DELIBERA CONSIGLIO DI ISTITUTO DEL 11/06/2020 N. 284

REGOLAMENTO SERVIZI INTERNET E POSTA ELETTRONICA

Visto il Codice dell'Amministrazione Digitale, D.Lgs. 7 marzo 2005, n. 82, modificato e integrato dal decreto legislativo 22 agosto 2016 n. 179 e dal decreto legislativo 13 dicembre 2017 n. 217;

Viste le Direttive impartite in materia dal Ministero per la Pubblica Amministrazione e l'Innovazione;

Visto il Codice in materia di protezione dati personali (D.Lgs 196/2003) e sue ss. mm.ii.;

Viste le Linee Guida del garante per internet e posta elettronica (Provvedimento n. 13 del 1° marzo 2007);

Visto il Regolamento UE 2016/679 (G.D.P.R.);

Ritenuto opportuno richiamare gli artt. 2086, 2087 e 2014 del Codice Civile;

Considerato, inoltre, che, se correttamente applicato e fatto rispettare, il regolamento può risultare un efficace strumento della Policy scolastica anche al fine di limitare il rischio di insorgenza di responsabilità amministrativa della Scuola;

Tenuto conto che il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, a tutti i collaboratori della scuola, interni od esterni, ai collaboratori a progetto ed a quelli durante il periodo di stage, a prescindere dal rapporto contrattuale con la stessa intrattenuto, nonché agli alunni;

Ritenuto, pertanto, di dover adottare apposito regolamento per l'utilizzo di Internet e della Posta Elettronica viene disposto il seguente

Disciplinare per l'utilizzo della strumentazione, della rete internet e della posta elettronica

Il presente Regolamento disciplina le modalità di accesso e di uso delle strumentazioni, della Rete Informatica, telematica e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Istituto per dare il supporto informativo documentario alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuole ed enti, nonché per tutti gli adempimenti amministrativi di legge.

Si conforma ai seguenti principi:

- di necessità**,** secondo cui i sistemi e i programmi informativi devono essere configurati riducendo al minimo l'utilizzo di dati personali e identificativi in relazione alle finalità perseguite,

- di correttezza**,** secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori al fine di evitare trattamenti aggiuntivi rispetto a quelli connessi ordinariamente all'attività lavorativa all'insaputa dei lavoratori,

- di pertinenza e non eccedenza**,** in virtu' del quale, i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime e nella misura meno invasiva possibile e le attività di monitoraggio devono essere svolte da soggetti preposti.

DEFINIZIONI

- **POSTAZIONE DI LAVORO:** Personal Computer, PC portatile, Tablet collegato alla rete informatica dell'Istituto tramite il quale l'utente accede ai servizi informatici.

- **UTENTE DI POSTA ELETTRONICA:** persona autorizzata ad accedere al servizio di posta elettronica.

- **UTENTE INTERNET:** persona autorizzata ad accedere al servizio Internet.

- **LOG:** archivio delle attività effettuate in rete dall'utente.

- **INTERNET PROVIDER:** azienda che fornisce alla scuola il canale d'accesso alla rete Internet.

- **CREDENZIALI DI AUTENTICAZIONE:** codice utente e password richieste dal sistema o dalla postazione di lavoro per verificare se l'utente è autorizzato ad accedere e con quali modalità.

- **WHITE LIST:** elenco di siti che l'Ente ritiene comunemente attinenti all'attività lavorativa.

- **BLACK LIST:** elenco di siti che presentano contenuti non attinenti all'attività lavorativa.

- **TRATTAMENTO:** costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

- **TITOLARE DEL TRATTAMENTO:** persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione ed organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nel presente contesto, Titolare del trattamento risulta essere il Dirigente Scolastico Dott. Germano Cipolletta in qualità di legale rappresentante dell'Istituto.

- **RESPONSABILE DEL TRATTAMENTO:** persona fisica, giuridica, PA e qualsiasi altro ente, associazione, od organismo designati facoltativamente dal titolare al trattamento dei dati personali.

- **INCARICATO DEL TRATTAMENTO:** persona fisica autorizzata da titolare o dal responsabile a compiere operazioni di trattamento di dati personali.

§§§§§§§§§§§§§§§§§§

Valutazione del rischio

La rete informatica di Istituto, l'accesso alla rete internet e alla posta elettronica, la strumentazione affidata al dipendente sono strumenti di lavoro; su di essi vengono effettuate regolari attività di controllo, amministrazione e back up ed essi non possono in alcun modo essere utilizzati per scopi diversi poiché ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

In relazione all'utilizzo non corretto di detti strumenti si individuano i seguenti possibili rischi e conseguenti effetti, rappresentati nella tabella sottostante:

Attività	Rischio	Motivazione	Possibile effetto
Manutenzione di periferiche hardware interne (scheda video, ecc.)	Alto	Possono essere Danneggiati componenti interne e il PC	Danneggiamento della strumentazione
Manutenzione di periferiche hardware esterne (tastiera, mouse, ecc.)	Basso		Limitazione nell'utilizzo
Download non controllato o non programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete	Alto	Possono essere scaricate applicazioni non verificate con il pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore	Danneggiamento del software del PC o della rete informatica interna
Download controllato o programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete	Basso		
Download di dati non inerenti alle attività lavorative (musica, giochi, ecc.)	Alto	Possono essere scaricate applicazioni non verificate con il pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore	Danneggiamento del software del PC o della rete informatica interna. Gravi responsabilità civili e penali per l'Istituto in caso di violazione della normativa a tutela dei diritti d'autore
Installazione di applicazioni senza l'autorizzazione del responsabile della rete	Alto	Possono essere installate applicazioni non compatibili	Danneggiamento del software del PC o della rete informatica interna
Accesso alla rete effettuato da Pc di proprietà dell'utente	Alto	Accessi non autorizzati alla rete	Furto di dati

Apertura di allegati di posta elettronica di incerta provenienza	Alto	Possono contenere Malware/Spyware	Danneggiamento del Software del PC o della rete informatica interna. Divulgazione di password e dati riservati
Elaboratore connesso alla rete lasciato incustodito o divulgazione di password	Alto	Possibile utilizzo da parte di terzi	Uso indebito di dati riservati, danneggiamento della rete informatica interna
Utilizzo di supporti removibili esterni non autorizzati	Alto	Possono essere trasferite applicazioni dannose per il PC nella rete informatica	Danneggiamento dei PC o della rete informatica interna
Furto di dati Mancata distruzione o perdita accidentale di supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi usb, cd riscrivibili,...) contenenti dati sensibili e giudiziari	Alto	Recupero di dati memorizzati anche dopo la loro cancellazione	Uso indebito di dati riservati

Nomina dell'Amministratore di sistema e del Custode delle password

Il Dirigente Scolastico conferisce all'Amministratore di sistema il compito di sovrintendere alle risorse informatiche dell'Istituto assegnandogli in maniera esclusiva le seguenti attività:
a) gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'istituto, siano esse collegate in rete o meno;
b) configurazione dei servizi di accesso alla rete interna, ad internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account;
c) attivazione della password di accensione (BIOS);
d) creazione di un'area condivisa sul server per lo scambio di dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel PC che non siano strettamente necessarie perché sono un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema;
e) controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
f) rimozione sia sui PC degli incaricati sia sulle unità di rete, di ogni tipo di file o applicazione che può essere pericoloso per la sicurezza o costituisce violazione del presente regolamento;
g) distruzione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;
h) utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, solo

per il tempo necessario al compimento di attività indifferibili solo su richiesta del Responsabile del trattamento.
L'Amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al PC di ciascun utente.
Il Custode delle password è incaricato di custodire e conservare in luogo riservato e sicuro, in formato cartaceo, le credenziali. E' tenuto a ottemperare al suo compito avendo cura di non diffondere, nemmeno accidentalmente, le stesse a persone estranee al loro utilizzo.

Assegnazione delle postazioni di lavoro

Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro provvede a:
- individuare preventivamente le postazioni di lavoro e assegnarle a ciascun dipendente,
- individuare preventivamente gli utenti a cui è accordato l'utilizzo della posta elettronica e l'accesso a internet.

La strumentazione dell'Istituto non è di esclusivo dominio del dipendente, ma rientra tra i beni a cui determinati soggetti possono comunque sempre accedere. L'eventuale accesso del datore di lavoro, qualora necessiti di informazioni contenute nei documenti residenti sul PC assegnato al dipendente, è legittimo.

Utilizzo dei personal computer

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'Istituto di cui sono responsabili, salvo eccezioni autorizzate dal datore di lavoro e dall'Amministratore di sistema.
Sono tenuti a:
• applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete,
• custodirlo con diligenza e in luogo protetto durante gli spostamenti,
• rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna,
• non disattivare sul PC lo screen saver e la relativa password,
• conservare la password nella massima riservatezza e con la massima diligenza,
• non modificare la configurazione hardware e software del PC se non esplicitamente autorizzati dall'amministratore di sistema,
• non rimuovere, danneggiare o asportare componenti hardware,
• nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso, senza spegnere il PC e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica,
• permettere l'autoaggiornamento del PC,
• prestare la massima attenzione ai supporti di origine esterna (es. pendrive), verificando preventivamente, tramite il programma antivirus, ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti,
• non lasciare incustodita e accessibile la propria postazione una volta eseguita la connessione al sistema con le proprie credenziali di autenticazione,
• non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica,
• spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

Utilizzo di supporti magnetici

Gli utenti devono trattare con particolare cura i supporti magnetici (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,…) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti. Di conseguenza le azioni da compiere obbligatoriamente sono le seguenti:
a) porre attenzione nell'utilizzo dei supporti rimovibili personali,
b) custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto (presso il custode delle password),
c) consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili, ...) obsoleti all'Amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere successivamente alla cancellazione recuperato.

Utilizzo delle stampanti e dei materiali d'uso

Stampanti e materiali di consumo in genere (carta, inchiostro, toner e supporti digitali) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi eccessivi.
Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati, distruggere personalmente e sistematicamente le stampe che non servono più.

Utilizzo di telefonini e altre apparecchiature

Il telefono affidato al dipendente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative e non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa.
La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso a disposizione. Al cellulare d'Istituto qualora venisse assegnato, si applicano le medesime regole sopra previste. È vietato l'utilizzo del fax e delle fotocopiatrici d'Istituto per fini personali. È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo:
a) diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento,
b) informazione preventiva degli interessati,
c) acquisizione del loro libero consenso, preventivo ed informato.

Utilizzo della rete informatica
Le reti interne:
nel Plesso Pistelli sono tre linee: una linea destinata alla segreteria e due linee alla didattica (ADSL e FIBRA) negli altri plessi (Pieve, Marignana, Orbicciano, Tabarrani e Arcobaleno) esiste linea ADSL in ciascuno dei plessi
La rete informatica permette di salvare su server i files relativi alla produttività individuale.

Le cartelle presenti nei server di segreteria e di laboratorio sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup.
L'accesso è regolamentato da policies di sicurezza che suddividono gli accessi fra gruppi e utenti.
Periodicamente si provvede alla pulizia degli archivi, con cancellazione dei files obsoleti ed inutili.
Gli utenti della rete informatica sono tenuti a utilizzare la rete in modo conforme a quanto stabilito dal presente regolamento e quindi:
a) mantenere segrete e non comunicare a terzi, inclusi gli amministratori di sistema, le password d'ingresso alla rete ed ai programmi e non permettere ad alcuno di utilizzare il proprio accesso,
b) provvedere periodicamente alla pulizia degli archivi con cancellazione dei file obsoleti o inutili ed evitare un'archiviazione ridondante,
c) verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pendrive) prima di trasferirlo su aree comuni della rete.
Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferendo con la connettività altrui o con il funzionamento del sistema e quindi di:
a) utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files o software di altri utenti, utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e delle privacy,
b) sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate,
c) modificare le configurazioni impostate dall'amministratore di sistema,
d) limitare o negare l'accesso al sistema a utenti legittimi,
e) effettuare trasferimenti non autorizzati di informazioni (software, dati, ...),
f) distruggere o alterare dati altrui,
g) usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Utilizzo delle password

Per l'accesso alla strumentazione informatica di Istituto ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione previste ed attribuite dall'incaricato della custodia delle password.
Le credenziali di autenticazione per l'accesso alla rete consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà essere custodita dal Custode delle password con la massima diligenza e non può essere divulgata.

Procedure di gestione delle credenziali di autenticazione

È necessario procedere alla modifica della parola chiave, a cura dell'incaricato, al primo utilizzo. Se l'utente non provvede autonomamente a variare la password entro i termini massimi, viene automaticamente disabilitato. Provvederà l'Amministratore di sistema a riabilitare l'utente e ad assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso.
Per scegliere una parola chiave si devono seguire le seguenti istruzioni:
-usare una parola chiave di almeno otto caratteri,
-usare una combinazione di caratteri alfabetici e numerici (meglio inserire anche segni di interpunzione o un carattere speciale),

-non usare mai il proprio nome o cognome, né quello di congiunti (le migliori password sono quelle facili da ricordare, ma allo stesso tempo difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe).
La password deve essere cambiata a intervalli regolari a cura dell'incaricato del trattamento d'intesa con il custode della password (ogni sei mesi) e comunicata al custode delle password perché ne curi la conservazione.
Bisogna evitare di comunicarla ad altri, di trascriverla su supporti (agenda, post-it, ...) che siano accessibili ad altri o di consentire che qualcuno sbirci quello che si sta scrivendo sulla tastiera quando viene immessa la password.
Nel caso si sospetti che la password abbia perso la segretezza essa deve essere immediatamente sostituita.

Art. 1 – Posta elettronica

1. La posta elettronica costituisce modalità normale di trasmissione delle comunicazioni ufficiali dell'Istituto, quali circolari e convocazioni di organi e commissioni, che si considerano acquisite, ai fini interni, dal momento dell'avvenuto regolare invio.

2. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano a non commettere violazioni alle norme generali e speciali civili, penali ed amministrative, nonché al presente regolamento, aderendo ad un principio di autodisciplina.

3. L'indirizzo di posta elettronica può essere correlato ad altri servizi come accesso a portali, piattaforme didattiche e tutti gli ambienti internet legati solo ed esclusivamente ad attività lavorative e didattiche.

Art. 2 – Soggetti che possono avere accesso al servizio di posta elettronica

1. La casella viene assegnata agli utenti che necessitano di tale servizio a scopi lavorativi e/o didattici (docenti, studenti, personale interno e, previa autorizzazione, terze parti) e viene ritirata alla cessazione dello stesso.

2. Possono essere assegnate ulteriori caselle, in relazione alle necessità, alle seguenti categorie:

- docenti a contratto, collaboratori esterni impegnati nelle attività istituzionali;

- componenti degli organi dell'Istituto non dipendenti, per il periodo di durata della carica;

- altri utenti per i quali si disporrà di volta in volta per il tempo necessario o di svolgimento dell'incarico.

3. L'accesso di determinate categorie può essere regolamentato anche per motivi tecnici e per il tempo strettamente necessario alle attività da svolgere.

4. L'accesso al servizio è assicurato compatibilmente con le potenzialità delle risorse.

Art. 3 – Tipologie di caselle

1. In prima applicazione vengono attivate due diverse tipologie di caselle, una personale ed una funzionale.

2. L'account personale è fornito gratuitamente a tutte le categorie di utenza di cui all'art. 2. L'indirizzo è del tipo cognome.nome@dominio.ext, tenendo conto di eventuali implementazioni/modifiche del/dei domini scolastici secondo comunicazioni del MIUR.

3. L'account funzionale è fornito gratuitamente ed è riservato agli organi, agli uffici, a specifiche deleghe direttoriali, ad altre categorie ritenute utili per i fini istituzionali. In questo caso l'indirizzo è del tipo funzione@dominio.ext.

4. L'account funzionale può essere utilizzato da qualsiasi dipendente inquadrato nella medesima funzione e dal personale con funzioni direttoriali; in caso di assenza, può essere utilizzato da chi legittimamente lo sostituisca. L'indirizzo funzione@domino si riferisce infatti ad una casella di posta elettronica istituzionale e le comunicazioni inviate a tale indirizzo sono conoscibili da tutti gli appartenenti a tale funzione e, se giuridicamente rilevanti, verranno registrate nel protocollo ufficiale dell' Istituto.

5. Ogni casella di posta elettronica viene fornita insieme ad uno spazio disco limitato.

6. L'amministratore di posta, tenuto conto delle risorse tecniche a disposizione, può limitare momentaneamente il numero di account per categorie di utenti ed incrementarlo con gradualità.

7. L'attivazione dell'account avverrà dopo la verifica dei requisiti richiesti.

8. È prevista la pubblicazione degli indirizzi di posta, che avverrà dopo che l'utente abbia dato riscontro all'attivazione dell'account.

Art. 4 – Condizioni di utilizzo

1. Qualsiasi utilizzo della posta elettronica e servizi ad essa collegati viene associato ad un persona fisica cui imputare le attività svolte.

2. L'Utente ottiene l'accesso dopo essersi impegnato ad osservare il presente regolamento, le altre norme disciplinanti le attività e i servizi di posta elettronica comprese le funzionalità ad essa collegate ed essersi impegnato a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

3. L'Utente è responsabile dell'attività espletata tramite il suo account.

4. L'Utente si impegna ad adoperarsi attivamente per salvaguardare la riservatezza della sua password e a segnalare qualunque situazione che possa inficiarla.

5. L'Utente si impegna a segnalare, con tempestività, all'amministratore di posta eventuali malfunzionamenti delle caselle di posta a lui assegnate.

6. Di norma gli Utenti possono accedere gratuitamente al servizio, tramite le infrastrutture dell'Istituto.

7. Restano a carico dell'Utente eventuali oneri relativi a collegamenti da punti di accesso privati.

8. L'Utente riconosce che le comunicazioni ufficiali, quali circolari e convocazioni di organi e commissioni, inviate agli indirizzi di posta elettronica valgono quali comunicazioni interne e si considerano consegnate al momento dell'avvenuto regolare invio.

Art. 5 – Obblighi dell'Istituto

1. L'Istituto si impegna a fornire il servizio in modo continuativo, fatte salve eventuali sospensioni dovute all'ordinaria o straordinaria manutenzione, malfunzionamenti e ad altre eventualità.

2. L'Istituto si impegna ad utilizzare i dati, già forniti dall'Utente ai sensi della normativa vigente, con chiaro riferimento al "D.Lgs. 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali" e successiva normativa nazionale e comunitaria, con particolare riferimento al Regolamento UE 2016/679 (G.D.P.R.), ai soli fini dell'erogazione e gestione del servizio e di attuare quanto in suo potere per proteggere la privacy dell'Utente medesimo.

Art. 6 – Limiti di responsabilità dell'Istituto

1. L'Istituto si serve di fornitori che si impegnano ad attuare tutte le misure ritenute necessarie e sufficienti a minimizzare il rischio di perdita d'informazioni; ciò nonostante l'Utente solleva l'Istituto da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, al mancato invio/ricezione o all'omessa conservazione di messaggi di posta (e-mail) o di altri contenuti, derivanti da guasti e/o malfunzionamenti degli apparati di gestione e, in generale, dall'erogazione del servizio stesso.

2. L'Istituto si riserva il diritto di non memorizzare o di cancellare i messaggi dell'Utente stesso, qualora questi ecceda lo spazio disco a sua disposizione.

3. Non sono previste attività di backup e di ripristino individuale sui server che sono gestiti esternamente e internamente.

Art. 7 – Riservatezza della posta elettronica

1. L'Istituto persegue la riservatezza e l'integrità dei messaggi di posta elettronica e servizi ad essa collegati diretti alle caselle personali durante il loro transito e la loro permanenza nel sistema di posta.

2. Per il raggiungimento di tale obiettivo l'Amministratore di Sistema, l'Amministratore di posta ed il Fornitore possono avvalersi anche di strumenti idonei a verificare, mettere in quarantena o cancellare i messaggi che potrebbero compromettere il buon funzionamento del servizio.

3. In linea generale, i messaggi di posta sono conservati nella mailbox associata all'Utente, finché non vengano dallo stesso rimossi.

Art. 8 – Liste di utenti

1. In osservanza di quanto disposto dal D.Lgs. 30 giugno 2003, n. 196 e dal Regolamento UE 2016/679 (G.D.P.R.), al fine di tutelare la riservatezza degli utenti e la libertà e segretezza della corrispondenza, possono essere predisposte liste di utenti, distinte per oggetto, volte a semplificare le comunicazioni istituzionali

2. In particolare, possono essere attivate liste permanenti, in relazione alla qualifica, alla funzione svolta, alla materia di insegnamento, per le comunicazioni istituzionali.

3. Possono inoltre essere attivate liste temporanee in relazione a progetti od esigenze particolari.

4. L'utilizzo delle liste è disciplinato dal Dirigente.

Art. 9 – Attività vietate

1. È vietato usare il servizio:

a. in modo difforme da quanto previsto nel presente regolamento;

b. in modo difforme dalle regolamentazioni dettate dai responsabili della rete e del servizio di posta;

c. in modo difforme da quanto previsto dalle norme penali, civili e amministrative generali e specifiche in materia;

d. per scopi incompatibili con le finalità e con l'attività istituzionale dall'Istituto;

e. per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'Istituto;

f. per commettere attività che violino la riservatezza di altri utenti o di terzi;

g. per attività che influenzino negativamente la regolare operatività della rete o ne restringano l'utilizzabilità e le prestazioni per gli altri utenti;

h. per attività che distraggano risorse (persone, capacità, elaboratori) in misura anomala;

i. per attività che provochino trasferimenti non autorizzati di informazioni (software, basi dati, etc.);

j. per attività che violino le leggi a tutela delle opere dell'ingegno.

2. Nessun utente può utilizzare la casella di posta elettronica e servizi ad essa collegati attribuendosi qualifiche improprie, inesatte, non più attuali, ovvero con finalità diverse da quelle istituzionali o ad esse comunque correlate. È fatto inoltre rigoroso divieto di utilizzare l'indirizzo di posta elettronica o le credenziali di accesso quale recapito per l'accesso a siti o servizi internet non correlati con l'attività istituzionale.

Art. 10 – Ulteriori divieti, limiti di utilizzo, responsabilità dell'Utente

1. L'Utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio; esonera contestualmente l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di tale uso improprio.

2. L'Utente, inoltre, non può utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l'utilizzo e il godimento del servizio da parte di altri utenti.

3. L'Utente, salvo giustificabili eccezioni, di cui comunque risponde personalmente, non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino a:

▪ pubblicità non istituzionale, manifesta o occulta;

▪ comunicazioni commerciali private;

▪ materiale pornografico o simile, in particolare in violazione delle vigenti norme contro lo sfruttamento sessuale dei minori;

▪ materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;

▪ materiale che violi la legge sulla privacy;

▪ contenuti o materiali che violino i diritti di proprietà di terzi;

▪ altri contenuti illegali.

L'elenco riportato è da intendersi non esaustivo.

4. In nessun caso l'Utente potrà utilizzare la posta elettronica e servizi ad essa collegati per diffondere codici dannosi per i computer quali virus e simili.

5. È assolutamente vietato tentare di accedere in modo non autorizzato, tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti, ai servizi, ad altri account, ai sistemi o alle reti connesse.

6. L'Utente si impegna ad implementare, nel caso utilizzi una propria stazione di accesso alla posta elettronica, tutte quelle misure idonee e necessarie ad evitare, o comunque minimizzare, la divulgazione di virus informatici e simili.

7. L'Utente si impegna a non divulgare messaggi di natura ripetitiva (catene di Sant'Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

8. L'Utente accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.

Art. 11 – Internet

1. È vietato navigare o registrarsi in siti non attinenti alle mansioni dell'Utente.

2. È vietato scaricare programmi o file musicali ancorché gratuiti.

3. È vietato partecipare a forum se non attinenti con la propria attività lavorativa e utilizzare chat line.

4. È vietato conservare file di contenuto discriminatorio.

5. Data la vasta gamma di attività, non è definito a priori un elenco di siti autorizzati; vengono utilizzati appositi strumenti di filtraggio, mediante i quali viene bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi dell'Istituzione Scolastica. Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.

Art. 12 – Computer

Nelle postazioni attive nell'istituto non è consentito:

1. installare programmi se non debitamente autorizzati;

2. modificare le configurazioni esistenti;

3. installare modem, router e switch o altri apparecchi se non debitamente autorizzati.

4. utilizzare dispositivi di archiviazione esterni diversi da quelli appositamente autorizzati.

Ogni dispositivo di archiviazione di provenienza esterna all'Istituto dovrà essere verificato mediante programma antivirus prima del suo utilizzo.

Il Dirigente si riserva di effettuare controlli, conformi alla legge, anche saltuari e occasionali, indicando le ragioni legittime – specifiche e non generiche – per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni).

Per quanto concerne le prescrizioni sulla sicurezza dei dati e dei sistemi si rinvia alla documentazione interna dell'istituto.

Art. 13 - Controlli a distanza

In via generale, non sono consentiti i trattamenti effettuati mediante sistemi hardware e software che consentono il controllo dell'attività degli Utenti. Il divieto riguarda l'attività lavorativa e didattica in senso stretto e altre condotte personali poste in essere all'interno del luogo di lavoro.

A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili.

Sono ovviamente vietati i sistemi preordinati al controllo diretto, che consentono di ricostruire l'attività di Utenti come nel caso di:

● Lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;

● Riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

● Lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

● Analisi occulta di computer portatili affidati in uso.

Altrettanto vietati sono i sistemi che consentono indirettamente il controllo, quando non siano preordinati a esigenze produttive od organizzative o, comunque, non siano necessari per la sicurezza sul lavoro. In caso di necessità produttiva, organizzativa o di sicurezza, il trattamento dei dati che ne consegue può essere lecito, è però necessario rispettare le procedure di informazione e di consultazione di lavoratori e sindacati (di cui all'art. 4, comma 2, della L. 300/1970 aggiornata dalla L.92/2912), in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

Art. 14 - Graduazione dei controlli

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali degli Utenti, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

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

Per quanto possibile, deve essere 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 aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

Art. 15 - Conservazione

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra-registrazione come, ad esempio, la cd.

rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla.

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

● esigenze tecniche o di sicurezza del tutto particolari;

● 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.

In questi casi, il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Art. 16 - Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve le ulteriori conseguenze di natura disciplinare, penale, civile e amministrativa, saranno messi in atto i previsti interventi sanzionatori, regolativi e, laddove previsto, si procederà a segnalare il reato alle Autorità competenti. Il Dirigente, in via provvisoria e di urgenza, in deroga all'art. seguente, può ordinare all'Amministratore di posta o al Fornitore l'immediata cessazione dell'attività all'origine dell'abuso, adottando le necessarie misure per impedire che l'abuso venga portato ad ulteriori conseguenze.

Nel caso b dell'art. 9, c.1, e a seguito di segnalazione da parte dei gestori della rete, l'Istituto è autorizzato alla immediata sospensione dell'accesso senza preavviso. Nei casi c, e, f, g, i, l, dell'art. 9, c.1, l'Istituto è autorizzato alla immediata sospensione dell'accesso senza preavviso, dandone successivamente comunicazione al Dirigente.

Informativa agli utenti

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'istituto (circolare, sito) e quindi portato a conoscenza di ciascun dipendente.
L'utente qualora l'istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta elettronica e della navigazione in internet, viene informato degli strumenti e dei modi di trattamento effettuati prime che questo sia iniziato.

Aggiornamento e revisione del Regolamento

Il presente regolamento è soggetto a revisione con frequenza annuale e ogni qualvolta sia necessario un aggiornamento alla luce dell'esperienza, di nuove normative e dell'innovazione tecnologica.
Tutti gli utenti possono proporre quando ritenuto necessario, integrazioni al presente regolamento e le proposte saranno esaminate dal Responsabile del trattamento in collaborazione con l'Amministratore di sistema.