MINISTERO DELLA ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
REPUBBLICA ITALIANA – REGIONE SICILIANA
Istituto Comprensivo Statale "Politeama"
Piazza Castelnuovo, 40 – 90141 Palermo- Tel. 091-331037 – Fax 091-304720 - C.F. 97163050822
www.icspoliteama.it e-mail:paic890009@istruzione.it paic890009@pec.istruzione.it

POLICY DI UTILIZZO DELLA RETE INFORMATICA E DELLE CASELLE DI POSTA ELETTRONICA PER IL PERSONALE SCOLASTICO

La presente Policy contiene la descrizione delle misure operative che i soggetti incaricati del trattamento dei dati personali sono chiamati ad adottare per garantire la sicurezza dei dati personali, in conformità agli standard di tutela previsti dal Reg. (UE) 2016/679 (GDPR), nell'utilizzo della rete informatica e delle caselle di posta elettronica istituzionali. La Policy è portata a conoscenza degli utenti e disponibile per la consultazione tramite i mezzi di comunicazione interna utilizzati dall'Istituto (circolare, sito).

Definizioni

Trattamento di dati : qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati (art. 5 GDPR).

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 la Dirigente Scolastica Camilla Pasqualini 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 : chiunque agisca sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento (art. 29 GDPR).

Violazione dei dati personali (*) : la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, *12* GDPR)

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.

****

Rete Informatica

Art.1- Identificazione e distribuzione della rete informatica

Le reti interne, in totale n. 4 connessioni internet presenti nell'Istituto Scolastico sono così distribuite:

n. 1 rete internet Plesso Archimede

n. 1 rete internet Plesso Serpotta

n. 1 rete internet Plesso La Masa

n. 1 rete internet Plesso Federico II

Art.2 - Utilizzo delle Cartelle

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.

Art. 3 - Regole di condotta

1. Gli utenti della rete informatica sono tenuti a :

a) provvedere periodicamente alla pulizia degli archivi con cancellazione dei file obsoleti o inutili ed evitare un'archiviazione ridondante;

b) verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pendrive) prima di trasferirlo su aree comuni della rete.

2. Agli utenti della rete informatica è fatto espresso divieto di:

a) utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file 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;

h) navigare o registrarsi in siti non attinenti alle mansioni dell'Utente;

i) scaricare programmi non autorizzati;

l) partecipare a forum, se non attinenti con la propria attività lavorativa, e utilizzare chat line.

****

Posta elettronica

Art.1 - Utilizzo della Posta Elettronica

1. La posta elettronica costituisce modalità normale di trasmissione delle comunicazioni ufficiali dell'Istituto, che si considerano acquisite, ai fini interni, dal momento dell'avvenuto regolare invio.
2. L'indirizzo di posta elettronica può essere correlato ad altri servizi come accesso a portali, piattaforme didattiche e tutti gli ambienti Internet funzionali solo ed esclusivamente allo svolgimento di attività lavorative e didattiche.

Art. 2 – Soggetti che possono avere accesso al servizio di posta elettronica ad uso esclusivamente interno e finalizzato all'utilizzo della piattaforma G-Suite

1. La casella istituzionale con dominio @icspoliteama.edu.it viene assegnata agli utenti che necessitano di tale servizio a scopi lavorativi e/o didattici (docenti, alunni, 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 , 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.

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

Art. 3 – Condizioni di utilizzo

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

2. L'Utente riconosce che le comunicazioni ufficiali, inviate agli indirizzi di posta elettronica della scuola valgono quali comunicazioni interne e si considerano consegnate al momento dell'avvenuto regolare invio.

3. Qualora l'Utente dovesse ricevere per errore nell'invio, una e-mail in realtà destinata ad altri, si impegna a recapitarla al destinatario - se facilmente identificabile- al quale la comunicazione era originariamente indirizzata.

4. Prima di aprire file allegati ad una e-mail accertarsi che il mittente sia affidabile verificandone il dominio, e accertarsi che l'estensione del file non sia di origini sospette .

5. Qualsiasi utilizzo della posta elettronica e servizi ad essa collegati viene associato ad un persona fisica cui imputare le attività svolte: pertanto, l'utente è responsabile dell'attività espletata tramite il suo account.

Art. 4 – Riservatezza della posta elettronica

- L'Istituto rispetta 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.

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

Art. 5 -Trasmissione di categorie particolari di dati personali o dati personali relativi a condanne penali e reati

- Qualora all'e-mail sia allegato un file contenente categorie particolari di dati personali o dati personali relativi a condanne penali e reati ai sensi degli artt. 9 e 10 Reg. (UE) 2016/679, il mittente è tenuto a prestare un maggiore grado di cautela , assicurandosi di inviare la comunicazione all'effettivo destinatario a cui questa deve essere rivolta e di effettuare la registrazione (protocollo) in modalità riservata, con accesso riservato esclusivamente alle persone autorizzate.

- Al fine di proteggere adeguatamente il file allegato contenente categorie particolari di dati personali o dati personali relativi a condanne penali, il mittente deve obbligatoriamente inviare il file in modalità protetta tramite password, la quale deve essere comunicata al destinatario con un mezzo diverso (consegnata a mano, via sms, oppure tramite indirizzo e-mail secondario.)

Art. 6 – Liste di utenti

- 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.
- In particolare, possono essere attivate liste permanenti, in relazione alla qualifica, alla funzione svolta, alla materia di insegnamento, per le comunicazioni istituzionali.
- Possono inoltre essere attivate liste temporanee in relazione a progetti od esigenze particolari.
- l'utilizzo delle liste è disciplinato dal DSGA.

Art. 7 – Attività vietate

1. È vietato usare il servizio:
a. in modo difforme da quanto previsto nel presente regolamento;

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

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

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

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

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

g. 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.

Art. 8 – Ulteriori divieti, limiti di utilizzo, responsabilità dell'Utente

- L'Utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio.
- 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.
- L'Utente 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.

Art. 9 - 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.
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. 10 - Conservazione dei log

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 conseguirla.
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. 11 - Sanzioni

In caso di abuso, a seconda della gravità del medesimo, fatte salve le ulteriori conseguenze di natura disciplinare, penale, civile e amministrativa, saranno messi in atto i seguenti interventi sanzionatori: Rimprovero Scritto. Qualora l'abuso configuri gli estremi di un reato, si procederà a segnalare il fatto alle Autorità competenti. Il DSGA, in via provvisoria e di urgenza, e previa indicazione del Dirigente Scolastico (Titolare del Trattamento), può sospendere l'accesso dell'Utente senza preavviso, adottando le necessarie misure per impedire che l'abuso venga portato ad ulteriori conseguenze.

Il Dirigente Scolastico

Dott.ssa Aurora Fumo