di assicurazione, Associazioni e fondazioni, Organizzazioni di volontariato, Clienti ed utenti, Familiari dell'interessato, Diffusione al pubblico

LUOGO OVE RISIEDONO I DATI

Segreteria didattica sede TO1

BANCA DATI PERSONALE DIRETTIVO, INSEGNANTE E NON INSEGNANTE**FONTI NORMATIVE**

T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

FINALITA' DEL TRATTAMENTO

Trattamento giuridico ed economico del personale, Gestione del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Formazione professionale, Adempimento di obblighi fiscali e contabili, Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali, Igiene e sicurezza del lavoro, Programmazione delle attività, Gestione dei fornitori, Istruzione ed assistenza scolastica, Istruzione ed assistenza universitaria

MODALITA' DI TRATTAMENTO (INFORMATIZZATA)

Raccolta dati tramite schede o coupon, Raccolta dati in luoghi pubblici o aperti al pubblico, Raccolta di dati ai fini di trattamento da parte di terzi, Registrazione ed elaborazione su supporto cartaceo, Registrazione ed elaborazione su supporto magnetico, Organizzazione degli archivi in forma prevalentemente automatizzata, Trattamenti temporanei finalizzati ad una rapida aggregazione dei dati o alla loro trasformazione in forma anonima, Verifiche e modifiche dei dati solo ad istanza di parte, Raccolta di dati presso registri, elenchi atti o documenti pubblici

MODALITA' DI TRATTAMENTO (NON INFORMATIZZATA)

Raccolta dati tramite schede o coupon, Raccolta dati in luoghi pubblici o aperti al pubblico, Registrazione ed elaborazione su supporto cartaceo, Organizzazione degli archivi in forma prevalentemente non automatizzata, Raccolta di dati presso registri, elenchi atti o documenti pubblici

NATURA DEI DATI

Origini razziali ed etniche, Convinzioni religiose; adesione ad organizzazione a carattere religioso, Adesione a sindacati o organizzazione a carattere sindacale, Stato di salute, Informazioni concernenti taluni provvedimenti giudiziari, Codice fiscale ed altri numeri di identificazione personale (carte sanitarie), Nominativo indirizzo o altri elementi di identificazione personale (nome, Cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, n° di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; n° carta di identità, passaporto, patente di guida; n° di posizione previdenziale o assistenziale; targa automobilistica; dati fisici: altezza, peso ecc.), Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al nucleo familiare),

Lavoro (occupazione attuale, precedente; informazione sul reclutamento, sul tirocinio o sulla formazione professionale; informazione sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione; curriculum vitae o lavorativo, competenze professionali,; retribuzioni assegni, integrazioni salariali o trattenute; beni aziendali in possesso del dipendente; dati sulla gestione e sulla valutazione delle attività lavorative; cariche pubbliche rivestite), Istruzione e cultura (curriculum di studi e accademico; pubblicazioni di articoli, monografie, relazioni, materiale audiovisivo; titolo di studio)

COMUNICAZIONE E DIFFUSIONE

Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze di polizia, Uffici giudiziari, Enti locali, Associazioni di enti locali, Enti pubblici non economici, Altre amministrazioni pubbliche, Enti pubblici economici, Ordini e collegi

professionali, Datori di lavoro, Organizzazioni sindacali e patronati, Istituzione di formazione professionale, Banche ed istituti di credito, Associazioni e fondazioni, Organizzazioni di volontariato, Familiari dell'interessato, Diffusione al pubblico

LUOGO OVE RISIEDONO I DATI

Segreteria amministrativa / contabilità

BANCA DATI FORNITORI (BENI E SERVIZI)**FONTI NORMATIVE**

T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

FINALITA' DEL TRATTAMENTO

Adempimento di obblighi fiscali e contabili, Gestione dei fornitori

MODALITA' DI TRATTAMENTO (INFORMATIZZATA)

Elaborazione di dati per via telefonica o telematica, Raccolta e diffusione di dati via cavo o satellite, Raccolta dati tramite schede o coupon, Raccolta dati in luoghi pubblici o aperti al pubblico, Registrazione ed elaborazione su supporto cartaceo, Registrazione ed elaborazione su supporto magnetico, Organizzazione degli archivi in forma prevalentemente automatizzata, Trattamenti temporanei finalizzati ad una rapida aggregazione dei dati o alla loro trasformazione in forma anonima, Creazione di profili relativi a clienti, fornitori o consumatori, Raccolta di dati presso registri, elenchi atti o documenti pubblici

MODALITA' DI TRATTAMENTO (NON INFORMATIZZATA)

Raccolta di dati presso l'interessato, Elaborazione di dati per via telefonica o telematica, Raccolta e diffusione di dati via cavo o satellite, Raccolta dati tramite schede o coupon, Raccolta dati in luoghi pubblici o aperti al pubblico, Registrazione ed elaborazione su supporto cartaceo, Trattamenti temporanei finalizzati ad una rapida aggregazione dei dati o alla loro trasformazione in forma anonima

NATURA DEI DATI

Informazioni concernenti i provvedimenti giudiziari di cui all'art. 686, commi 1, lett. A) e d), 2 e 3, del codice di procedura penale, Informazioni concernenti taluni provvedimenti giudiziari, Codice fiscale ed altri numeri di identificazione personale (carte sanitarie), Nominativo indirizzo o altri elementi di identificazione personale (nome, Cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, n° di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; n° carta di identità, passaporto, patente di guida; n° di posizione previdenziale o assistenziale; targa automobilistica; dati fisici: altezza, peso ecc.), Attività economiche, commerciali, finanziarie e assicurative (dati contabili, ordini, buoni di spedizione, fatture; articoli, prodotti, servizi; contratti accordi transazioni; identificativi finanziari; redditi beni patrimoniali, investimenti, passività, solvibilità; prestiti, mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi; dati assicurativi e previdenziali), Beni, proprietà, possesso (proprietà, possessi, locazioni; beni e servizi forniti ed ottenuti)

COMUNICAZIONE E DIFFUSIONE

Organi costituzionali o di rilievo costituzionale, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze di polizia, Uffici giudiziari, Enti locali, Associazioni di enti locali, Enti pubblici non economici, Camere di commercio, industria, artigianato ed agricoltura, Altre amministrazioni pubbliche, Enti pubblici economici, Ordini e collegi professionali, Banche ed istituti di credito, Imprese di assicurazione, Diffusione al pubblico

LUOGO OVE RISIEDONO I DATI:

Segreteria amministrativa / contabilità

BANCA DATI PERSONALE A.T.A.**FONTI NORMATIVE**

T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

FINALITA' DEL TRATTAMENTO

Trattamento giuridico ed economico del personale, Gestione del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Formazione professionale, Adempimento di obblighi fiscali e contabili, Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali, Igiene e sicurezza del lavoro, Programmazione delle attività, Gestione dei fornitori, Istruzione ed assistenza scolastica, Istruzione ed assistenza universitaria

MODALITA' DI TRATTAMENTO (INFORMATIZZATA)

Raccolta dati tramite schede o coupon, Raccolta dati in luoghi pubblici o aperti al pubblico, Raccolta di dati ai fini di trattamento da parte di terzi, Registrazione ed elaborazione su supporto cartaceo, Registrazione ed elaborazione su supporto magnetico, Organizzazione degli archivi in forma prevalentemente automatizzata, Trattamenti temporanei finalizzati ad una rapida aggregazione dei dati o alla loro trasformazione in forma anonima, Verifiche e modifiche dei dati solo ad istanza di parte, Raccolta di dati presso registri, elenchi atti o documenti pubblici

MODALITA' DI TRATTAMENTO (NON INFORMATIZZATA)

Raccolta dati tramite schede o coupon, Raccolta dati in luoghi pubblici o aperti al pubblico, Registrazione ed elaborazione su supporto cartaceo, Organizzazione degli archivi in forma prevalentemente non automatizzata, Raccolta di dati presso registri, elenchi atti o documenti pubblici

NATURA DEI DATI

Origini razziali ed etniche, Convinzioni religiose; adesione ad organizzazione a carattere religioso, Adesione a sindacati o organizzazione a carattere sindacale, Stato di salute, Informazioni concernenti taluni provvedimenti giudiziari, Codice fiscale ed altri numeri di identificazione personale (carte sanitarie), Nominativo indirizzo o altri elementi di identificazione personale (nome, Cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, n° di telefono o di fax o post a elettronica; posizioni rispetto agli obblighi militari; n° carta di identità, passaporto, patente di guida; n° di posizione previdenziale o assistenziale; targa automobilistica; dati fisici: altezza, peso ecc.), Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al nucleo familiare),

Lavoro (occupazione attuale, precedente; informazione sul reclutamento, sul tirocinio o sulla formazione professionale; informazione sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione; curriculum vitae o lavorativo, competenze professionali,; retribuzioni assegni, integrazioni salariali o trattenute; beni aziendali in possesso del dipendente; dati sulla gestione e sulla valutazione delle attività lavorative; cariche pubbliche rivestite), Istruzione e cultura (curriculum di studi e accademico; pubblicazioni di articoli, monografie, relazioni, materiale audiovisivo; titolo di studio).

COMUNICAZIONE E DIFFUSIONE

Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze di polizia, Uffici giudiziari, Enti locali, Associazioni di enti locali, Enti pubblici non economici, Altre amministrazioni pubbliche, Enti pubblici economici, Ordini e collegi professionali, Datori di lavoro, Organizzazioni sindacali e patronati, Istituzione di formazione professionale, Banche ed istituti di credito, Associazioni e fondazioni, Organizzazioni di volontariato, Familiari dell'interessato, Diffusione al pubblico

LUOGO OVE RISIEDONO I DATI

Segreteria amministrativa / contabilità

PROTEZIONE DATI TRATTATI CON STRUMENTI NON AUTOMATIZZATI

Verifica	Misure Idonee	Misure Adottate	Misure da Adottare	Adottare entro
Accesso archivi dati comuni	Chiusura a chiave Procedura gestione chiavi Assegnazione incarico Cartelli Segnaletici	Chiusura a chiave Assegnazione incarico		
Accesso archivi dati sensibili o giudiziari	Armadi chiusi a chiave Custodia in cassaforte Sistemi di allarme Videoregistrazione Registrazione accessi Carico/scarico documenti Smart card Rilevazioni biometriche badge	Armadi chiusi a chiave Custodia in cassaforte		
Fotocopia abusiva	Fotocopiatrice con chiave Registrazione numero copie	Fotocopiatrice con chiave		
Presenza visione abusiva atti	Formazione Autenticazione utenti Identificazione Utenti Registrazione accessi Chiusura a chiave Istruzione incaricati	Formazione Autenticazione utenti Identificazione Utenti Chiusura a chiave Istruzione incaricati		
Uso non autorizzato dei dati	Istruzione incaricati Sanzioni disciplinari	Istruzione incaricati Sanzioni disciplinari		
Comunicazione illegale dei dati e dei documenti	Istruzione incaricati	Istruzione incaricati		
Diffusione illegale dei dati	Controllo fotocopiatrice Contr. Ripr. audio/video Istruzione incaricati	Istruzione incaricati		
Distruzione documento o atti	Registro distruzione		Registro distruzione	12 mesi
Furto dei documento o atti	Videoregistrazione Sistemi di allarme Armadi chiusi a chiave Casseforti Rilevazione accessi Vigilanza	Armadi chiusi a chiave Casseforti Vigilanza		
Ignoranza procedure gestione	Informazioni Formazione del personale Circolari	Informazioni Formazione del personale Circolari		
Mancata conservazione o restituzione dei documenti	Sanzioni disciplinari Verifiche	Sanzioni disciplinari Verifiche		
Mancata chiusura dei contenitori	Sanzioni disciplinari Verifiche	Verifiche	Sanzioni disciplinari	12 mesi
Mancata distruzione dei supporti raggiunta la finalità	Sanzioni disciplinari		Sanzioni disciplinari	12 mesi
Mancato rispetto divieto di accesso	Sanzioni disciplinari		Sanzioni disciplinari	12 mesi

PROTEZIONE TRASMISSIONE DATI

Verifica	Misure Idonee	Misure Adottate	Misure da Adottare	Adottare entro
Intercettazione dati	Crittografia Firma digitale Firewall Formazione personale Rapporti provider	Firewall Formazione personale	Rapporti provider	12 mesi
Sottrazione dati	Crittografia Firma digitale Firewall Rapporti provider Back-up Log file	Firewall Back-up	Log file	12 mesi
Distruzione dati	Crittografia Firma digitale Firewall Back-up Log file	Firewall Back-up	Log file	12 mesi
Alterazione dati	Crittografia Firma digitale Firewall Back-up Log file	Firewall Back-up	Log file	12 mesi
Perdita dati	Back-up Log file	Back-up	Log file	12 mesi
Errore invio	Gestione risorse umane Log file	Gestione risorse umane	Log file	8 mesi
Mancata destinazione	Rapporti provider Gestione risorse umane	Rapporti provider Gestione risorse umane		
Guasto tecnologico	Back-up Manutenzione Assistenza	Back-up Manutenzione Assistenza		
Interruzione trasmissione	Rapporti provider Formazione personale	Formazione personale		
Errore umano	Formazione personale	Formazione personale		
Dolo	Firewall Log file Back-up	Firewall Back-up	Log file	12 mesi

PROTEZIONE INTEGRITÀ DATI AUTOMATIZZATI SERVER O MEMORIE OVE RISIEDONO I DATI

Verifica	Misure Idonee	Misure Adottate	Misure da Adottare	Adottare entro
Accesso abusivo	Formazione Autorizzazioni accesso Autenticazione utenti Identificazione Utenti Registrazione accessi Password User-id Log file	Formazione Autorizzazioni accesso Autenticazione utenti Identificazione Utenti Password User-id	Log file	12 mesi
Presa visione abusiva	Formazione Autenticazione utenti Identificazione Utenti Registrazione accessi Password User-id Log file	Formazione Autenticazione utenti Identificazione Utenti Registrazione accessi Password User-id	Log file	12 mesi
Copia abusiva	Formazione Autenticazione utenti Identificazione Utenti Registrazione accessi Password User-id Log file	Formazione Autenticazione utenti Identificazione Utenti Registrazione accessi Password User-id	Log file	12 mesi
Virus HW e SW	Antivirus aggiornato almeno ogni sei mesi Assistenza Back-up Log file	Antivirus aggiornato almeno ogni sei mesi Assistenza Back-up	Log file	8 mesi
Guasto Tecnologico	Manutenzione Back-up Log file	Manutenzione Back-up	Log file	8 mesi
Malfunzionamento HW	Assistenza Back-up	Assistenza Back-up		
Malfunzionamento SW	Assistenza Back-up	Assistenza Back-up		
Alterazione HW e SW	Assistenza Back-up Log file	Assistenza Back-up	Log file	8 mesi
Furto HW	Chiusura a chiave Sistemi di allarme Registro controllo accessi Back-up Videosorveglianza	Chiusura a chiave Registro controllo accessi Back-up		
Furto o copiatura SW	Videosorveglianza Password User-id Back-up Log file	Password User-id Back-up	Log file	12 mesi
Disastro Naturale	Formazione Piano di emergenza Linee guida Dispositivi antincendio Back-up	Formazione Piano di emergenza Linee guida Dispositivi antincendio Back-up		
Uso Non autorizzato	Formazione Linee guida Autenticazione utenti Identificazione Utenti Registrazione accessi Password User-id	Formazione Linee guida Autenticazione utenti Identificazione Utenti Registrazione accessi Password User-id	Log file	12 mesi

	Back-up Log file	Back-up		
Manzanza di alimentazione	Gruppo di continuità manutenzione Back-up	Gruppo di continuità manutenzione Back-up		
Distruzione	Password User-id Log file Back-up	Password User-id Back-up	Log file	12 mesi
Distruzione HW e SW	Password User-id Log file Back-up	Password User-id Back-up	Log file	12 mesi
Alterazione dolosa o colposa	Password User-id Back-up Log file	Password User-id Back-up	Log file	12 mesi
Ignoranza procedurale	Formazione Informazione Back-up	Formazione Informazione Back-up		
Ignoranza misure minime	Formazione e Informazione Back-up	Formazione e Informazione Back-up		
Assenza personale	Gestione risorse umane	Gestione risorse umane		

PROTEZIONE AREE E LOCALI

Verifica	Misure Idonee	Misure Adottate	Misure da Adottare	Adottare entro
Ingresso non controllato	Vigilanza Sistemi di allarme Videoregistrazioni Registro controllo accessi Badge controllo accessi Sistemi biometrici contr. Acc. Smart Card contr. Accessi	Vigilanza Sistemi di allarme	Badge controllo accessi	12 mesi
Ingresso non autorizzato	Registro controllo accessi Autenticazione accessi Badge controllo accessi Sistemi biometrici contr. Acc. Smart Card contr. Accessi		Registro controllo accessi Badge controllo accessi	12 mesi
Incendio	Sistemi antincendio Piano di emergenza	Sistemi antincendio Piano di emergenza		
Allagamento	Piano di emergenza	Piano di emergenza		
Cedimento strutturale	Costruzione antisismica			
Sabotaggio	Videoregistrazioni Registro controllo accessi		Registro controllo accessi	12 mesi
Terremoto	Costruzione antisismica Piano di emergenza	Piano di emergenza		
Cortocircuito	Impianto certificato		Impianto certificato	12 mesi
Mancanza energia elettrica	Gruppo di alimentazione elet. Dispositivi di emergenza	Dispositivi di emergenza		

Tabella 2 - Descrizione della struttura organizzativa dell'Istituto

Struttura	Descrizione dei compiti e delle responsabilità della struttura
Area Presidenza	Supporto Ufficio Presidenza, ECDL, Stages, Archivio Storico. All'occorrenza collabora con l'area didattica.
Area Protocollo	Gestione del protocollo informatico (reso obbligatorio dal 1° gennaio 2004 dall'art. 50 del DPR 28/12/2000 n. 445) di tutti i documenti ricevuti o spediti dalla scuola e smistamento dei documenti alle varie aree, servizi, destinatari, archivio. Gestione delle commissioni esterne (consegna posta, raccomandate...).
Area Didattica	Ha il compito di seguire e supportare l'allievo/famiglia nell'intero percorso scolastico, dal momento in cui accede ai servizi offerti al momento della certificazione delle competenze acquisite. Pratiche infortuni, assicurazione alunni, docenti e ATA, adempimenti INAIL.
Area Personale	Ha il compito di gestire la carriera di tutto il personale, nonché la predisposizione di tutti gli atti amministrativi
Area Contabilità, Patrimonio, Magazzino	Ha il compito di gestire tutto l'iter progettuale sia in fase di programmazione e predisposizione della documentazione relativa all'offerta formativa, sia in fase di attuazione operativa. Si propone di dare corso a tutte le procedure relative all'acquisizione di tutti i beni necessari per attuare il piano dell'offerta formativa dal momento dell'analisi dei possibili fornitori alla gestione dei beni patrimoniali.

Tabella 3 - Elenco del personale incaricato del trattamento in ogni struttura e delle dotazioni informatiche

Incaricati del trattamento dei dati sono tutti gli insegnanti, gli assistenti amministrativi, gli assistenti tecnici e i collaboratori scolastici.

Tabella 4 - Connettività internet

Connettività	Apparecchiature di comunicazione	Provider
Fibra ottica 10 Mb sede TO1/TO4	Router Cisco	Fastweb
Adsl sede TO2/TO3	Router Cisco	Albedo

ALLEGATO 2

Regolamento per l'utilizzo del sistema informatico

Art. 1

Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica dell'istituto "Paolo Boselli" e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

Art. 2

Principi generali – diritti e responsabilità

L'istituto "Paolo Boselli" promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.

Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

Art. 3

Abusi e attività vietate

E' vietato ogni tipo di abuso. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale dell'istituto "Paolo Boselli"
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne a quella dell'istituto "Paolo Boselli"
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;

- agire deliberatamente con attività che distruggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica dell'istituto "Paolo Boselli" per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

Art. 4 **Attività consentite**

E' consentito all'amministratore di sistema o a un suo delegato:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Art. 5

Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete dell'istituto "Paolo Boselli" tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.

L'amministratore e/o il gestore del sistema informatico possono regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'amministratore del sistema informatico può adottare appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Art. 6

Modalità di accesso alla rete e agli applicativi

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.

L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.

Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password.

Art. 7

Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia.

Chiunque (personale docente, A.T.A. e allievi) utilizzi internet non rispettando la POLICY, incorrerà in sanzioni disciplinari decise dal C.d.C. e nella sanzione amministrativa pecuniaria di **100,00 €** (cento/00 euro). Saranno i responsabili al trattamento dei dati e i gestori del sistema informatico a procedere a quanto sopra previsto. (delibera del Consiglio di Istituto n. 244 del 28 novembre 2006).

Art. 8

Regole per la gestione di strumenti informatici

Per i server che ospitano i database sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;

- le copie di backup realizzate su unità HP SURESTORE 72 Gb sono conservate nella cassaforte dell'ufficio del Direttore S.G.A.;
- divieto di utilizzare floppy disk come mezzo per il backup;
- divieto per gli utilizzatori di computer di lasciare incustodito, o accessibile, il computer stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screen saver automatico dopo 2 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.
- divieto di utilizzare sistemi di P2P.

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

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

Il fax si trova nell'ufficio del Dirigente Scolastico ma a breve sarà spostato nell'ufficio protocollo (locale ad accesso controllato) e l'utilizzo è e sarà consentito unicamente agli incaricati del trattamento dei dati.

La manutenzione dei computer, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

Art. 9

Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei Personal Computer adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS;
- controllare con l'antivirus qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento e/o dal responsabile della sicurezza informatica;
- disattivare gli Activex e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene

da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");

- non cliccare mai su un link presente in un messaggio di posta elettronica da provenienza sconosciuta, in quanto potrebbe essere falso e portare a un sito-truffa;
- non utilizzare le chat;
- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche Personal Computer, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio Personal Computer (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC Personal Computer);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore del Sistema o un suo delegato procede a reinstallare il sistema operativo, i programmi applicativi ed i dati.

ALLEGATO 3

Lettera di incarico per i responsabili del trattamento dei dati

Lettera di nomina del responsabile del trattamento dei dati

Prot.

Al Direttore S.G.A.

Paolo ASTUTI

IL DIRIGENTE SCOLASTICO

in qualità di legale rappresentante dell'Istituzione scolastica e titolare del trattamento dei dati personali ;
ai sensi degli art. 29 e 30 del Testo Unico in materia di trattamento dei dati personali D. L.vo 196/03;
tenuto conto del ruolo funzionale svolto dalla S.V. nell'istituzione scolastica ai sensi della Tabella A, area D del CCNL vigente del Comparto scuola ;
considerato che, nell'ambito di tale ruolo, la S.V. è già interessata alle procedure del trattamento dei dati personali e/o sensibili e garantisce in modo idoneo, per capacità, esperienza ed affidabilità, il pieno rispetto e l'applicazione delle norme previste in materia di trattamento dei dati personali e di individuazione e attuazione delle misure di sicurezza;

NOMINA la S.V.

RESPONSABILE DEL TRATTAMENTO DEI DATI

In particolare, nel rispetto della normativa del codice in materia di protezione dei dati personali e/o sensibili, alla S.V. vengono affidate le seguenti responsabilità e compiti :

- Organizzare le operazioni di trattamento, al fine di rispettare le disposizioni di legge previste dal Testo Unico sulla privacy, con particolare riferimento alle misure minime di sicurezza di cui all'art.31 del T.U., lettere d'incarico, disposizioni e istruzioni, informazione e consenso degli interessati, anche nel rispetto di quanto indicato nel documento programmatico della sicurezza;
- Individuare tra il personale alle dirette dipendenze della S.V. gli incaricati del trattamento dei dati personali, attraverso un atto di nomina individuale, dando loro istruzioni scritte;
- Garantire che tutte le misure di sicurezza riguardanti i dati personali e/o sensibili siano applicate da tutti i soggetti della S.V. incaricati del trattamento;
- Vigilare sul rispetto delle istruzioni impartite a tutti gli incaricati del trattamento dei dati personali e/o sensibili;
- Interagire con il Garante, in caso di richieste di informazioni o effettuazione di controlli;
- Individuare, incaricare e nominare per iscritto, qualora la S.V. lo ritenga necessario, un Incaricato della gestione e della manutenzione degli strumenti elettronici, un Incaricato della custodia delle copie delle credenziali e un Incaricato delle copie di sicurezza delle banche dati;
- Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento e l'elenco dei sistemi di elaborazione;
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati;
- Verificare periodicamente le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità;
- Custodire e conservare i supporti utilizzati per le copie dei dati;
- Interagire con il Garante, in caso di richieste di informazioni o effettuazione di controlli;
- Informare prontamente il titolare di ogni questione rilevante ai fini della normativa sulla privacy;
- Verificare che venga effettuata in tutti i casi l'informativa all'interessato;
- Verificare che per ogni trattamento, ove sia necessario, sia stato acquisito il consenso dell'interessato;
- Verificare che le misure di sicurezza adottate siano costantemente adeguate agli aggiornamenti legislativi e al progresso tecnico.

In funzione dell'incarico conferito, sarà inoltre cura della S.V. verificare:

- che il trattamento dei dati avvenga in modo lecito e secondo correttezza;
- che la raccolta e la registrazione avvengano: per scopi determinati e legittimi ed in modo compatibile con tali scopi e nell'ambito del trattamento necessario per il funzionamento dell'istituzione scolastica; in modo esatto e se necessario con gli opportuni aggiornamenti; in modo che essi risultino pertinenti, completi e non eccedenti rispetto alle finalità di raccolta; in modo che la loro conservazione sia funzionale al periodo di tempo necessario allo scopo per il quale sono stati raccolti e successivamente trattati.

La S.V. provvederà alla distribuzione del documento programmatico per la sicurezza agli incaricati e contribuirà, sulla base della sua applicazione, alla revisione periodica del documento stesso.

La presente nomina di responsabile del Trattamento dei dati è a tempo indeterminato e può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati personali senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità civili e penali, ai sensi delle norme contenute nel D. Lvo 196/03.

IL DIRIGENTE SCOLASTICO

Titolare del trattamento dati

Lettera di nomina del responsabile del trattamento dei dati - SEDE

Prot.

Alla prof.ssa

IL DIRIGENTE SCOLASTICO

in qualità di legale rappresentante dell'Istituzione scolastica e titolare del trattamento dei dati personali ; ai sensi degli art. 29 e 30 del Testo Unico in materia di trattamento dei dati personali D. L.vo 196/03; tenuto conto della funzione svolta dalla S.V. nell'istituzione scolastica ai sensi degli articoli dal 22 al 34 del CCNL vigente del Comparto scuola; considerato che, nell'ambito di tale ruolo, la S.V. è già interessata alle procedure del trattamento dei dati personali e/o sensibili e garantisce in modo idoneo, per capacità, esperienza ed affidabilità, il pieno rispetto e l'applicazione delle norme previste in materia di trattamento dei dati personali e di individuazione e attuazione delle misure di sicurezza;

NOMINA la S.V.**RESPONSABILE DEL TRATTAMENTO DEI DATI DELLA SEDE _____**

In particolare, nel rispetto della normativa del codice in materia di protezione dei dati personali e/o sensibili, alla S.V. vengono affidate le seguenti responsabilità e compiti:

- Organizzare le operazioni di trattamento, al fine di rispettare le disposizioni di legge previste dal Testo Unico sulla privacy, con particolare riferimento alle misure minime di sicurezza di cui all'art.31 del T.U., lettere d'incarico, disposizioni e istruzioni, informazione e consenso degli interessati, anche nel rispetto di quanto indicato nel documento programmatico della sicurezza;
- Garantire che tutte le misure di sicurezza riguardanti i dati personali e/o sensibili della sede siano applicate da tutti i soggetti incaricati del trattamento;
- Vigilare sul rispetto delle istruzioni impartite a tutti gli incaricati del trattamento dei dati personali e/o sensibili;
- Prendere provvedimenti e iniziative per aggiornare, ad ogni variazione, gli uffici in cui viene effettuato il trattamento dei dati;
- Informare prontamente il titolare di ogni questione rilevante ai fini della normativa sulla privacy;
- Verificare che venga effettuata in tutti i casi l'informativa all'interessato;
- Verificare che per ogni trattamento, ove sia necessario, sia stato acquisito il consenso dell'interessato;
- Verificare che il trattamento dei dati avvenga in modo lecito e secondo correttezza;

La S.V. vigilerà alla distribuzione del documento programmatico per la sicurezza agli incaricati e contribuirà, sulla base della sua applicazione, alla revisione periodica del documento stesso.

La presente nomina di responsabile del Trattamento dei dati della sede TO1 è a tempo indeterminato e può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati personali senza preavviso. La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione, per cambio mansione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità civili e penali, ai sensi delle norme contenute nel D. Lvo 196/03.

IL DIRIGENTE SCOLASTICO
Titolare del trattamento dati

ALLEGATO 4

Lettera di incarico per gli incaricati al trattamento dei dati

Lettera di nomina dell'incaricato del trattamento dei dati

Prot.

AI/Alla prof./ssa

IL DIRIGENTE SCOLASTICO

in qualità di Titolare del trattamento dei dati personali dell'Istituzione scolastica ;
ai sensi degli art. 29 e 30 del Testo Unico in materia di trattamento dei dati personali D. L.vo 196/03;
tenuto conto della funzione svolta dalla S.V. nell'istituzione scolastica ai sensi degli articoli dal 22 al 34 del CCNL
vigente del Comparto scuola;
considerato che, nell'ambito di tale funzione, la S.V. compie operazioni di trattamento dei dati personali e/o
sensibili, nel rispetto delle norme previste in materia di trattamento dei dati ed è quindi obbligatorio e necessario
per lo svolgimento delle specifiche funzioni;

NOMINA la S.V. INCARICATO DEL TRATTAMENTO DEI DATI

i docenti e il personale educativo, di ruolo o supplente, di volta in volta assegnati all'Istituzione e per gli ambiti per
ognuno specificati.

Funzione	Ambito dei trattamenti
Docente	ogni dato inerente gli studenti, le rispettive famiglie e la carriera scolastica, limitatamente agli aspetti rilevanti e funzionali allo svolgimento della funzione docente ed educativa e finalizzati alla realizzazione dell'offerta formativa, limitatamente agli studenti delle classi a ciascuno affidate o agli studenti che partecipano a progetti o attività, anche integrative e complementari, in cui il docente sia coinvolto per progetti o incarichi previsti dal Piano dell'Offerta Formativa; dati relativi ad esperti e ditte esterne per quanto riguarda le attività didattiche, integrative e complementari per gli studenti, per incarichi organizzativi o funzionali all'offerta formativa dell'Istituzione deliberati dal collegio dei docenti e/o su espresso incarico o delega del Dirigente Scolastico.

La S.V. è pertanto autorizzata all'accesso e al trattamento dei dati personali e/o sensibili di alunni e genitori, nella
misura e nei limiti previsti dal profilo di appartenenza e dai compiti esso previsti e nel rispetto della normativa del
codice della privacy.

Istruzioni specifiche sul trattamento dei dati

Nello svolgimento di tale incarico la S.V. avrà accesso ai dati personali e/o sensibili gestiti da questa istituzione
scolastica e dovrà attenersi alle seguenti istruzioni, ai sensi dell'art. 11 del D.Lvo 196/2003:

- Trattare i dati personali e/o sensibili in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati personali e/o sensibili per scopi determinati, espliciti e legittimi, ed utilizzarli
in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e
successivamente trattati;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non
superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'estero i dati personali e/o sensibili esclusivamente
ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e
comunque nel rispetto delle istruzioni ricevute;
- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia
dato personale e/o sensibile;
- Fornire sempre l'informativa agli interessati, ai sensi dell'art 13 del D.Lvo 196/2003, utilizzando i moduli
appositamente predisposti e a disposizione presso le segreterie di ogni sede;
- Informare prontamente il Titolare e il Responsabile del trattamento di ogni circostanza idonea a
determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;

- Informare prontamente il Titolare e il Responsabile del trattamento qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali e/o sensibili per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali e/o sensibili da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alla S.V.
- Accedere solo ai dati strettamente necessari all'esercizio delle proprie funzioni ;
- Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare;
- Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
- Rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, indicate nelle allegate "Linee guida" elaborate ai sensi dell'art. 31 del D.Lvo 196/2003;
- Seguire le attività di formazione organizzate dalla istituzione scolastica per gli incaricati del trattamento dati;
- Partecipare alla attività di verifica e revisione del documento programmatico della sicurezza.

La presente nomina di Incaricato al trattamento dei dati è a tempo indeterminato e può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità civili e penali, ai sensi delle norme contenute nel D. Lvo 196/03.

IL DIRIGENTE SCOLASTICO

Titolare del trattamento dati

Lettera di nomina dell'incaricato del trattamento dei dati

Prot.

All'assistente amministrativo

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

in qualità di Responsabile del trattamento dei dati personali dell'Istituzione scolastica; ai sensi degli art. 29 e 30 del Codice in materia di protezione dei dati personali D. L.vo 196/03; tenuto conto del ruolo funzionale svolto dalla S.V. nell'istituzione scolastica ai sensi della Tabella A, area B del vigente CCNL del Comparto scuola; considerato che, nell'ambito di tale ruolo, la S.V. è già incaricata di compiere attività che implicano il trattamento dei dati personali e/o sensibili, nel rispetto delle norme previste in materia di trattamento dei dati personali;

**NOMINA la S.V.
 INCARICATO DEL TRATTAMENTO DEI DATI**

Per gli uffici di seguito indicati e per gli ambiti per ognuno specificati:

n.	Ufficio	Ambito dei trattamenti
1	Didattica	ogni dato inerente gli alunni e le rispettive famiglie; la carriera scolastica degli alunni; l'orientamento per le scuole medie; le ditte esterne per quanto riguarda le attività didattiche e l'attività formativa agli alunni.
2	ATA e Docenti	ogni dato inerente il personale ATA o il personale docente; le graduatorie interne ed esterne degli aspiranti all'impiego presso l'Istituzione.
3	Protocollo	ogni corrispondenza o atto in entrata o in uscita dall'Istituzione, con l'esclusione del protocollo riservato, anche quando tratti di persone e riguardi i dati sensibili.
4	Contabilità Amministrazione	ogni dato inerente esperti, consulenti, fornitori per tutti gli adempimenti preliminari o conseguenti a contratti per la fornitura di beni e servizi; ogni dato relativo ai dipendenti per quanto riguarda la liquidazione di compensi, le assicurazioni, i contributi e le trattenute fiscali o a qualunque titolo.
5	Magazzino	ogni dato inerente i terzi per tutti gli adempimenti preliminari o conseguenti a contratti per la fornitura di beni e servizi;

La S.V. è pertanto autorizzata all'accesso e al trattamento dei dati personali e/o sensibili di tutti i soggetti con i quali l'istituzione scolastica entra in relazione per i suoi fini istituzionali, nella misura e nei limiti previsti dalle mansioni assegnate, dagli ordini di servizio ricevuti e dalle istruzioni ivi contenute e nel rispetto della normativa del codice della privacy.

In particolare, alla S.V. è affidato l'incarico di trattare i dati personali e/o sensibili relativi all'area di assegnazione risultante dal piano delle attività e dagli ordini di servizio.

Istruzioni specifiche sul trattamento dei dati

Nello svolgimento di tale incarico la S.V. avrà perciò accesso alle banche dati gestite da questa istituzione scolastica e dovrà attenersi alle seguenti istruzioni, ai sensi dell'art. 11 del D.Lvo 196/2003:

- Trattare i dati personali e/o sensibili in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati personali e/o sensibili per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'estero i dati personali e/o sensibili esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- Fornire sempre l'informativa agli interessati, ai sensi dell'art 13 del D.Lvo 196/2003, utilizzando i moduli appositamente predisposti;
- Accertarsi che gli interessati abbiano autorizzato l'uso dei dati richiesti;
- Informare prontamente il Titolare e il Responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;

- Informare prontamente il Titolare e il Responsabile del trattamento qualora verificasse la necessità di porre in essere operazioni di trattamento di dati personali e/o sensibili per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali e/o sensibili da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alla S.V. ;
- Accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile;
- Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
- Rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, indicate nelle allegate "Linee guida in materia di sicurezza" elaborate ai sensi dell'art. 31 del D.Lvo 196/2003;
- Seguire le attività di formazione organizzate dalla istituzione scolastica per gli incaricati del trattamento dati;
- Partecipare alla attività di verifica e revisione del documento programmatico della sicurezza.

La presente nomina di incaricato al trattamento dei dati personali e/o sensibili è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali e/o sensibili senza preavviso .

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità civili e penali, ai sensi delle norme contenute nel D. L.vo 196/03.

IL DIRETTORE S.G.A.
Responsabile del trattamento dati

Lettera di nomina dell'incaricato del trattamento dei dati

Prot.

All'assistente tecnico
_____**IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI**

in qualità di Responsabile del trattamento dei dati personali dell'Istituzione scolastica; ai sensi degli art. 29 e 30 del Codice in materia di protezione dei dati personali D. L.vo 196/03; tenuto conto del ruolo funzionale svolto dalla S.V. nell'istituzione scolastica ai sensi della Tabella A, area B del vigente CCNL del Comparto scuola; considerato che, nell'ambito di tale ruolo, la S.V. può compiere attività che implicano il trattamento dei dati personali e/o sensibili, nel rispetto delle norme previste in materia di trattamento dei dati personali;

NOMINA la S.V.**INCARICATO DEL TRATTAMENTO DEI DATI**

Per le sedi di seguito indicate e per gli ambiti per ognuno specificati:

n.	Ufficio	Ambito dei trattamenti
1	SEDE TO1	rete informatica (gestione della rete e dei singoli Personal Computer)
2	SEDE TO2	rete informatica (gestione della rete e dei singoli Personal Computer)
3	SEDE TO3	rete informatica (gestione della rete e dei singoli Personal Computer)
4	SEDE TO4	rete informatica (gestione della rete e dei singoli Personal Computer)

La S.V. è pertanto autorizzata all'accesso e al trattamento dei dati personali e/o sensibili di tutti i soggetti con i quali l'istituzione scolastica entra in relazione per i suoi fini istituzionali, nella misura e nei limiti previsti dalle mansioni assegnate, dagli ordini di servizio ricevuti e dalle istruzioni ivi contenute e nel rispetto della normativa del codice della privacy.

In particolare, alla S.V. è affidato l'incarico di trattare i dati personali e/o sensibili relativi all'area di assegnazione risultante dal piano delle attività e dagli ordini di servizio.

Istruzioni specifiche sul trattamento dei dati

Nello svolgimento di tale incarico la S.V. avrà perciò accesso alle banche dati gestite da questa istituzione scolastica e dovrà attenersi alle seguenti istruzioni, ai sensi dell'art. 11 del D.Lvo 196/2003:

- Trattare i dati personali e/o sensibili in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati personali e/o sensibili per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'estero i dati personali e/o sensibili esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- Fornire sempre l'informativa agli interessati, ai sensi dell'art 13 del D.Lvo 196/2003, utilizzando i moduli appositamente predisposti;
- Accertarsi che gli interessati abbiano autorizzato l'uso dei dati richiesti;
- Informare prontamente il Titolare e il Responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;

- Informare prontamente il Titolare e il Responsabile del trattamento qualora verificasse la necessità di porre in essere operazioni di trattamento di dati personali e/o sensibili per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali e/o sensibili da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alla S.V. ;
- Accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile;
- Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
- Rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, indicate nelle allegate "Linee guida in materia di sicurezza" elaborate ai sensi dell'art. 31 del D.Lvo 196/2003;
- Seguire le attività di formazione organizzate dalla istituzione scolastica per gli incaricati del trattamento dati;
- Partecipare alla attività di verifica e revisione del documento programmatico della sicurezza.

La presente nomina di incaricato al trattamento dei dati è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati senza preavviso .

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità civili e penali, ai sensi delle norme contenute nel D. L.vo 196/03.

IL DIRETTORE S.G.A.
Responsabile del trattamento dati

Lettera di nomina dell'incaricato del trattamento dei dati

Prot.

AI Collaboratore Scolastico

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

in qualità di Responsabile del trattamento dei dati personali dell'Istituzione scolastica ;
ai sensi degli art. 29 e 30 del Codice in materia di protezione dei dati personali D. L.vo 196/03;
tenuto conto del ruolo funzionale svolto dalla S.V. nell'istituzione scolastica ai sensi della Tabella A, area A del vigente CCNL del Comparto scuola;
considerato che, nell'ambito di tali mansioni, la S.V. compie attività che possono comprendere il trattamento dei dati personali e/o sensibili;

**NOMINA la S.V.
INCARICATO DEL TRATTAMENTO DEI DATI**

La S.V. è pertanto autorizzata all'accesso e al trattamento dei dati personali e/o sensibili in occasione della gestione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta, del trasferimento fra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali e/o sensibili, della gestione degli studenti che svolgono il servizio hostess/steward.

Istruzioni specifiche sul trattamento dei dati

Nello svolgimento di tale incarico la S.V. avrà perciò accesso ai dati personali e/o sensibili gestiti da questa istituzione scolastica e dovrà attenersi alle seguenti istruzioni, ai sensi dell'art. 11 del D.Lvo 196/2003:

- Trattare i dati personali e/o sensibili in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati personali e/o sensibili per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'estero i dati personali e/o sensibili esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale
- Fornire sempre l'informativa agli interessati, ai sensi dell'art 13 del D.Lvo 196/2003, utilizzando i moduli appositamente predisposti;
- Informare prontamente il Titolare e il Responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
- Informare prontamente il Titolare e il Responsabile del trattamento qualora riverificasse la necessità di porre in essere operazioni di trattamento di dati personali e/o sensibili per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali e/o sensibili da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alla S.V.
- Accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile;
- Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della sua identità;
- Seguire le attività di formazione organizzate dalla istituzione scolastica per gli incaricati del trattamento dati;
- Partecipare alla attività di verifica e revisione del documento programmatico della sicurezza.

La presente nomina di Incaricato al trattamento dei dati è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro.

Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità civili e penali, ai sensi delle norme contenute nel D. L.vo 196/03.

IL DIRETTORE S.G.A.
Responsabile del trattamento dati

ALLEGATO 5

Lettera di incarico per il Custode delle Password

Legge n. 675/96 e D.P.R. n. 318/99 misure di sicurezza per la protezione dei dati personali

Al Direttore S.G.A.

Paolo Astuti

IL DIRIGENTE SCOLASTICO

In qualità di "Titolare del trattamento dei dati", conformemente a quanto stabilito dal DPR n. 318 del 28 luglio 1999

DELEGA

il Direttore S.G.A. Sig. Paolo ASTUTI "Custode delle Password".

Il "Custode delle Password" dichiara di essere a conoscenza di quanto stabilito dal DPR 318 del 28 luglio 1999 e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

In particolare dovrà:

- Predisporre, per ogni "Incaricato del trattamento" e per ogni "Banca Dati", una busta sulla quale è indicato lo "User-ID" utilizzato: all'interno della busta deve essere indicata la "Password" usata per accedere alla "Banca Dati".
- Conservare le buste con le "Password" in un luogo chiuso e protetto.
- Revocare tutte le "Password" non utilizzate per un periodo superiore a 6 (sei) mesi.
- Revocare tempestivamente tutte le "Password" assegnate a soggetti che su comunicazione scritta del "Responsabile del Trattamento" non sono più autorizzati ad accedere ai dati.
- Nel caso in cui l'"Incaricato del trattamento" può modificare autonomamente la propria "Password" di accesso, quest'ultimo deve consegnare ad ogni variazione al "Custode della Password" una busta chiusa sulla quale è indicato il proprio "USER-ID" che contiene la password in vigore: il "Custode della Password" provvederà a sostituire la precedente busta con quest'ultima.

Torino,

Prot. nr.

IL DIRIGENTE SCOLASTICO
Titolare del trattamento

IL DIRETTORE S.G.A.
per accettazione

ALLEGATO 6

Lettera di incarico per i Gestori del Sistema Informatico

Legge n. 675/96 e D.P.R. n. 318/99 misure di sicurezza per la protezione dei dati personali

Prot.

Al Direttore S.G.A.
Paolo ASTUTI

Al Prof.
Pietro EYDOUX

IL DIRIGENTE SCOLASTICO

in qualità di legale rappresentante dell'Istituzione scolastica, titolare del trattamento dei dati personali e di amministratore del sistema informatico;
ai sensi degli art. 29 e 30 del Testo Unico in materia di trattamento dei dati personali D. L.vo 196/03;
tenuto conto del ruolo funzionale svolto dalla S.V. nell'istituzione scolastica ai sensi della Tabella A, area D del CCNL vigente del Comparto scuola ;
considerato che, nell'ambito di tale ruolo, la S.V. è già interessata alle procedure del trattamento dei dati personali e/o sensibili e garantisce in modo idoneo, per capacità, esperienza ed affidabilità, il pieno rispetto e l'applicazione delle norme previste in materia di trattamento dei dati personali e di individuazione e attuazione delle misure di sicurezza;
vista la contrattazione integrativa di istituto a.s. 2006/2007 firmata il 22 febbraio 2007;

NOMINA le SS.LL.

GESTORE DEL SISTEMA INFORMATICO

In particolare, nel rispetto della normativa del codice in materia di protezione dei dati personali e/o sensibili, alla S.V. vengono affidate le seguenti responsabilità e compiti:

E' delegato dall'amministratore del sistema alla gestione della rete. La designazione di un responsabile è facoltativa e non esonera da responsabilità l'amministratore del sistema, il quale impartisce precise istruzioni per il buon andamento del sistema informatico. Il gestore è fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Conosce le vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

Il gestore del sistema informatico ha le seguenti responsabilità:

- sovrintende al funzionamento della rete;
- sovrintende al funzionamento del portale boselli;
- collabora con i responsabili del trattamento dei dati;
- monitora lo stato dei sistemi, con particolare attenzione alla sicurezza;
- informa il Titolare del Trattamento dei dati sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.
- effettua le copie di backup e di restore del database ARGO.
- provvede ad effettuare gli aggiornamenti degli applicativi ARGO sia sul server sia sui personal computer degli uffici.
- collabora con la Commissione New Technologies.

Nello svolgimento delle funzioni, qualora sia necessario, il gestore può avvalersi di personale tecnico per lo svolgimento di attività informatiche che richiedono complesse conoscenze e capacità.

La presente nomina di Gestore del Sistema Informatico è a tempo indeterminato e può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati personali senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità civili e penali, ai sensi delle norme contenute nel D. Lvo 196/03.

IL DIRIGENTE SCOLASTICO

Titolare del trattamento dati

ALLEGATO 7

Elenco personal computer

Vedere elenco allegato.