Disciplinare per l'utilizzo degli strumenti informatici

Versione 1.0

Scopo del Documento:

Il presente documento ha l'obiettivo di definire i principi generali per il corretto utilizzo degli strumenti informatici.

E. BOGGIO LERA
LICEO SCIENTIFICO STATALE

Sistemi Informatici

L'uso degli strumenti informatici, della posta elettronica e l'accesso ad Internet da parte delle amministrazioni pubbliche si và sempre più diffondendo sotto l'impulso della nuova legislazione, con l'obiettivo di migliorare l'efficienza operativa, contenere i costi e assicurare una maggiore qualità delle prestazioni.

I servizi informativi sono ormai diventati fondamentali anche per gli istituti scolastici che sempre più dovranno utilizzare strumenti come il registro elettronico, la posta elettronica e Internet per fornire servizi all'utenza e per migliorare la propria efficienza.

Pertanto è necessario che siano adottate adeguate e opportune misure organizzative e di sicurezza volte a proteggere la disponibilità e l'integrità delle risorse informative e a tutelare la riservatezza dei dati personali di tutti.

A questo proposito si richiama quanto è riportato anche nelle Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni dell'AGID (Agenzia per l'Italia Digitale):

> *"Tutti i dipendenti dell'Amministrazione sono tenuti a utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che l'ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet, evitando eventi dannosi, anche al fine di non danneggiare l'immagine dell' Amministrazione".*

Dall'esame di diversi reclami, segnalazioni e quesiti pervenuti, il Garante per la protezione dei dati personali ha preso atto dell'esigenza di prescrivere ai datori di lavoro pubblici e privati alcune misure, necessarie o opportune, per conformare alle vigenti disposizioni in materia di Privacy il trattamento di dati personali effettuato per verificare il corretto utilizzo, nel rapporto di lavoro, della Posta elettronica e di Internet.

A tale scopo è stato emanato il provvedimento generale pubblicato sul Bollettino n. 81 del Marzo 2007 e, successivamente, sulla Gazzetta Ufficiale – Serie generale n. 58 del 10.03.2007 (di seguito "il Provvedimento").

Con il presente disciplinare si fornisce concreto riscontro alle prescrizioni del Garante e si conforma a quanto previsto nelle conclusioni del Provvedimento, al punto 2), lett. a).

Principi

Il presente disciplinare è predisposto nel rispetto della vigente disciplina in materia di Privacy, con riguardo, in particolare, alle norme del D. Lgs. 196/03 (Codice in materia di protezione dei dati personali) che disciplina il trattamento effettuato dai soggetti pubblici.

L'Istituto Scolastico garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo della posta elettronica e di Internet, si conforma ai seguenti principi:

a. principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2 del Provvedimento);

b. principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, c. 1, lett. a, del Codice) poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori (par. 3 del Provvedimento);

c. principio di pertinenza e non eccedenza (par. 6 del Provvedimento), in virtù del quale:

- i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, c. 1, lett. b del Codice; par. 4 e 5 del Provvedimento);
- il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile";
- le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8 del Provvedimento) ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001, punti 5 e 12).

Sommario

1. Generalità

1.1 Principali riferimenti

Rif. Identificativo
Testo Unico sulla Privacy, Codice in materia di protezione dei dati personali, D. Lgs. 196/2003
Provvedimento del Garante dell'1 marzo 2007, "Linee guida del Garante per posta elettronica e internet", pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007, bollettino n. 81/marzo 2007, cod. doc. web. N. 1387522.
Direttiva n. 2/2009 della Presidenza del consiglio dei Ministri concernente l'utilizzo d'internet e della casella di posta elettronica istituzionale sul luogo di lavoro.
Legge 18 agosto 2000, n. 248 "Nuove norme di tutela del diritto d'autore".
Legge 23 dicembre 1993 n. 547 "Modificazioni e integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica."

2. Introduzione

Il presente documento stabilisce i principi generali per il corretto utilizzo degli strumenti informatici dell'Istituto scolastico al fine di tutelare il sistema informatico dello stesso.

In particolare, definisce:

- i ruoli e le responsabilità delle figure dell'Istituto scolastico coinvolte nel processo di gestione dei servizi informatici;
- le raccomandazioni generali e le regole comportamentali cui devono attenersi gli utenti, al fine di garantire l'utilizzo in sicurezza dei servizi informatici e degli strumenti in coerenza con la politica dell'Istituto scolastico e con le norme di legge attualmente in vigore (a es, D.Lgs. 196/2003, Provvedimento del Garante dell'1 marzo 2007, Direttiva n. 2/2009 della Presidenza del consiglio dei Ministri relativa all'utilizzo d'internet e della casella di posta elettronica istituzionale sul luogo di lavoro, Crimine Informatico L. 547/1993, Tutela del diritto d'autore L. 248/2000); in questa ottica, il presente documento si pone anche come strumento per la prevenzione degli illeciti derivanti dall'utilizzo improprio dei servizi informatici da parte degli utenti;
- le attività di monitoraggio e di tracciamento dei servizi di navigazione Internet del personale della scuola e degli alunni, in conformità con le indicazioni del Garante stabilite nel Provvedimento Generale dell'1 marzo 2007, "Linee guida del Garante per posta elettronica e internet".

3. Campo di applicazione

I contenuti di questo documento si applicano a tutti i lavoratori dell'Istituto agli studenti e, in generale, a tutti coloro che, in virtù di un rapporto di lavoro o fornitura (per esempio, consulenti, formatori, di seguito denominati utenti esterni), gestiscono e utilizzano gli strumenti informatici forniti dall'Istituto.

Ogni nuovo contratto di fornitura di servizi, dovrà richiedere l'osservanza delle disposizioni enunciate nel presente documento.

I responsabili della conduzione di contratti di servizi informatici in cui sono previste risorse umane esterne, hanno la responsabilità di notificare il presente disciplinare e far adottare le norme comportamentali in esso contenute da parte dei fornitori coinvolti.

4. Ruoli e Responsabilità

4.1 Gestione Sistemi Informatici e Tecnologici

DEFINIZIONI E RESPONSABILITÀ

AMMINISTRATORE DI SISTEMA: soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo dei server d'istituto o del sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera d'incarico.

RESPONSABILI TECNICI DEI LABORATORI INFORMATICI: soggetti cui sono conferiti il compiti di sovrintendere alle risorse del sistema operativo di un elaboratore. Sono amministratori delle postazioni a loro affidate.

TITOLARE: il titolare del trattamento è l'Ente (ISTITUTO SCOLASTICO) e la titolarità è esercitata dal rappresentante legale (DIRIGENTE SCOLASTICO).
I compiti che la legge gli assegna e che non sono delegabili sono: la vigilanza sul rispetto da parte dei Responsabili dei compiti assegnati, nonché la puntuale osservanza delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

TITOLARE, RESPONSABILI, INCARICATI

- **Titolare del trattamento**: DIRIGENTE SCOLASTICO dell' Liceo Scientifico Statale "Boggio Lera" - Prof.ssa Lo Bianco Maria Giuseppa
- **Custode delle password:** DSGA dott.ssa Antonia Musmeci (vedi nomina)
- **Amministratore di sistema e responsabile della sicurezza informatica (rete di segreteria e rete didattica):** Ass tecnico Bisicchia Stefano (vedi nomina)
- **Responsabile tecnico del laboratorio di Lingue - Centrale**: Ass tecnico Di Stefano Carmelo
- **Responsabile tecnico del laboratorio Multimediale - Centrale:** Ass tecnico Sapienza Francesco
- **Responsabile tecnico del laboratorio d'Informatica - Centrale:** Ass tecnico Melarosa Salvatore
- **Responsabile tecnico del laboratorio d' Informatica e Lingue –** Grassi: Ass tecnico Zuccarello Paolo
- **Responsabile tecnico del laboratorio d' Informatica -Teatro Greco**: Ass tecnico Stefano Bisicchia
- **Responsabili dei portatili, LIM e postazioni alternative ai laboratori** –vedi nomina.

Sito web:

- **Web editor:** Prof.ssa Lo Bianco Maria Giuseppa
- **Web master:** Ass. tec. Stefano Bisicchia
- **Web editor con credenziali amministrative:** Prof.ssa Lina Lo Presti
- **Web editor:** Prof. Alfredo Motta

Obiettivi

Il Dirigente Scolastico ha adottato il suddetto modello tecnico-organizzativo per la gestione del sistema informatico dell' Istituto definendo i criteri e gli aspetti relativi alla sicurezza inerenti ai servizi informatici dell'Istituto.

Inoltre, definisce con i membri della commissione informatica le procedure organizzative e/o operative che disciplinano i servizi informatici dell'Istituto.

L'istituto sarà dotato di un sistema che permetterà di:

- definire le politiche di URL Filtering, identificando le categorie di siti Internet il cui accesso sarà bloccato perché contrari alla legge, all'ordine pubblico, al buon costume, all'etica dell'Istituto;
- analizzare, in forma aggregata ed anonima, i log di sicurezza e di individuare le possibili contromisure per risolvere eventuali minacce alla sicurezza;
- fornire indicazioni al fine di stabilire il limite massimo dello spazio riservato alle cartelle personali sul server;
- provvedere all'attività di installazione ed attivazione di software antivirus, a protezione delle postazioni di lavoro degli utenti, conformi allo standard dell'Istituto;
- definire i processi di creazione, abilitazione, modifica, disattivazione, ripristino e cessazione degli account di accesso ai servizi informatici.

Utente

L'utente è responsabile delle credenziali a lui assegnate e di tutte le attività che svolge attraverso l'utilizzo degli strumenti informatici.

In particolare, l'utente è personalmente responsabile del rispetto del presente disciplinare.

Ogni violazione o comportamento non conforme alle regole indicate, laddove ne ricorrano le condizioni, oltre ad essere rilevante sul piano della responsabilità civile e penale, è valutato ai fini disciplinari.

L'utente è tenuto a contattare l' amministratore di sistema nei seguenti casi:

- se ritiene che su una o più postazioni di lavoro siano state apportate delle modifiche non autorizzate alla configurazione standard;
- se ritiene che siano state violate le password di accesso ai sistemi o alle applicazioni;
- se ha ricevuto e-mail sospette (tentativi di phishing) sull'account di posta elettronica;
- se l'account di posta elettronica è oggetto di molteplici e-mail non desiderate e ricevute in maniera ricorrente (spamming) non filtrate dal sistema di sicurezza antispam;
- se ritiene di essere stato vittima di un furto di informazioni relativi ai dati dell'istituto;
- se sia stata riscontrata una qualsiasi altra violazione alle politiche di sicurezza.

5. Regole per l'utilizzo dei sistemi informatici

Tutti i sistemi informatici (personal computer, notebook, tablet, ecc.) ed i relativi programmi e/o applicazioni affidati dall'Istituto agli utenti, sono considerati strumenti di lavoro. L'uso è quindi consentito per scopi attinenti l'attività lavorativa e di studio ed in relazione alle funzioni assegnate.

Al fine di tutelare la sicurezza del patrimonio informativo dell'Istituto, il dipendente è tenuto a rispettare le raccomandazioni e le regole comportamentali definite nel presente disciplinare.

L'Istituto scolastico, tramite l' amministratore di sistema e i responsabili tecnici, svolgerà sulle postazioni di lavoro tutte le attività necessarie a verificare le impostazioni di sicurezza applicate ed il rispetto delle politiche dell'Istituto.

5.1 Utilizzo della Postazione di lavoro

Gli utenti, autorizzati ad accedere al Sistema Informatico dell'Istituto, devono utilizzare le postazioni di lavoro per scopi professionali e/o di studio ed in relazione alle funzioni assegnate.

Al fine di non compromettere le funzionalità ed il livello di sicurezza della postazione di lavoro, non è consentita l'installazione e la rimozione di hardware o software, né la modifica delle configurazioni impostate (ad es. parametri di rete, configurazioni di sistema, ecc.), se non espressamente autorizzate dall' amministratore di rete.

I supporti di memoria rimovibili (compact disk, chiavi USB, hard disk esterni, ecc.) contenenti dati sensibili o giudiziari devono essere conservati in luoghi protetti (ad esempio, armadi e cassettiere chiusi a chiave). I dati in essi contenuti devono essere cancellati, quando non sono più necessari o, nel caso non fosse possibile cancellarli, i supporti devono essere distrutti.

In caso di furto o smarrimento di risorse informatiche dell'Istituto, l'utente deve tempestivamente darne comunicazione al responsabile della struttura e all'amministratore di sistema.

Senza una specifica autorizzazione, l'utente non deve utilizzare modem, chiavette USB di connessione ad Internet o dispositivi affini che consentono la connessione diretta della postazione di lavoro a reti esterne pubbliche (Internet) o private (sistemi di altre società), ivi incluso il collegamento tramite telefoni cellulari o in genere dispositivi wireless (ad es. router wireless, access point, ecc..). In nessun caso il modem ed i dispositivi affini possono essere utilizzati quando la postazione di lavoro è collegata contemporaneamente alla rete dell'Istituto.

Compatibilmente con la logistica del luogo di lavoro il monitor delle postazioni di lavoro dovrà essere posizionato in modo che non sia possibile, se non per il suo utilizzatore, leggere le informazioni visualizzate. Qualora il monitor sia ubicato a ridosso di finestre o presso gli sportelli aperti al pubblico è necessario verificarne l'orientamento al fine di garantire la riservatezza delle informazioni.

5.2 Utilizzo della posta elettronica

5.2.1 Raccomandazioni generali

Pur essendo consentito l'acceso web a caselle di posta personali private, i dipendenti sono tenuti ad evitare il download di allegati che possono essere veicolo di virus o di elementi dannosi per l'integrità del sistema informativo.

5.2.2 Comportamenti non permessi

Al fine di garantire il corretto utilizzo della posta elettronica, all'utente non è consentito di:

- inviare o archiviare sul server o sulla propria postazione di lavoro messaggi ed allegati in violazione di norme di legge. A titolo esemplificativo, e non esaustivo, non sono consentiti:
  - il mailing di massa, non autorizzato, di qualunque contenuto (per esempio " Catene di S. Antonio");
  - l'invio di software, file musicali, video ed in generale di qualsiasi tipologia di materiale protetto dalle norme sul diritto d'autore;
  - i messaggi e gli allegati dal contenuto contrario a norme di legge, all'ordine pubblico o al buon costume;
  - l'uso improprio del servizio, mediante l'adozione di strumenti atti a mascherare la propria identità;
- inviare od archiviare sul server o sulla propria postazione di lavoro, messaggi ed allegati contenenti informazioni riservate dell'Istituto, con particolare riferimento a:
  - password ed altri codici di accesso ai sistemi informatici dell'Istituto;
  - documenti dell'Istituto, se non nel caso in cui ciò sia necessario in ragione delle funzioni svolte;
- inviare messaggi destinati direttamente (A/To) e/o per conoscenza (CC/CCn) ad un elevato numero di utenti, se non necessario, in quanto questo può richiedere eccessive capacità elaborative e di occupazione delle risorse di rete con il conseguente rallentamento del servizio;
- esprimersi in nome e per conto dell'Istituto, senza la preventiva autorizzazione. In assenza dell'autorizzazione, l'utente deve indicare che il contenuto della comunicazione rappresenta solo la propria posizione personale;
- diffondere notizie a carattere riservato ed inviare documenti di lavoro ad indirizzi di posta elettronica, se non necessario per l'attività lavorativa.

5.3 Accesso ad Internet

5.3.1 Raccomandazioni generali

La connessione ad Internet è resa disponibile da parte dell'Istituto ai fini dello svolgimento dell'attività lavorativa e di studio. E' tuttavia tollerato l'utilizzo della navigazione Internet per finalità non direttamente correlate alla prestazione lavorativa, purché ciò avvenga per una durata limitata e tale da non incidere sulla propria prestazione lavorativa e, comunque, in modo da non mettere a repentaglio la

disponibilità, l'integrità e la riservatezza dei dati e del sistema informatico dell'Istituto, ovvero, provocare per lo stesso un danno di immagine.

Ciò comporta che, fermo restando il rispetto delle disposizioni di legge in materia, dell'etica dell'Istituto, degli obblighi di riservatezza e degli standard previsti da specifiche normative interne, l'utente non può utilizzare l'accesso ad Internet per motivi personali, se non in maniera breve ed occasionale e, comunque, con modalità che non arrechino intralcio/rallentamento alla normale attività lavorativa propria e di terzi.

All'utente del servizio Internet è richiesto di attenersi alle seguenti indicazioni:

- porre la massima attenzione al fine di evitare che, anche a propria insaputa, il sistema informatico sia attaccato da programmi idonei, o potenzialmente idonei, a danneggiarlo (per esempio, virus e trojan horses);
- dare comunicazione immediata all' amministratore di sistema, di eventi sospetti o di comportamenti anomali nel funzionamento del servizio di accesso ad Internet o di altri problemi di sicurezza che dovessero sorgere in connessione alla propria attività di navigazione su Internet.

5.3.2 Comportamenti non permessi

Al fine di garantire il corretto utilizzo del servizio Internet, all'utente, salvo casi espressamente autorizzati, non è consentito:

- utilizzare modem o altri dispositivi per effettuare connessioni ad Internet o ad altre reti informatiche esterne da postazioni collegate alla rete dell'Istituto;
- collegarsi con reti Wireless ad eccezione di quelle autorizzate dall'Istituto;
- utilizzare collegamenti speciali (VPN o tunnelling) o comunque tecniche per trasmettere dati privati attraverso Internet nel tentativo di eludere i sistemi protezione.
- memorizzare le password di accesso ai siti Web attraverso le funzioni automatiche offerte dai software di navigazione. Le password non devono essere salvate nella cache ma digitate ogni volta che sono richieste;
- scaricare da Internet sulla propria Postazione di lavoro:
    - software, file e qualsiasi tipologia di materiale multimediale che viola o per mezzo dei quali possono essere violati diritti d'autore;
    - file di qualsiasi genere di dimensioni eccessive, in quanto questo può provocare un traffico di rete elevato ed un conseguente rallentamento del servizio;
- visitare siti e/o memorizzare documenti che abbiano un contenuto contrario a norme di legge, all'ordine pubblico e al buon costume.
- accedere attraverso le infrastrutture dell'Istituto, a qualsivoglia gruppo di discussione, forum, o conferenza in rete se non espressamente autorizzati e finalizzati allo svolgimento di attività lavorative per l'Istituto;
- esprimere opinioni su Internet, utilizzando il nome ed i dati dell'Istituto ed utilizzando il dominio registrato dallo stesso, se non espressamente autorizzati.

5.3.3 Regole generali per l'accesso ad Internet

L'accesso ad Internet è consentito solo:

- ai dipendenti e agli studenti dell'Istituto;

- al personale esterno che frequenta la scuola per motivi di formazione.

Per recepire le indicazioni del Garante, l'Istituto attiverà meccanismi automatici di blocco di accesso ai siti Internet i cui contenuti non sono conformi al presente disciplinare. Possono altresì essere bloccati particolari contenuti multimediali quali file musicali, video o altri, che potrebbero violare le norme sul diritto di autore.

L'Istituto si riserva di stabilire le categorie di siti non permessi, il cui accesso viene automaticamente bloccato. A titolo di esempio, si riporta un elenco non esaustivo di alcune categorie di siti non permessi:

- siti contenenti materiale pornografico;
- siti di messaggistica online;
- siti di scommesse e giochi online;
- siti che trattano temi di pirateria informatica;
- ecc..

Tutte le comunicazioni con la rete Internet saranno sottoposte al controllo da parte di strumenti di protezione perimetrale e di monitoraggio delle attività, tali strumenti producono delle registrazioni (file di log) secondo le modalità e per le finalità già descritte.

5.4 Utilizzo del software

La legge n. 248/2000 "Nuove norme di tutela del diritto d'autore" prevede restrizioni molto severe relativamente all'utilizzo del software.

La duplicazione o l'uso non autorizzato di programmi software coperti da copyright è illegale e può esporre, chi commette l'illecito e l'Istituto stesso, ad una responsabilità civile e penale.

Per tale motivo, gli utenti non possono:

- utilizzare e duplicare software senza il possesso di una licenza d'uso;
- installare software gratuiti (freeware o shareware), se non con preventiva autorizzazione da parte l'amministratore di rete.

5.5 Protezione della sessione di lavoro

Al fine di impedire accessi non autorizzati alle risorse informatiche dell'Istituto, gli utenti non devono lasciare incustodita ed accessibile la propria Postazione di lavoro. A tale scopo è necessario adottare le seguenti misure:

- al termine dell'attività è importante chiudere la sessione di lavoro ed arrestare il sistema per impedire l'eventuale utilizzo improprio da parte di terzi della postazione stessa;
- non devono essere disattivati i previsti meccanismi automatici di "blocco del computer" (screensaver con password);
- in caso di abbandono temporaneo della sessione di lavoro, deve essere attivata la funzione di "blocca computer" (comando: CTRL+ALT-CANC).

5.6 Protezione antivirus

Ogni Postazione di lavoro dell'Istituto è dotata di un software antivirus in grado di aggiornarsi automaticamente ed eseguire un controllo dei file presenti sulla postazione e di quelli allegati ai messaggi di posta elettronica. Ove non sia possibile effettuare tali operazioni in modo automatico (ad es. notebook), sarà cura degli utenti effettuare autonomamente (con cadenza almeno settimanale), l'aggiornamento del software antivirus ed il controllo dei file archiviati sulla postazione.

Per minimizzare il rischio di infezione da virus, gli utenti dovranno evitare comportamenti considerati a rischio ed in particolare:

- è vietato disabilitare il controllo antivirus presente sulle Postazioni di lavoro;
- nel caso in cui il software antivirus rilevi la presenza di un virus e segnali di non essere riuscito a rimuovere l'infezione, l'utente dovrà immediatamente interrompere qualsiasi attività e segnalare l'incidente all' amministratore di rete;
- ogni dispositivo esterno di memorizzazione, (ad esempio CD o DVD, chiavi USB, dischi esterni), dovrà essere verificato mediante il programma antivirus prima del suo utilizzo. In caso di rilevazione di virus il supporto dovrà essere rimosso immediatamente.

5.7 Accesso al sistema informativo

L'accesso ai servizi del sistema informativo è consentito solo attraverso un sistema di identificazione ed autenticazione basato su credenziali di accesso che possono essere costituite da una nome utente e password.

5.8 Monitoraggio delle attività

Al fine esclusivo di difendere il suo patrimonio informativo, l'Istituto può adottare misure tecniche idonee a prevenire e rilevare usi illeciti o abusi dei servizi informatici. A questo scopo l'Istituto predisporrà la registrazione delle attività degli utenti (file di Log) in modalità conforme alle disposizioni di legge e salvaguardando i diritti degli utenti.

5.8.1 Trattamento dei file di Log

I file di log sono utilizzati per le seguenti finalità:

a) per finalità di sicurezza informatica, allo scopo di ricercare ed individuare eventuali agenti automatici malevoli (ad es. virus, worm, trojan), presenti sulla rete interna dell'Istituto o per prevenire potenziali minacce informatiche (siti di phishing, truffe informatiche ai danni del dipendente o dell'Istituto, ecc.);
b) per risalire all'autore di accessi Internet o e-mail inviate per esclusive finalità legate alla repressione di reati e su richiesta da parte dell'Autorità Giudiziaria;
c) per la risoluzione di problemi tecnici legati all'utilizzo degli strumenti informatici dell'Istituto;
d) per l'identificazione di eventuali comportamenti non consentiti attraverso strumenti automatici di monitoraggio ed analisi dei log;
e) per il monitoraggio prestazionale e funzionale dei servizi informatici a disposizione degli utenti;
f) per analisi statistiche, in forma aggregata ed anonima, senza associazione esplicita fra l'utente e i dati di traffico;

Con particolare riferimento ai log di navigazione internet, l'analisi dei log per l'identificazione di eventuali comportamenti non consentiti e l'analisi statistica (per esempio, i siti Web più visitati, i file scaricati, la banda di connessione utilizzata, il numero di pagine visitate, ecc.) verrà condotta attraverso log anonimizzati o aggregati senza associazione esplicita fra l'utente e i dati di traffico, in modo da precludere l'identificazione degli utenti stessi. A fronte dell'accertata esistenza di violazioni potranno essere condotti controlli più circoscritti fino all'individuazione del soggetto autore della violazione.

Il trattamento dei dati di log è consentito esclusivamente a personale espressamente autorizzato (amministratore di sistema). Ai fini del monitoraggio dei servizi non è comunque consentito ad alcuno, ivi inclusi i soggetti appena citati, di prendere visione del contenuto dei messaggi di posta elettronica, degli allegati e delle pagine Web accedute.

L'Istituto, a fronte di anomalie o presunti incidenti di sicurezza, può adottare misure straordinarie, per la verifica di eventuali comportamenti anomali. Tali misure saranno effettuate sempre nel rispetto dei principi di pertinenza e non eccedenza. Le attività saranno svolte solo da soggetti autorizzati e nel rispetto della normativa sulla protezione dei dati personali e del principio di segretezza della corrispondenza.

5.8.2 Conservazione dei file di Log

In conformità con le direttive del Garante, la configurazione dei sistemi informatici prevede la cancellazione periodica ed automatica dei file di log (per esempio mediante meccanismi di sovrascrittura come la rotazione dei file di log) contenenti dati personali relativi agli accessi ad Internet , la cui conservazione non sia necessaria. Allo scadere del periodo di conservazione i log sono cancellati in via definitiva fatta salva la possibilità di conservarne aggregati statistici che non possano in alcun modo ricondurre all'identità dell'utente.

In generale, i dati di log sono conservati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Con particolare riferimento ai log di navigazione internet in formato completo, la loro conservazione avviene in formato crittografato e per un periodo non superiore a sei mesi. I log di navigazione Internet in formato anonimo, prodotti per le finalità precedentemente rappresentate, sono conservati in chiaro sul sistema di *reporting* dell'infrastruttura *proxy.* I log anonimi sono privati dell'informazione sull'utenza utilizzata e della parte più significativa dell'indirizzo IP (ultimo ottetto x.x.x.0) e sono conservati per un periodo non superiore ai sei mesi.

5.8.3 UTILIZZO DELLE CASELLE ISTITUZIONALI DI LAVORO

Le caselle istituzionali sono gestite dagli incaricati in base ai compiti loro assegnati. In caso di assenza dell'incaricato abituale, questo potrà essere sostituito da altro personale, in base all'organizzazione interna del lavoro disposta dal D.S. o D.S.G.A., tali caselle devono essere utilizzate solo a scopo lavorativo e NON devono essere utilizzate come caselle personali.

Oltre alle disposizioni impartite per l'utilizzo delle caselle personali, si aggiungono le seguenti disposizioni:

- Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,....). In caso di dubbio consultare un tecnico.
- Nel caso in cui si debba inviare un documento all'esterno dell'Istituto, se non specificamente destinato alla modifica, è preferibile utilizzare il formato *.pdf.
- Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar,...)
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

Misure di tipo tecnologico connesse all'uso di Internet

L'Istituto Scolastico intende limitare nel maggior grado possibile i controlli sulla navigazione (che potrebbero determinare il trattamento di informazioni personali o sensibili anche non pertinenti l'amministrazione).
Per tale motivo è fondamentale il rispetto delle disposizioni elencate, che hanno il fine di ridurre il rischio di usi impropri della "navigazione".

1. Al personale non è consentito:
   - servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
   - utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting social network o similari (salvo specifiche attività espressamente autorizzate per le finalità istituzionali).
   - Utilizzare sistemi Social Network quali twitter, facebook, etc.
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (attenzione nell'aprire mail e relativi allegati, non navigare su siti poco professionali, ecc..)
3. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus, segnalando ogni eventuale problema all'amministratore di sistema.

Si ricorda poi che scaricare file audio e video (o comunque grandi quantità di dati) è in grado di degradare le prestazioni offerte dal servizio agli altri utenti: per tale motivo ciò può avvenire solo se necessario e, possibilmente, al di fuori dei momenti "di punta" a livello di Istituto.

Trattamenti esclusi

L'Istituto Scolastico non effettua controlli prolungati, costanti o indiscriminati dell'uso dei servizi Internet da parte dei dipendenti.

L'Istituto Scolastico non effettua trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori attraverso:

- lettura e registrazione sistematica dei messaggi di posta elettronica personali dei dipendenti o dei relativi dati esteriori;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto.

Graduazione dei controlli e possibili provvedimenti

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Dirigente Scolastico può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Per quanto possibile, sarà preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti d'Istituto e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti al settore in cui è stata rilevata l'anomalia.

La presenza di successive anomalie potrà comportare controlli su base individuale. Il personale deve inoltre attenersi alle disposizioni in materia di sicurezza e a quanto disposto con il disciplinare.

La violazione delle disposizioni riportate nel presente disciplinare può comportare l'applicazione delle sanzioni disciplinari previste dalle vigenti norme e Contratti di Lavoro.

Rimane ferma ogni ulteriore forma di responsabilità civile e penale, quali ad es.:

- violazione della privacy e della tutela dell'immagine;
- diffamazione;
- accesso abusivo ad un sistema informatico e telematico;
- violazione della legge sul copyright.

Registro elettronico

Nell'ambito del gruppo di lavoro è attiva una struttura funzionale quale punto di contatto per la gestione dei problemi inerenti all'utilizzo e più in generale a possibile anomalie.

Il gruppo è quindi tenuto a ricevere, analizzare e gestire le segnalazioni ricevute per sospette violazioni di sicurezza o malfunzionamenti ed è contattabile tramite i seguenti riferimenti:

Dirigente scolastico

-Gestione generale-

Bisicchia Stefano

– Accesso alla rete d'istituto – Rilascio dei vaucher – Configurazione tablet – installazione Argo DidUp- Piattaforma classi virtuali- Classi 2.0

Distefano Carmelo

Consegna tablet sede centrale e Teatro Greco, gestione guasti software/hardware tablet e supporto alla configurazione.

Zuccarello Paolo

Consegna tablet sede Grassi, gestione guasti software/hardware tablet e supporto alla configurazione.

Leanza Angelo

Supervisione e gestione Scuolanext/ArgoDidUp, rilascio password di accesso a Scuolanext/ArgoDidUp, associazione dei docenti alle classi, autorizzazione genitori.

Longo Francesco

Rilascio password di accesso a Scuolanext/ArgoDidUp.

Prof.ssa Carmela Lo Presti
Rilascio password di accesso a Scuolanext/ArgoDidUp, comunicazione alle famiglie, gestione ingressi/uscite, giustificazioni.

Aggiornamento periodico

Il presente regolamento è aggiornato con cadenza almeno annuale o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali dei lavoratori, e portato a conoscenza di tutti i lavoratori mediante affissione all'albo dell'istituto e pubblicazione nel sito internet.

5.9 Supporto tecnico

Di seguito si riepilogano le figure di riferimento citate nel presente documento.

Riferimento	Da utilizzare per:	Modalità di contatto
Amministratore di rete amministrativa/didattica. **Gestione Wi-Fi** **A.P.M. rete GARR** Sig. Bisicchia Stefano	Sospette violazioni di sicurezza quali ad esempio: - tentativi di phishing; - spamming; - furto o alterazione di informazioni dell'Istituto; - modifiche non autorizzate alla configurazione delle postazioni di lavoro; - violazione delle password di accesso	**Email:** stefanobisicchia@live.it

	ai sistemi o alle applicazioni; - qualsiasi altra violazione alle politiche di sicurezza.	
Responsabile Tecnico sede centrale: **Laboratorio linguistico** Sig. Di Stefano Carmelo	Segnalazioni ed allarmi generati dall'antivirus. Guasto tecnico Supporto per la gestione della postazione di lavoro e autorizzazione all'installazione di software. Problematiche di posta elettronica.	**Email:** cdistefano@ymail.com
Responsabile Tecnico sede centrale: **Laboratorio Multimediale** Sig. Sapienza Francesco	Segnalazioni ed allarmi generati dall'antivirus. Guasto tecnico Supporto per la gestione della postazione di lavoro e autorizzazione all'installazione di software. Problematiche di posta elettronica.	**Email:**
Responsabile Tecnico sede centrale: **Laboratorio Informatica** Sig. Melarosa Salvatore	Segnalazioni ed allarmi generati dall'antivirus. Guasto tecnico Supporto per la gestione della postazione di lavoro e autorizzazione all'installazione di software. Problematiche di posta elettronica.	**Email:** melarosa56@hotmail.it
Responsabile Tecnico Grassi **Laboratorio Multimediale/Linguistico/Lim** Sig. Zuccarello Paolo	Segnalazioni ed allarmi generati dall'antivirus. Guasto tecnico Supporto per la gestione della postazione di lavoro e autorizzazione all'installazione di software. Problematiche di posta elettronica.	**Email:** jonia_ten@yahoo.it
Responsabile Tecnico sede Teatro Greco: **Laboratorio Multimediale/Lim** Sig. Stefano Bisicchia	Segnalazioni ed allarmi generati dall'antivirus. Guasto tecnico Supporto per la gestione della postazione di lavoro e autorizzazione all'installazione di software. Problematiche di posta elettronica.	**Email:** stefanobisicchia@live.it

Lim e postazioni distribuite. **Da definire:**		

Si allega al documento, come parte integrante:

- policy sottoscritta con la **rete GARR Prot. n. U/424-15/CG**
- policy servizi Argo

Data **Il Dirigente Scolastico**