Documento Programmatico sulla Sicurezza

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

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

aggiornamento 2017

Il presente documento si compone di n. 37 pagine (inclusa la presente)

ISTITUTO DI ISTRUZIONE SUPERIORE "PAOLO BOSELLI"
ISTITUTO TECNICO PER IL TURISMO - ISTITUTO PROFESSIONALE PER I SERVIZI COMMERCIALI E SOCIO-SANITARI

AGGIORNAMENTO 2017

Art. 2
Supervisor della rete informatica
Responsabile del trattamento dei dati
Amministratore esterno del sistema informatico (Omnia Computers - prot. 1660/G1) in base all'art. 29 del D.Lgs. 196/2003;
Responsabile esterno del trattamento dei dati (Omnia Computers - prot. 1660/G1) in base all'art. 29 del D.Lgs. 196/2003;
Responsabile esterno del trattamento dei dati (Argosoft - prot. 1388/A15) in base all'art. 29 del D.Lgs. 196/2003;

Art. 3
server HP Proliant DL380Gen 9 (Rete uffici sede TO1)
firewall Sophos XG210
sistema antivirus/antispyware Kaspersky Endpoint Security for Business Select rete uffici

Art. 5
Aggiornamento titolare, responsabili, incaricati

Gli allegati al presente Documento Programmatico sulla Sicurezza, depositati agli atti della scuola, formano parte integrante dello stesso e sono immediatamente modificabili in base a future disposizioni di legge.

- 1 - elenco trattamenti dei dati
- 2 - descrizione della struttura organizzativa
- 3 - elenco del personale incaricato del trattamento
- 4 - connettività internet
- 5 - regolamento per l'utilizzo del sistema informatico
  (Inserito nel Documento Programmatico sulla Sicurezza come art. 19)
- 6 - lettera di incarico per il responsabile del trattamento dei dati
- 7 - lettera di incarico per gli incaricati al trattamento dei dati docenti/ATA
- 8 - lettera di incarico per il custode delle password
- 9 - lettera di incarico amministratore dei domini del sistema informatico
- 10 - lettera di incarico amministratore di dominio / D.P.S. di sede
- 11 - rifiuti di apparecchiature elettriche ed elettroniche e sicurezza dei dati personali
- 12 - netiquette (il Galateo della rete)
- 13 - elenco personal computer
- 14 - regolamento d'uso strumenti audiovisivi
- 15 - attuazione della normativa in materia di sicurezza sui luoghi di lavoro
- 16 - utilizzo di Internet e casella di posta elettronica istituzionale sul luogo di lavoro
- 17 - Informativa ex art. 13 D.Lgs. n.196/2003 e s.m.i. per il trattamento dei dati personali degli alunni e delle famiglie

Premessa

Tutto il personale dipendente della scuola (docenti, ATA) e tutti gli alunni, sono tenuti al rispetto delle norme e dei regolamenti inseriti nel presente regolamento. Utilizzando le applicazioni della rete informatica dell'istituto, l'utente (personale docente, ATA, alunni, personale esterno) acconsente al monitoraggio delle attività svolte. L'uso delle applicazioni deve essere limitato al solo scopo lavorativo. L'uso non autorizzato delle applicazioni può essere oggetto di sanzioni amministrative e/o penali.

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" e ss.mm.ii. così come modificato con Provvedimento del 25/6/2009, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema".

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 e/o archivi informatici e/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 web www.istitutoboselli.gov.it

ll presente documento è redatto dal Dirigente Scolastico Prof. Attilio Giaculli in qualità di Titolare del Trattamento dei Dati coadiuvato dal Direttore S.G.A. Sig. Paolo Astuti in qualità di Responsabile del Trattamento dei Dati e di Amministratore dei domini del sistema informatico.

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.

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 corsi diurni)
- Via Sansovino n. 150 (di seguito denominata TO2)
- Via Luini n. 123 (di seguito denominata TO3)
- Via Montecuccoli n.12 (di seguito denominata TO4 corsi serali)

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»)*";
- Pareri vincolanti Garante della Privacy;
- Normativa vigente.

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. Tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte del Responsabile 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. **Titolare del trattamento dei dati dell'Istituto "Paolo Boselli" è il Dirigente Scolastico Prof. Attilio Giaculli.**

SUPERVISOR 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. **Supervisor del sistema informatico dell'Istituto "Paolo Boselli" è il Dirigente Scolastico Prof. Attilio Giaculli.**

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.
Responsabile del trattamento dei dati dell'Istituto "Paolo Boselli" è il Direttore S.G.A. Sig. Paolo ASTUTI.

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.**
- **Responsabile esterno del trattamento dei dati:** (prot. 1388/A15) in base all'art. 29 del D.Lgs. 196/2003 ditta Argo Software Zona Ind. III fase 97100 Ragusa;
- **Responsabile esterno del trattamento dei dati:** (prot. 1660/G1) ditta Omnia Computer Via Col Bettoja 81/A 10014 Caluso (TO).

AMMINISTRATORE ESTERNO DEL SISTEMA INFORMATICO
il soggetto esterno delegato dall'amministratore del sistema a:

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, proxy server, filtri per la posta elettronica, antivirus, ecc…);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza informatica;

- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- gestire, in collaborazione con gli altri responsabili del trattamento dei dati personali, il sistema di attribuzione e gestione dei codici di accesso agli strumenti informatici;
- collaborare con l'amministratore della rete informatica rete uffici dell'istituto (Direttore S.G.A.)
- collaborare con gli assistenti tecnici dell'I.I.S. "Paolo BOSELLI" a cui è stata assegnata la password con privilegi di amministratore di dominio della rete informatica didattica/laboratori di ogni sede;
- collaborare con il responsabile del trattamento dei dati personali (Direttore S.G.A.);
- collaborare con il custode delle password (Direttore S.G.A.);
- informare il titolare del trattamento o il responsabile in caso di mancato rispetto delle norme di sicurezza e in caso di eventuali incidenti.

L'Amministratore esterno è a conoscenza e rispetta quanto stabilito dal D.Lgs n. 196 del 30/06/2003 e s.m.i. ed in particolare:

1. di conoscere e impegnarsi a rispettare, sotto la propria responsabilità e nell'ambito delle materie oggetto del presente incarico, quanto indicato nell'allegato B del "Disciplinare tecnico in materia di misure minime di sicurezza";
2. di attenersi agli obblighi di assoluta riservatezza connessi al suo incarico;
3. di trattare dati personali e/o sensibili solo se indispensabile in relazione all'assolvimento degli incarichi assegnati;
4. di rispettare le prescrizioni impartite dal titolare, tra cui il divieto assoluto di comunicare e diffondere a terzi non autorizzati le informazioni e i dati personali di cui sia venuto a conoscenza;
5. s'impegna ad adottare tutte le misure necessarie all'attuazione di quanto descritto nel Documento Programmatico sulla Sicurezza della scrivente Istituzione scolastica, in relazione ai compiti sopra indicati.

L'amministratore esterno del sistema informatico dell'Istituto "Paolo Boselli" è la Ditta Omnia Computers Via Col Bettoja 81/A 10014 Caluso (TO).

AMMINISTRATORE DEI DOMINI DEL SISTEMA INFORMATICO:
il soggetto delegato dall'amministratore del sistema all'accesso completo a tutti i dati ed a tutte le macchine appartenenti ai domini della rete (a meno di diversa ed esplicita configurazione) e alla creazione degli account e all'abilitazione degli accessi degli amministratori di dominio della rete didattica/laboratori delle sedi TO1-TO2-TO3-TO4.
La designazione di un amministratore dei domini non esonera da responsabilità l'amministratore del sistema, il quale impartisce precise istruzioni per il buon andamento del sistema informatico. L'amministratore di dominio è fornito di esperienza, capacità e affidabilità nella gestione delle reti locali e conosce le vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

L'amministratore dei domini ha le seguenti responsabilità e mansioni:

- sovrintende al funzionamento della rete informatica con particolare attenzione al controllo della sicurezza;
- sovrintende alla gestione e alla configurazione delle reti uffici segreteria e didattica/laboratori e degli apparati di rete;
- sovrintende alla gestione e all'archiviazione dati;
- definisce le modalità di monitoraggio della funzionalità e della stabilità della rete;
- controlla l'applicazione delle procedure relative alle politiche di sicurezza: controllo degli accessi interni ed esterni, salvataggio dei dati, riservatezza dei dati;
- coordina l'attività del personale tecnico interno ed esterno che interviene sulla rete;

- 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 recupero dei dati (restore) del database ARGO (applicativi uffici);
- provvede ad effettuare gli aggiornamenti degli applicativi ARGO sia sul server sia sui personal computer degli uffici;
- collabora con i responsabili del trattamento dei dati delle sedi;
- collabora con il referente del progetto Portale Boselli.

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. **L'amministratore dei domini del sistema informatico dell'Istituto "Paolo Boselli" è il Direttore S.G.A. Sig. Paolo ASTUTI.**

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. Attilio Giaculli con delega al Direttore S.G.A Sig. Paolo ASTUTI.

AMMINISTRATORE DEI DOMINI DELLA RETE INFORMATICA DIDATTICA/LABORATORI DI SEDE

- Figura di amministratore di dominio della rete didattica/laboratori in ogni sede, con conseguente assunzione di responsabilità, con l'obiettivo di una figura di responsabile della sicurezza informatica nel rispetto delle vigenti disposizioni di legge. Nella nomina individuale saranno elencate le modalità operative.
- Incarico, con conseguente assunzione di responsabilità, di responsabile per adottare e applicare in ogni sede tutte le norme e le disposizioni contenute nel Documento Programmatico sulla Sicurezza**.** Nella nomina individuale saranno elencate le modalità operative.

Per ogni sede: amministratore di dominio della rete informatica didattica/laboratori; responsabile attuazione delle disposizioni contenute nel documento programmatico sulla sicurezza (vedere allegato 11 del DPS) come da provvedimento del Garante della Privacy del 27/11/2008 e successivi.
Il Prof. Attilio Giaculli, in qualità di rappresentante legale dell'Istituto Paolo Boselli di Torino, Titolare del trattamento dei dati ai sensi del D.lgs N. 196 del 30/06/2003, supervisore della rete informatica dell'istituto**;** tenuto conto delle competenze possedute e dopo averne verificato l'idoneità rispetto alle caratteristiche di esperienza, capacità e affidabilità richieste dalle vigenti disposizioni per adempiere agli obblighi in materia di sicurezza del trattamento informatico dei dati e per svolgere l'attività di gestione tecnica dei server della rete didattica/laboratori; considerato che l'assegnazione in oggetto attiene a fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati; nomina gli assistenti tecnici:

- **amministratore dI dominio della rete informatica didattica/laboratori di sede;**
- **responsabile attuazione delle disposizioni contenute nel Documento Programmatico sulla Sicurezza;**

i cui compiti, mansioni e responsabilità sono analiticamente descritti nella nomina individuale.
Le password di amministratore di dominio della rete informatica didattica/laboratori di ogni sede sono inserite e modificate periodicamente dall'amministratore dei domini del sistema informatico; sono conservate dal custode delle password in busta chiusa nella cassaforte e assegnate agli assistenti tecnici e agli incaricati della ditta esterna. La password di acceso in caso di manutenzione straordinaria deve essere prontamente sostituita dall'amministratore dei domini del sistema informatico al termine delle operazioni di manutenzione a cui lo stesso deve sovrintendere. Al momento della generazione dell'account all'utente viene assegnata una propria cartella in cui salvare i propri archivi. **Ai sensi dell'Allegato B al D.Lgs. 196/2003 la**

password deve essere modificata almeno ogni 6 mesi. In caso di trattamento di dati sensibili, la modifica deve avvenire ogni 3 mesi.

Gli amministratori di dominio della rete informatica didattica/laboratori di sede e i responsabili dell' attuazione delle disposizioni contenute nel Documento Programmatico sulla Sicurezza dell'Istituto "Paolo Boselli" sono:

- SEDE TO1 – TO4 assistenti tecnici Sigg.re Brunilde Mazzocca e Saverio Vadrucci
- SEDE TO2 assistente tecnico Sig. Domenico Bellantone
- SEDE TO3 assistente tecnico Sig.ra Antonietta Camuso

Art. 3
Il Sistema Informatico

L'attuale configurazione della rete informatica dell'Istituto "Paolo Boselli" prevede n. 6 server ubicati in:

n. 1 Server HP Proliant DL380Gen 9 (Rete uffici sede TO1)
n. 1 Server assemblato Omnia (web server TO1)
n. 1 Server HP DL 360 P (Rete didattica/laboratori sede TO1 + server OSRA)
n. 1 Server HP DL 360 E GEN (Rete didattica/laboratori sede TO2)
n. 1 Server HP DL 360 E GEN (Rete didattica/laboratori sede TO3)

e la rete informatica è così strutturata:

- **TO1/TO4** FIBRA OTTICA FASTWEB con circa 100 computer configurazione Pentium Dual Core
- **TO2** FIBRA OTTICA FASTWEB con circa 75 computer configurazione Celeron e Pentium IV
- **TO3** FIBRA OTTICA FASTWEB con circa 65 computer configurazione Celeron e Pentium IV

Miglioramenti proposti: acquisto nuovi firewall; aggiornamento del sistema operativo su tutti i computer esistenti; acquisto nuovi personal computer; partecipazione ai PON; GECODOC e digitalizzazione PSDN (cd. dematerializzazione).

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 e s.m.i.) sia perché è installata una unità di backup BACKUP-NAS che effettua la copia giornaliera di backup del database utenti. Per la rete segreteria gli harde disk sono in mirroring sul server con contestuale backup dei dati su NAS.

FIREWALL/PROXY SERVER
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 dal fornitore di connettività (Fastweb) tutto il traffico da e per le altre sedi e verso la rete pubblica Internet per

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 sui firewall Sophos XG210 (uno per ogni sede) comprensivi di maintenance pack.
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 titolare del trattamento dei dati e/o dal responsabile del trattamento dei dati.

I firewall Sophos XG210 sono ubicati in:

- Via Montecuccoli, 12 sede TO1 - TO4
- Via Sansovino, 150 sede TO2
- Via Luini, 123 sede TO3

UNITÀ DI BACKUP
L'unità di BACKUP-NAS 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 Direttore S.G.A. verificare la correttezza della procedura che 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 un DVD per ogni mese per la durata annuale.

SISTEMA ANTIVIRUS/ANTISPYWARE
Nella rete informatica dell'istituto è installato il software antivirus Kaspersky Endpoint Security for Business Select un sistema antivirus/antispyware server/client installato su tutti i pc e server presenti nella rete informatica uffici 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 attacchi. 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.

CONTROLLO DEI CONTENUTI
Nel contesto educativo è necessario distinguere le fasce di età. Nel caso della scuola secondaria di secondo grado (superiore), può essere utile responsabilizzare gli studenti e il personale docente e ATA e consegnare le credenziali di autenticazione individuali.
Specifiche richieste:

- Filtrare in base al contenuto delle pagine web visitate;
- Filtrare in base alla classificazione PICS (Platform fo Internet Control Selection);
- Filtrare in base agli URL;
- Offrire flessibilità in modo da adattarsi a utenti di diverse età.

FILTRO CONTENUTI
L'Istituto "Paolo BOSELLI" ha installato sulla propria rete informatica un software per il filtraggio dei contenuti sul web. Il filtraggio è attuato usando molti metodi, quali white list/black list, l'analisi dell'URL e del dominio, del contenuto testuale, delle immagini, del contenuto MIME, dell'estensione del file. È in grado di controllare liste anche molto grandi di domini, URLs, parole o frasi correlate alla pornografia e altro.

FILE LOG
L'Istituto "Paolo BOSELLI" ha installato sulla propria rete informatica un software di controllo degli accessi logici degli amministratori di rete, di sistema e di dominio dell'istituto per adeguarla alle disposizioni impartite dal Garante della Privacy (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27/11/2008 G.U. n. 300 del 24/12/2008 e s.m.i del 25/06/2009 G.U. n. 149 del 30/06/2009). L'Autorità Garante ha inteso creare un sistema di controllo sulle attività effettuate dagli amministratori relativamente alle strutture informatiche ed ai dati in esse contenute. In questo modo si è cercato di limitare il rischio di commissione di reati da parte del personale che, sfruttando la qualifica di amministratore, può abusivamente permanere all'interno di sistemi informatici contro la volontà del titolare stesso**,** cancellare o alterare i dati in essi contenuti o, peggio, porre in essere attività lesive o dolose. Pertanto la creazione di un registro degli accessi logici (riferimenti temporali e la descrizione dell'evento che le ha generate) rappresenta un primo, sufficiente deterrente per attività illecite commesse da detto personale allorché operante in qualità di amministratore.
Il Dirigente Scolastico, nella veste di Supervisore della rete informatica, ha le credenziali per visionare i file log e redigere, almeno un volta l'anno, il rapporto di verifica dell'operato degli amministratori (i responsabili individuati dalla ditta Omnia Computers, il Direttore S.G.A. per la rete informatica e tutti gli assistenti tecnici per la rete "didattica/laboratori").
Il file log degli Amministratori di sistema registrerà gli accessi ai sistemi client, workstation e server, dove sono presenti dati sensibili in base alla normativa vigente.

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

INTERNET

Il collegamento ad INTERNET è controllato dal sistema USERNAME/PASSWORD. Ogni dipendente ed ogni studente dell'Istituto "Paolo Boselli" è dotato di USERNAME e password personale. In prima istanza la password è assegnata automaticamente dal sistema che deve essere cambiata, dall'utente, al primo accesso. Utilizzando le applicazioni della rete informatica dell'istituto l'utente acconsente al monitoraggio delle attività svolte. L'uso delle applicazioni deve essere limitato al solo scopo lavorativo. L'uso non autorizzato delle applicazioni può essere oggetto di sanzioni amministrative e/o penali.

POLICY (vedere anche l'art. 19 del presente documento)
La rete INTERNET della Scuola non può essere usata per:

- uso diverso da quello lavorativo;
- giocare in borsa;
- visitare siti pornografici;
- scommettere e fare giochi di azzardo;
- inserire nella "rete" dati sensibili e/o dati personali;
- eseguire tentativi di Port Scanning / Brute Force / Denial of Service;
- scaricare e diffondere programmi e/o file P2P (winmx, kazaa, emule, ecc….);
- utilizzare social network (face book, messanger, twitter, net log, ecc…)
- scaricare, diffondere e utilizzare software per il controllo remoto dei pc;
- caricare sui computer e sulla rete copie di opere dell'ingegno protette . Allo stesso modo, tali opere non possono essere distribuite tramite internet e gli utenti non sono autorizzati ad utilizzare sistemi di file sharing tramite computer di proprietà della scuola;
- 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.

L'Istituto "Paolo Boselli" rispetta il diritto d'autore di tutti coloro che sono coinvolti nella creazione e distribuzione di musica, film, software, opere letterarie, opere d'arte e lavori scientifici. Gli utenti dell'Istituto "Paolo Boselli" non possono scaricare, caricare, condividere, detenere e rendere disponibili copie non autorizzate di opere tutelate da diritto d'autore tramite la rete, i computer e ogni altro apparato informatico di proprietà della scuola.
Gli utenti dell'Istituto "Paolo Boselli" non possono installare e/o utilizzare sistemi di file sharing o gestire server per il peer to peer tramite la rete, i computer e ogni altro apparato informatico di proprietà della scuola.
L'utilizzo della rete informatica dell'istituto "Paolo Boselli" è disciplinata dal regolamento di cui all'art. 19 del presente documento.

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 a procedere a quanto sopra previsto. (delibera del Consiglio di Istituto n. 244 del 28 novembre 2006).

SITI WEB e CASELLA DI POSTA ELETTRONICA

Nel sito www.istitutoboselli.gov.it sono inserite le comunicazioni in base alla normativa vigente (albo on line, amministrazione trasparente, ecc…), le circolari, gli avvisi, le comunicazioni riguardanti il personale Docente, A.T.A. e alunni.

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

Sulle caselle di posta elettronica saranno inoltrate eventuali comunicazioni di servizio con valore di comunicazione. E' compito di ognuno verificarne la presenza sulla propria casella individuale ed utilizzarla anche per eventuali risposte.

Articolo 4
Firma digitale e posta elettronica certificata

Nell'ambito del processo di dematerializzazione, il decreto legge 185/2008, all'art. 16, commi 8, 9, 10 e 11, dispone che tutte le Pubbliche amministrazioni, comprese le scuole, devono istituire una casella di posta elettronica certificata (PEC) per ciascun registro di protocollo, dandone comunicazione al Cnipa (Centro nazionale per l'informatica nella pubblica amministrazione), che provvederà alla pubblicazione degli indirizzi in un elenco consultabile per via telematica.

L'istituto "Paolo Boselli" è in possesso della casella di posta certificata TOIS052008@pec.istruzione.it oltre a quella d'istituto TOIS052008@istruzione.it come da disposizioni della circolare n. 1/2010/DDI del 18/02/2010 del Dipartimento per la digitalizzazione della Pubblica Amministrazione e l'innovazione tecnologica.

L'attuazione di tali disposizioni dovrà essere effettuata senza maggiori oneri a carico della finanza pubblica, utilizzando le risorse disponibili.

Viene precisato, inoltre, che le comunicazioni tramite posta elettronica certificata, tra le pubbliche amministrazioni, possono avvenire senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo.

La consultazione on-line dei singoli indirizzi di posta elettronica certificata di imprese, professionisti e pubbliche amministrazioni dovrà essere libera e gratuita. L'estrazione di elenchi di indirizzi è consentita alle sole pubbliche amministrazioni per le comunicazioni relative agli adempimenti amministrativi di loro competenza.

Le copie su supporto informatico di qualsiasi tipologia di documenti analogici originali, formati in origine su supporto cartaceo o su altro supporto non informatico, sostituiscono ad ogni effetto di legge gli originali da cui sono tratte se la loro conformità all'originale è assicurata da chi lo detiene mediante l'utilizzo della propria firma digitale.

Articolo 5
Titolare – Responsabili - Incaricati

- Titolare del trattamento: Dirigente Scolastico Prof. Attilio Giaculli;
- Responsabile del trattamento dei dati: Direttore S.G.A. Sig. Paolo Astuti
- Supervisore del sistema informatico: Dirigente Scolastico Prof. Attilio Giaculli;
- Amministratore dei domini del sistema informatico: Direttore S.G.A. Sig. Paolo Astuti;
- Amministratore esterno del sistema informatico: ditta OMNIA COMPUTERS Via Col Bettola 81/A Caluso (TO);
- Amministratori di dominio della rete didattica/laboratori di sede: assistenti tecnici di sede;
- Responsabile gestione proxy server: ditta OMNIA COMPUTERS Via Col Bettola 81/A Caluso (TO);

- Responsabile attuazione delle disposizioni contenute nel Documento Programmatico sulla Sicurezza: assistenti tecnici di sede;
- Custode delle password: Dirigente Scolastico Prof. Attilio Giaculli 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;
- Responsabile esterno del trattamento dei dati: (prot. 1388/A15) in base all'art. 29 del D.Lgs. 196/2003 ditta Argo Software Zona Ind. III fase 97100 Ragusa;
- Responsabile esterno del trattamento dei dati: (prot. 1660/G1) in base all'art. 29 del D.Lgs. 196/2003 ditta Omnia Computer Via Col Bettoja 81/A 10014 Caluso (TO).

Articolo 6
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 locali chiusi a chiave ed appositamente predisposti e dotati 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. 5 Server di cui 4 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;
- utilizzo di pen drive non opportunamente verificate circa la presenza di software maligno;
- 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:
minaccia alla proprietà/confidenzialità/autenticità dell'informazione

- cattura di passwords (sniffers, trojan horse, worm, IP spoofing, brute force, password cracking, packet sniffing, port scanning, highjacking, social engineering, buffer overflow, logic bomb, malware e MMC (Malicious Mobile Code), DoS (Denial of Service), DDOS (Distributed Denial of Service);
- acquisizione dei privilegi di amministratore di sistema da parte di soggetti non autorizzati;
- mail spamming (utilizzo dei server di posta elettronica per la spedizione su Internet di messaggi non richiesti, ad esempio pubblicitari)

minaccia all'integrità dell'informazione: diffusione di virus informatici (application-layer attacks):
minaccia alla disponibilità dell'informazione: denial-of-service (fermo dei servizi, fermo macchina, distruzione di dati).

Art. 7
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		
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. 8
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. 9
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.

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 della 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 server 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;
- definizione delle regole per la gestione di strumenti informatici;
- definizione delle regole di comportamento per minimizzare i rischi da virus;
- separazione fisica e logica della rete locale delle segreterie da quella dei laboratori didattici per mezzo di USERNAME/password.

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 tecnico ad accesso controllato e in appositi armadi chiusi a chiave. Nell'ufficio del Direttore S.G.A. è ubicato lo switch, il router ed il firewall della rete informatica della sede TO1.

Difesa da accessi non autorizzati da rete geografica
La connettività internet è fornita tramite la rete FASTWEB, di apposito software antivirus Kaspersky, di firewall e di proxy server atti ad evitare l'accesso alla rete da parte di utenti non autorizzati.

Utilizzo del software gestionale ARGO
Tutti gli assistenti amministrativi che utilizzano i software gestionali ARGO accedono al sistema informativo per mezzo di USERNAME e password personale. La password 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).
USERNAME e password sono strettamente personali e non possono essere riassegnate ad altri utenti. L'elenco delle password è conservato in cassaforte.
Ai sensi dell'Allegato B al D.Lgs. 196/2003 la password deve essere modificata almeno ogni 6 mesi. In caso di trattamento di dati sensibili, la modifica deve avvenire ogni 3 mesi.

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:

a) la password dovrà essere composta da **almeno 8 caratteri;**
b) la riservatezza della password è responsabilità dell'utente che ne è proprietario;
c) la password fornita al primo accesso in rete deve essere modificata dall'utente al primo utilizzo e, successivamente, almeno ogni mese; la password è comunque modificabile dall'utente in qualsiasi momento (operazione periodicamente consigliata);
d) la password deve essere diversa dall'ultima utilizzata e non deve contenere riferimenti agevolmente riconducibili all'utente;
e) i codici identificativi e/o le password non vanno per alcun motivo comunicati a terzi, nemmeno agli amministratori del sistema e di dominio;
f) non è consentito trascrivere le password su supporti agevolmente accessibili da parte di terzi (post-it o altro sullo schermo o sulla scrivania);

g) le credenziali non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
h) le credenziali sono disattivate anche in caso di perdita dei requisiti per poter essere utente attivo del dominio boselli;
i) il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi;
j) l'utente è tenuto a rendere inaccessibile la propria postazione di lavoro ogni volta che si assenta, utilizzando la funzione di blocco del sistema (che viene attivata premendo contemporaneamente i tasti Ctrl/Alt/Canc e cliccando sul bottone "blocca computer");

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.
Gli assistenti amministrativi depositeranno, 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.
Ai sensi dell'Allegato B al D.Lgs. 196/2003 la password deve essere modificata almeno ogni 6 mesi. In caso di trattamento di dati sensibili, la modifica deve avvenire ogni 3 mesi.
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 esterna 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, chiavette USB, CD-ROM, DVD, ecc.) sono soggetti alle seguenti misure di sicurezza:

- I supporti 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.

Art. 10
Servizi "ARGO WEB" - GECODOC

L'Istituto "Paolo Boselli" utilizza i programmi software Argo. Il sistema Argo, grazie all'utilizzo dei più avanzati ambienti di sviluppo per il web, è in grado di operare via internet consentendo ai dirigenti e al personale della scuola di inserire e/o consultare in tempo reale il sistema informativo scolastico. Inoltre fornisce diversi servizi informativi alle famiglie via web e/o sms garantendo il massimo della sicurezza e della privacy. Si tratta di un portale grazie al quale le famiglie hanno la possibilità di comunicare con la segreteria, i docenti e il dirigente comodamente da casa o da qualunque accesso ad Internet.
La piattaforma SCUOLANEXT consente la piena digitalizzazione della scuola: completa gestione dei registri elettronici di classe e del professore, rilevazione delle assenze in tempo reale, orario scolastico, prenotazione colloqui, condivisione delle lezioni, bacheca on line, presa visione dei voti, degli scrutini, richieste via web di certificati e documenti, informazioni a supporto degli alunni e delle famiglie per

orientarsi nelle scelte future, spazi virtuali per docenti ed alunni dove condividere e rendere fruibili: lezioni multimediali, materiale didattico, link per approfondimenti, tesine, ecc....
L'utilizzo degli applicativi Argo offrono i seguenti vantaggi:

- Aggiornamento: le applicazioni WEB-based vengono aggiornate automaticamente in forma semplice e veloce perché distribuite via internet;
- Immediatezza di accesso: le applicazioni WEB-based non hanno bisogno di essere scaricate, installate e configurate. Basta l'autenticazione online da parte dell'utente attraverso login e password;
- Accesso multiutenza: questo tipo di applicazioni possono essere utilizzate da diversi utenti nello stesso momento attraverso un browser WEB;
- Libertà di lavoro: le applicazioni WEB-based lasciano libero l'utente di poter svolgere il proprio lavoro dal luogo che ritiene più opportuno. E' sufficiente un pc collegato a internet;
- Sicurezza dei dati: l'esecuzione automatica del backup dei dati ne garantisce la loro salvaguardia, limitando al massimo i rischi di perdita dei dati inseriti a causa di virus;
- Riduzione costi di gestione: le applicazioni su base WEB consentono di abbattere i costi di gestione aziendali. Investendo su un unico software, si può soddisfare un elevato numero di utenti, risparmiando i costi delle licenze d'uso multiple;
- Registro di classe/del professore: gestione del registro di classe e del professore informatizzata mediante il software scuolanext come da normativa sulla dematerializzazione.

Gecodoc è la piattaforma Argo pensata per la riorganizzazione dei documenti digitali della scuola (cd. dematerializzazione). L'evoluzione normativa degli ultimi anni, le disposizioni ministeriali, hanno modificato il panorama della gestione documentale, sostituendo sempre più la produzione di atti e documenti cartacei con modalità digitali.

Gecodoc favorisce contemporaneamente la trasparenza dei processi nella scuola: un sistema dotato di semplici e comodi strumenti che permetono alla scuola l'archiviazione di tutti quei documenti prodotti dai sistemi informatici consentendone il loro rapido reperimento, consente di:
- *protocollare direttamente dal gestionale i documenti in ingresso o in uscita*, ciò vi solleverà dal dover gestire separatamente la fase della protocollazione da quella dell'archiviazione documentale;
- *acquisire le fatture elettroniche scaricate dal SIDI*: i file potranno essere importati senza dover prima essere scompattati ed estratti dalla busta crittografica della firma;
- *parametrizzare le caselle di posta elettronica* (sia peo che pec) utilizzate dall'istituzione scolastica, e definire per ciascuna casella gli utenti abilitati alla consultazione della posta. Ciò permetterà agli utenti abilitati di importare all'interno del sistema le mail di interesse e di assegnarle agli uffici di pertinenza.

La ditta Argo software è stata nominata responsabile esterno del trattamento dei dati in base all'art. 29 del D.Lgs. 196/2003.

Art. 11
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.

Art. 12
Incidente informatico

Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come furto, 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 USERNAME/password;
- modifica e furto 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 riacceso.
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. e i responsabili del trattamento valuteranno se coinvolgere esperti e/o autorità di polizia 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. 13

Verifica dell'adeguatezza delle misure di sicurezza

L'Istituto "Paolo Boselli" verifica periodicamente l'adeguatezza ed efficacia delle misure di sicurezza adottate provvedendo ad adeguare le stesse alla particolare evoluzione tecnologica del settore, al fine di mantenere elevato il livello di protezione e ridurre, quindi, il livello di rischio.
L'attività di verifica viene attuata mediante procedure di *monitoraggio* e di *audit* ed in particolare:
• attraverso un sistema di monitoraggio effettuato da responsabili interni che eseguono un controllo costante dell'effettivo funzionamento del sistema informatico e delle misure di sicurezza, adottando tutte le misure necessarie ad incrementarne il livello di efficacia;

• attraverso la previsione di un'attività di audit, quale controllo saltuario svolto da soggetti *diversi* dai responsabili interni, al fine di ottenere un giudizio imparziale circa la qualità delle misure di sicurezza approntate ed in grado di evidenziarne eventuali debolezze od errori.

Art. 14
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.

Il piano è stato aggiornato a:

- Passaggio dall'Albo cartaceo a quello on-line (Legge 69/2009 art. 32 , come modificata nel 2010)
- Ampliamento dei contenuti obbligatori dei siti web ("Codice dell'Amministrazione Digitale": art. 54 del DLgs 82/2005 come modificato dal DLgs 235/2010)
- Ulteriori contenuti obbligatori del sito web della scuola: (Legge 69/2009 art. 21 , come modificata nel 2010)
- Ulteriori pubblicazioni obbligatorie sul sito web della scuola: (DLgs 150/2009 "ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni." (Capo III -art. 11 , come modificata nel 2010)
- Integrazione all'informativa dei dipendenti - Autorità Garante per la Privacy: Provvedimento di prescrizione <<Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)
- Obbligo di dare un'informativa specifica ai visitatori del sito web: "Linee guida per i siti web della PA - art. 4 della Direttiva 8/09 del Ministro per la pubblica amministrazione e l'innovazione"-26 luglio 2010
- Linee guida del Garante per posta elettronica e internet (Gazzetta Ufficiale n. 58 del 10 marzo 2007) , ora in combinato con la Direttiva n. 2 (26 maggio 2009) emessa dalla Presidenza del Consiglio dei ministri - Dipartimento della Funzione pubblica, avente il seguente oggetto: Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro
- Amministrazione trasparente adempimenti previsti dalla legge 190 del 6 novembre 2012 e dal d.lgs 33 del 14 marzo 2013. In particolare, sul tema della trasparenza amministrativa, l'art. 1, comma 32 della citata legge 190/2012, obbliga tutte le Pubbliche amministrazioni, tra cui le istituzioni scolastiche di ogni ordine e grado, a pubblicare nei propri siti web istituzionali tutti i contratti stipulati nell'anno precedente, ovvero: la struttura proponente; l'oggetto del bando; l'elenco degli operatori invitati a presentare offerte; l'aggiudicatario; l'importo di aggiudicazione; i tempi di completamento dell'opera, servizio o fornitura; l'importo delle somme liquidate.

L'obbligo di eseguire gli adempimenti e le relative scadenze/frequenze di seguito elencate:

Adempimenti annuali

- Aggiornamento del Documento Programmatico sulla Sicurezza (entro il 31 Marzo)
- Riferire nella relazione accompagnatoria del bilancio d'esercizio dell'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza
- Aggiornamento dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati (ove variato, anche parzialmente)
- Verifica della sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati (per l'accesso ai dati utilizzati nelle operazioni di trattamento)
- Verifica dell'operato degli amministratori di dominio
- Aggiornamento del Disciplinare Interno per l'utilizzo della posta elettronica e di Internet
- Pianificazione degli interventi formativi degli incaricati del trattamento
- Aggiornamento dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne eventuali difetti (l'aggiornamento deve essere effettuato con cadenza semestrale in caso di trattamento di dati sensibili o giudiziari).

Adempimenti semestrali

- Aggiornamento dei software antimalware e degli Intrusion Detection System
- Cambio password (trimestrale nel caso di trattamento di dati sensibili e/o giudiziari)

Adempimenti periodici

- Disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi
- Salvataggio dei dati con frequenza almeno settimanale.

Art. 15
Norme per il personale

Tutti i dipendenti (docenti, A.T.A., studenti) 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, dal regolamento di utilizzo della rete e dalla normativa vigente.

Art. 16
Misure di sicurezza suppletive relative al trattamento di particolari dati sensibili

Il presente articolo 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 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 sul 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.

Art. 17
Protezione da malintenzionati

Ogni computer collegato in rete può essere oggetto di tentativi di connessione effettuati da soggetti che utilizzano altri computer collegati alla rete.
Quando il computer è collegato a Internet le intrusioni possono teoricamente essere effettuate da computer connessi a Internet situati in un qualsiasi punto della rete mondiale.
La gestione della sicurezza rispetto a possibili intrusioni esterne viene garantita da un sistema di Firewall/proxy server (gestito internamente) che controlla sia il traffico in ingresso che in uscita attraverso strategie definite di autorizzazioni che impediscono intrusioni dall'esterno.
Per motivi di sicurezza, vengono mantenuti temporaneamente i file log di tutti gli accessi in entrata/uscita al firewall.

Art. 18
Regolamento
amministratore di dominio / amministratore di sistema

In data 24 dicembre 2008 è stato pubblicato sulla Gazzetta Ufficiale n° 300 il provvedimento del Garante della privacy recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008", parzialmente modificato con la comunicazione del Garante del 10/12/2009. Il provvedimento del Garante

serve soprattutto a richiamare l'attenzione "sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare al titolare in caso di incauta o inidonea designazione". E' dunque importante che queste persone godano della fiducia del Dirigente Scolastico. Infatti il provvedimento del Garante richiama l'uso di "criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

I punti principali del provvedimento sono:

1) Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza, gli amministratori di sistemi software complessi e gli amministratori di dominio.

2) Gli amministratori di sistema così ampiamente individuati nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

3) Tra l'altro, lo svolgimento di mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non sempre si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti.

4) Il Codice privacy non ha incluso questa figura tra le proprie definizioni normative (al contrario degli incaricati e del responsabile del trattamento che sono figure tipizzate). Tuttavia le funzioni tipiche dell'amministrazione di un sistema sono richiamate nell'Allegato B del Codice privacy, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione.
Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

5) In relazione a tali attività il Titolare del trattamento (e dunque l'istituzione scolastica attraverso il Dirigente pro tempore) deve adottare opportune cautele, avendo ben presente che si tratta di un incarico a carattere fiduciario da assegnare a persona competente e affidabile. Ci sono, al riguardo, responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare dalla incauta o inidonea designazione.

6) La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche amministratori di sistema e di dominio, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza.

7) Qualora l'attività degli amministratori di sistema e di dominio riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, questi vanno informati attraverso gli strumenti consentiti dal Codice privacy (ad es. informativa ex art. 13 del Codice privacy).

8) L'operato degli amministratori di sistema e di dominio deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti. Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema e di dominio. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
L'attività dell'amministratore di sistema si inquadra in due contesti:

a) **L'attività di ordinaria amministrazione** volta a garantire il normale funzionamento e lo sviluppo dei sistemi amministrati. In tal caso l'amministratore di sistema opera di concerto con l'utente, e comunque coordinandosi in via preventiva con il supervisore della sistema e/o con il gestore del sistema informatico;

b) **La gestione delle emergenze** quando si rilevino condizioni che pongano a rischio immediato la corretta funzionalità dei sistemi o della rete, o la sicurezza dei dati e dei sistemi, l'amministratore di sistema può operare in autonomia e per le vie brevi, qualora l'onere del coordinamento limiti l'efficacia e la tempestività degli interventi.
Immediatamente dopo l'intervento, è tenuto comunque a segnalare per iscritto agli utenti coinvolti e al supervisore della sistema e/o il gestore del sistema informatico i dettagli dell'evenienza occorsa.

L'amministratore di sistema deve avere ragionevole cura:

a) nel prendere precauzioni contro i furti ed i danni ai componenti del sistema;
b) nell'attuare rigorosamente tutti gli accordi di licenza hardware e software applicabili al sistema;
c) nel trattare informazioni riguardanti gli utenti del sistema, nonché le informazioni depositate nel sistema dagli utenti medesimi, in modo appropriato, applicando rigorosamente le norme e le pratiche atte a garantire la sicurezza dei sistemi, delle reti e dei dati. Si fa particolare riferimento al caso di azioni dolose volte a violare l'integrità dei sistemi, dei dati o della privacy (ad es. intrusioni, diffusioni di virus, etc.), ed al caso di incidenti di natura tecnica (ad es. incendio, perdita di dati, etc.);
d) nel diffondere informazioni sui regolamenti e le procedure specifiche che regolano l'accesso e l'uso del sistema, sui servizi forniti e su quelli esplicitamente non forniti. Un documento scritto consegnato agli utenti o messaggi inviati tramite il sistema stesso saranno considerati una notifica adeguata;
e) nel collaborare con il supervisore della sistema e/o con il gestore del sistema informatico per trovare e correggere problemi causati ad altri dall'uso/abuso del proprio sistema. Un amministratore di sistema può temporaneamente interdire l'accesso e l'uso delle risorse informatiche ad un utente se, sulla base di comprovati motivi, lo ritiene necessario per garantire la sicurezza del sistema o della rete.

Se l'amministratore di sistema ha chiare evidenze di cattivo uso delle risorse informatiche che indirizzino ad attività di elaborazione o files di uno specifico individuo, deve attuare uno o più dei seguenti passi, considerati appropriati per la protezione degli altri utenti, della rete e dei sistemi di computer:

1) notificare per iscritto le eventuali indagini al supervisore della sistema e/o al gestore del sistema informatico;
2) adottare tutti i provvedimenti e le azioni ritenute necessarie e/o opportune dai responsabili di cui al punto a), per inibire il propagarsi dei danni alle risorse di rete.

In risposta alle disposizioni del garante a breve sarà installato sulla rete interna dell'istituto un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema e di dominio. Le registrazioni (access log) avranno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni comprenderanno i riferimenti temporali e la descrizione dell'evento che le ha generate e saranno conservate per un congruo periodo, non inferiore ai 6 mesi.
All'amministratore di dominio è riservata la manutenzione dei dati relativi ai servizi attivi sul dominio nel rispetto della normativa vigente.

Art. 19
Regolamento per l'utilizzo del sistema informatico

A) Oggetto e ambito di applicazione
Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica dell'istituto "Paolo Boselli" e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire. Utilizzando le applicazioni della rete informatica dell'istituto l'utente acconsente al monitoraggio delle attività svolte. L'uso delle applicazioni deve essere limitato al solo scopo lavorativo
L'uso non autorizzato delle applicazioni può essere oggetto di sanzioni amministrative e/o penali.

B) Principi generali – diritti e responsabilità

Durante l'utilizzo della rete informatica dell'Istituto e accedendo a Internet dalla stessa vanno sempre rispettate tutte le disposizioni di legge, in particolare la legge n. 547 del 31/12/93 (sui crimini informatici) e il D.Lgs 196/03 (sulla tutela dei dati personali) e s.m.i..
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.
E' vietato modificare la configurazione dei personal computers. E' 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.

L'utilizzo dei servizi della rete è autorizzato solo per scopi didattici.

È vietato danneggiare in qualunque modo l'attrezzatura utilizzata, in particolare è vietato compromettere il funzionamento della rete e degli apparati che la costituiscono con programmi (virus, worm, trojan horses, o simili) costruiti appositamente.

È vietato modificare in qualsiasi modo la configurazione fisica e logica della rete. In particolare:

- è vietato modificare la configurazione TCP/IP degli elaboratori che si utilizzano;
- è possibile collegare alla rete didattica "notebook" personali solo previa autorizzazione dell'amministratore di sistema / rete, che fornirà l'autorizzazione necessaria;
- è vietato collegare alla rete in qualsiasi modo elaboratori personali o altri dispositivi compresi portatili, palmari e simili;
- è vietato l'utilizzo di credenziali altrui di cui si è venuti casualmente o intenzionalmente a conoscenza.
- è vietato comunicare e diffondere i dati personali conosciuti o ai quali si abbia avuto accesso nello svolgimento delle prestazioni lavorative, se non autorizzati dal titolare del trattamento;

Sono vietati comportamenti lesivi dei diritti di altri, quali:

- archiviare, inserire, accedere, diffondere in rete dati personali (e in particolare: informazioni su gusti, opinioni politiche o religiose, fotografie) propri o di terze persone;
- violare la privacy di altri utenti, ad esempio intercettandone la posta elettronica o accedendo senza autorizzazione ai loro files/cartelle;
- violare la sicurezza di archivi e/o computer della rete;
- furto di dati e/o manomissione

Durante l'accesso alla rete Internet si devono rispettare le prescrizioni della cosiddetta "netiquette – il galateo della rete" (allegato 13 del DPS).

In caso di manutenzioni ordinarie o straordinarie, guasti o altri problemi non è garantito il ripristino di tutte e parte delle funzionalità dei sistemi o degli account, né tantomeno il rapido intervento o il preavviso su base personale. Nessun danno diretto o indiretto sarà attribuibile alla perdita di dati o al mancato utilizzo dei servizi abitualmente disponibili. È responsabilità dei singoli utenti il salvataggio del proprio lavoro mediante copia dei file importanti.

L'accesso ai laboratori di informatica non è permesso agli allievi in assenza di un insegnante responsabile o del personale ATA incaricato della sorveglianza. I singoli alunni, possono accedere ai laboratori, esclusivamente per scopi didattici, previa autorizzazione rilasciata dal Dirigente Scolastico o dal Collaboratore Vicario con la presenza di un assistente tecnico.

Qualunque violazione delle modalità sopra indicate viene perseguita, civilmente e penalmente, ai sensi delle norme contenute nel D. L.vo 196/03 e s.m.i.

C) Attività vietate (policy)

E' 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 la rete per le scommesse e per i giochi di azzardo;
- utilizzare la rete con le credenziali di accesso di altri utenti e/o cedere a terzi codici personali (USER NAME e PASSWORD) di accesso al sistema;
- 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 o che ne distraggano 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 database per scopi personali;
- installare, rimuovere, danneggiare componenti hardware;
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare Internet e la posta elettronica per scopi personali e/o inviando e ricevendo materiale che violi le leggi;
- 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, anche in remoto, 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;
- usare la rete a scopo diverso da quello lavorativo;
- inserire nella "rete" dati sensibili e/o dati personali;
- eseguire tentativi di Port Scanning / Brute Force / Denial of Service;
- scaricare e diffondere programmi, file P2P (winmx, kazaa, emule, ecc….) ed utilizzare social network (face book, messanger, net log, ecc…);
- scaricare, diffondere e utilizzare software per il controllo remoto dei pc;
- effettuare copie di backup dei database dei server contenenti dati sensibili;
- caricare sui computer e sulla rete copie di opere dell'ingegno protette . Allo stesso modo, tali opere non possono essere distribuite tramite internet e gli utenti non sono autorizzati ad utilizzare sistemi di file sharing tramite computer di proprietà della scuola.
- divieto di aggirare le regole di sicurezza imposte sugli strumenti informatici e sulle reti di collegamento interne;

- divieto di aggirare gli strumenti informatici di filtro/monitoraggio;
- divieto di alterare e/o modificare documenti informatici aventi efficacia probatoria;
- il divieto della connessione, consultazione, navigazione, streaming ed estrazione mediante downloading, a siti web che siano considerabili illeciti (e quindi, a titolo esemplificativo, giocare in borsa, siti pornografici, siti che presentino contenuti contrari alla morale, alla libertà di culto ed all'ordine pubblico, che consentano la violazione della privacy, che promuovano e/o appoggino movimenti terroristici o sovversivi, riconducibili ad attività di pirateria informatica, ovvero che violino le norme in materia di copyright e di proprietà intellettuale).

Qualunque violazione delle modalità sopra indicate viene perseguita, civilmente e penalmente, ai sensi delle norme contenute nel D. L.vo 196/03 e s.m.i.. .

D) Attività consentite (policy)

E' consentito al supervisore 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 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.

E) 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 del sistema informatico e/o l'amministratore del dominio 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.

F) 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.

G) 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 a procedere a quanto sopra previsto. (delibera del Consiglio di Istituto n. 244 del 28 novembre 2006).

H) 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 BACKUP-NAS;
- divieto di utilizzare floppy disk e/o pen drive 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 (winmx, kazaa, emule, ecc….);
- utilizzare social network (face book, messanger, net log, ecc…)

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 Direttore S.G.A. e l'utilizzo è 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.

I) Virus informatici
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.

L) Responsabilità

Qualunque violazione delle modalità sopra indicate viene perseguita, civilmente e penalmente, ai sensi delle norme contenute nel D. L.vo 196/03 e s.m.i.

M) Utilizzo del registro elettronico da parte dei docenti

Al personale docente sono rilasciate apposite credenziali identificative (login e password) per accedere all'applicativo del registro elettronico. Il personale docente è tenuto ad osservare la politica di gestione delle credenziali, inserita nel Documento Programmatico sulla Sicurezza. L'accesso, effettuato tramite le credenziali, sarà tracciato secondo mediante file log come indicato nel presente Documento Programmatico sulla Sicurezza.

N) Controlli previsti e sanzioni

Nel rispetto della normativa vigente richiamata nelle premesse del presente disciplinare, l'istituzione scolastica non procede a verifiche che possano configurare il controllo a distanza dell'attività dei lavoratori.
L'Amministrazione, in persona del Dirigente Scolastico, si riserva la facoltà di eseguire controlli in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza di reti e sistemi, sia per eseguire verifiche sul corretto utilizzo dei servizi Internet e posta elettronica, in conformità a quanto prescritto dal presente disciplinare, dalla normativa posta a protezione dei dati personali.
I controlli sono posti in essere dal Titolare del trattamento dati coadiuvato dall'amministratore di sistema. Ci si potrà avvalere di personale esterno, appositamente nominato quale responsabile esterno di trattamento, secondo le previsioni del D. Lgs. 196/2003. I controlli sono eseguiti tenendo conto del principio di graduazione (par. 6.1 del Provvedimento del Garante per la Protezione dei Dati Personali 1/3/2007) e procederanno come segue:

a) al verificarsi di comportamenti anomali, il dirigente deve effettuare un controllo anonimo su dati aggregati, riferito all'intera struttura amministrativa oppure a sue aree. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo all'utilizzo anomalo degli strumenti dell'amministrazione e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite ai dipendenti.; in assenza di successive anomalie non si effettueranno controlli su base individuale;

b) in caso di abusi singoli e reiterati si procederà all'invio di avvisi individuali e si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro;

c) in caso di riscontrato e reiterato uso non conforme delle risorse informatiche, verrà attivato il procedimento disciplinare nelle forme e con le modalità di cui al D.lgs. n. 165 del 2001 articoli 55 bis e seguenti.

Fonti di documentazione

Il 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»)"*;*
- Codice dell'amministrazione digitale;
- Direttiva n. 02/09 del 26/05/2009 Dipartimento della Funzione Pubblica;
- Anagrafe degli studenti (DLgs 76/2005 e Ordinanze Ministeriali varie);
- Garante Privacy :"La privacy tra i banchi di scuola"
- Garante Privacy comunicato stampa del 10/12/2009;
- Decreto legge 5/2012 convertito in Legge 35/2012

Torino, 31 marzo 2017 - Prot. 3087/A17

Il Direttore S.G.A.
Paolo Astuti
Responsabile del trattamento dei dati

Il Dirigente Scolastico
prof. Attilio Giaculli
Titolare del trattamento dei dati