Disciplinare interno per l'utilizzo di Internet e della posta elettronica da parte del personale scolastico

Introduzione

In conformità al Regolamento (UE) 2016/679 (GDPR) e al D.Lgs. 30 giugno 2003 n.196 (**Codice in materia di protezione dei dati personali**), come aggiornato dal D.Lgs. 101/2018 e successive modifiche, l'Istituto adotta il presente disciplinare interno sull'utilizzo di Internet e della posta elettronica. Il documento tiene conto dell'art. 4 della Legge 300/1970 (**Statuto dei Lavoratori**, in tema di controlli a distanza) e dei più recenti provvedimenti e linee guida del Garante per la protezione dei dati personali in materia di utilizzo degli strumenti informatici e tutela della privacy dei lavoratori (es. linee guida 2021–2023 su posta elettronica e navigazione Internet aziendale). Inoltre, esso si inserisce nel contesto delle iniziative di trasformazione digitale della Pubblica Amministrazione, in coerenza con il Piano Triennale per l'Informatica nella P.A. (ultimi aggiornamenti 2024–2026) e con le misure previste dal **Piano Nazionale di Ripresa e Resilienza (PNRR)** per la digitalizzazione del sistema scolastico (ad esempio il programma "Scuola 4.0").

Scopo del presente disciplinare è stabilire regole chiare per un uso corretto, sicuro e legittimo delle risorse informatiche dell'Istituto (posta elettronica, accesso a Internet e dotazioni hardware/software) da parte del personale docente e non docente. Tali regole mirano a proteggere i dati personali e le informazioni dell'amministrazione scolastica, prevenire usi impropri o illegali delle risorse ICT, garantire la continuità del servizio e tutelare sia l'Istituto sia i dipendenti da possibili violazioni normative. Il presente documento aggiorna e sostituisce le precedenti disposizioni interne in materia, adeguandole al contesto normativo e tecnologico attuale. Esso ha validità immediata dalla data di adozione e resta in vigore fino a eventuali future revisioni.

Gestione delle password

Ogni dipendente a cui vengono affidate credenziali di accesso ai sistemi informatici dell'Istituto (account di rete, account di posta elettronica istituzionale, accessi a piattaforme ministeriali, registro elettronico, etc.) è tenuto a custodirle con la massima diligenza. Di seguito le regole fondamentali per la gestione sicura delle password personali:

- **Segretezza e responsabilità:** le credenziali (nome utente e password) sono strettamente personali e non vanno comunicate né condivise con nessun altro. Il dipendente è direttamente responsabile di ogni attività svolta con le proprie credenziali. È vietato annotare la password in luoghi facilmente accessibili o conservarla in file non protetti.
- **Requisiti di complessità:** la password scelta deve essere robusta, ossia difficile da intuire. Si raccomanda una lunghezza minima di **8 caratteri** (meglio se 12 o più) e la presenza di combinazioni di lettere maiuscole e minuscole, numeri e caratteri speciali. Evitare parole di uso comune, informazioni personali (nome, data di nascita, etc.) o sequenze semplici ("1234", "password", ecc.). L'Istituto si riserva di implementare requisiti minimi di complessità tramite i sistemi informatici.
- **Cambi periodici e aggiornamento:** è opportuno modificare la password con regolarità (ad esempio ogni 6 mesi) e comunque immediatamente qualora vi sia il sospetto che possa essere stata scoperta da altri o compromessa. Alcuni sistemi potrebbero richiedere il cambio password obbligatorio dopo un certo intervallo di tempo, in linea con le policy di sicurezza aggiornate. In fase di primo accesso o dopo reimpostazioni tecniche, il dipendente deve cambiare la password provvisoria iniziale fornitagli dall'amministratore.

- **Divieti e cautele:** non utilizzare le credenziali istituzionali per registrarsi a servizi esterni non autorizzati o per scopi estranei all'attività lavorativa. È vietato riutilizzare sul lavoro password già impiegate per account personali, oppure viceversa usare sul proprio account privato la stessa password dell'account scolastico. In caso di utilizzo di gestori di password o funzionalità di salvataggio automatico, assicurarsi che siano strumenti approvati e adeguatamente protetti.
- **Smarrimento o compromissione:** il dipendente deve avvisare tempestivamente l'Amministratore di Sistema (o l'ufficio preposto) nel caso sospetti che la propria password sia stata scoperta, rubata o che l'account sia stato oggetto di accesso non autorizzato. In tali casi, la password va immediatamente reimpostata. L'Amministratore di Sistema può procedere d'ufficio al blocco o cambio forzato delle credenziali qualora rilevi attività anomale o evidenze di compromissione, informandone il diretto interessato e il Dirigente Scolastico.

Utilizzo del PC e delle attrezzature informatiche

Le postazioni di lavoro informatiche (PC fissi, portatili, tablet, LIM, ecc.) e le altre attrezzature elettroniche fornite dall'Istituto devono essere utilizzate in modo appropriato e solo per finalità attinenti alle mansioni lavorative. Di seguito sono elencate le principali norme di comportamento nell'uso dei dispositivi scolastici:

- **Uso esclusivamente lavorativo:** il computer e le risorse informatiche assegnate sono strumenti di lavoro. È fatto divieto di utilizzarli per scopi privati, ludici o commerciali estranei all'attività dell'Istituto, salvo modestissime eccezioni di carattere personale e di breve durata (ad esempio consultare una notizia online durante una pausa), purché non interferiscano con i compiti lavorativi e non violino le altre regole del presente disciplinare. In nessun caso è consentito svolgere con i mezzi informatici della scuola attività esterne remunerative, attività politica/partitica, o altri utilizzi che possano arrecare danno all'amministrazione o configurare un illecito.
- **Divieto di installazione non autorizzata:** non è permesso installare software o applicativi sui computer dell'Istituto senza autorizzazione dell'Amministratore di Sistema. Qualunque programma necessario per esigenze di ufficio o didattiche deve essere richiesto attraverso le procedure interne; verranno installati solo software verificati, con regolare licenza d'uso, e compatibili con le policy di sicurezza. È vietato scaricare ed eseguire programmi da fonti non ufficiali o non attendibili, in quanto potrebbero contenere malware. Allo stesso modo, non si possono collegare alle postazioni periferiche hardware personali o supporti di memoria esterni (chiavette USB, hard disk, smartphone) senza preventiva verifica e autorizzazione, soprattutto se non forniti dall'amministrazione: supporti non controllati possono introdurre virus o sottrarre dati.
- **Aggiornamenti e protezioni:** il personale è tenuto a utilizzare sistemi operativi e software con **supporto aggiornato**. Non si devono utilizzare macchine con sistemi obsoleti per cui non sono più rilasciate patch di sicurezza (es. vecchie versioni di Windows non più supportate). Occorre inoltre effettuare con regolarità gli aggiornamenti di sicurezza del sistema operativo e dei programmi in uso, specialmente browser e client di posta. I software di protezione (antivirus, antimalware e firewall) presenti sulle postazioni non vanno disattivati né alterati, e devono rimanere costantemente attivi e aggiornati: l'utente collaborerà affinché le scansioni antivirus possano essere eseguite e segnalerà immediatamente all'Assistenza Tecnica eventuali messaggi di infezione o altri problemi di sicurezza riscontrati sul PC.
- **Cura della postazione e dati:** si deve aver cura dell'integrità fisica e logica della postazione informatica. Al termine dell'orario di lavoro o in caso di assenza prolungata dalla propria postazione, il dipendente dovrà effettuare il **log-out** dai sistemi e bloccare la sessione o spegnere il PC, in modo da impedire accessi indebiti al proprio account. Non lasciare mai incustodito un computer già

autenticato con le proprie credenziali, specialmente in presenza di studenti o persone non autorizzate. È opportuno mantenere ordinati gli archivi digitali: evitare di salvare dati personali o documenti riservati sul desktop o su percorsi locali non protetti; privilegiare le unità di rete o i repository ufficiali previsti dall'Istituto, che sono soggetti a backup regolari. In caso di trattazione di dati riservati (es. dati personali di studenti, documenti amministrativi interni), assicurarsi di rispettare le misure di sicurezza predisposte (es. cifratura dei file, utilizzo di piattaforme autorizzate) e non esportare tali dati al di fuori dell'ambiente di lavoro senza adeguata tutela.

- **Segnalazione guasti o anomalie:** ogni malfunzionamento, sospetto virus, incidente informatico o situazione anomala riscontrata sull'elaboratore va segnalata tempestivamente all'Amministratore di Sistema o al personale tecnico preposto. In questo modo si potrà intervenire rapidamente per risolvere il problema e prevenire conseguenze maggiori (es. diffusione di malware in rete, perdita di dati, accessi non autorizzati). Il dipendente deve collaborare alle attività di manutenzione e sicurezza pianificate (come interventi di aggiornamento, cambi password, installazione di nuove protezioni), attenendosi alle comunicazioni e istruzioni ricevute dall'Amministrazione.

Uso corretto della posta elettronica e di Internet

L'utilizzo della casella di **posta elettronica istituzionale** e l'accesso a **Internet** attraverso la rete dell'Istituto da parte del personale devono avvenire nel rispetto delle norme vigenti, delle finalità lavorative e delle regole di buona condotta. Di seguito vengono specificate le indicazioni per ciascuno di questi ambiti:

Posta elettronica istituzionale

L'account di posta fornito dall'Istituto (di norma nominativo @nomescuola.edu.it) va impiegato esclusivamente per motivi di servizio. Il dipendente è tenuto a utilizzare un linguaggio appropriato e professionale nelle comunicazioni, osservando le stesse regole di correttezza e rispetto che si applicano alle comunicazioni formali. È vietato inviare tramite l'e-mail di lavoro messaggi illeciti, offensivi, diffamatori o contenenti materiale osceno, molesto o discriminatorio. In particolare, non sono ammessi contenuti che possano costituire minaccia o molestia verso colleghi, studenti o terzi, né divulgare dati personali non autorizzati. Sono altresì proibiti l'invio di **catene di Sant'Antonio**, messaggi promozionali non richiesti (spam) o allegati di dimensioni irragionevoli/non pertinenti all'attività lavorativa.

L'account di posta istituzionale non deve essere utilizzato per scopi privati. Eventuali comunicazioni personali urgenti e indifferibili dovrebbero essere limitate e, se possibili, effettuate attraverso mezzi alternativi (telefono personale, account email privato durante la pausa, etc.), in modo da non gravare sui sistemi della scuola. **È tassativamente vietato utilizzare account email personali (non forniti dall'Istituto) per gestire pratiche d'ufficio o comunicare informazioni di servizio:** tutte le comunicazioni ufficiali devono transitare sui canali istituzionali, così da garantirne la **tracciabilità** e la conformità alle normative sulla trasparenza e conservazione dei documenti. **Il dipendente è responsabile del corretto utilizzo della propria casella:** è invitato a controllarla regolarmente durante l'orario di lavoro, mantenere un ordine nella gestione delle cartelle di posta e non eccedere con l'archiviazione di messaggi non attinenti al lavoro (che potrebbero saturare lo spazio di storage). In caso di assenza prolungata o cessazione del servizio, valgono le disposizioni organizzative dell'Istituto per garantire la continuità operativa: ad esempio, può essere predisposto un risponditore automatico o il reindirizzamento delle comunicazioni di servizio ad altri incaricati. In ogni caso, l'accesso ad account di posta di un dipendente da parte di altri (es. superiori o colleghi) è consentito solo nei limiti di legge e delle policy privacy (ad esempio per necessità indifferibili di ufficio, previa informativa all'interessato o coinvolgimento del DPO/RPD se richiesto dalle linee guida del Garante).

Nell'aprire i messaggi di posta, il personale dovrà porre attenzione alla sicurezza informatica: non cliccare su link sospetti né aprire allegati da mittenti sconosciuti o inattesi, specialmente se l'e-mail ha un oggetto

ambiguo o allarmistico (possibile phishing o malware). In caso di dubbi sull'autenticità di un messaggio, è opportuno consultare l'Amministratore di Sistema prima di intraprendere qualsiasi azione. I messaggi ricevuti identificati come spam o potenzialmente pericolosi non vanno inoltrati ad altri utenti interni. Si raccomanda inoltre di non configurare l'**autosalvataggio** delle credenziali sul client di posta (ad es. programmi come Outlook) su computer condivisi o non presidiati, e di bloccare la postazione quando ci si allontana, per evitare accessi non autorizzati alla propria posta.

Navigazione Internet

L'accesso a Internet dal sistema informatico scolastico è consentito ai dipendenti esclusivamente per motivi legati alle attività lavorative e professionali. Ciò include, ad esempio, la ricerca di informazioni normative o didattiche, l'uso di portali istituzionali o ministeriali, la fruizione di servizi online forniti dalla Pubblica Amministrazione, la partecipazione a corsi di formazione online autorizzati, l'utilizzo di piattaforme per la didattica digitale integrata o altri strumenti approvati dall'Istituto. Durante l'orario di lavoro, la navigazione verso siti non attinenti all'attività lavorativa deve essere evitata; un uso **occasionale e moderato** per esigenze personali non lavorative è tollerato solo se effettuato fuori dall'orario di servizio o durante le pause, e comunque nel rispetto di tutte le norme di sicurezza e dei limiti indicati (ad esempio, si può leggere una notizia di attualità durante una pausa caffè, ma non guardare video in streaming o navigare sui social media durante l'espletamento dei compiti d'ufficio).

Restano **assolutamente vietati** i siti e i servizi web che possano arrecare qualsiasi pregiudizio alla rete scolastica, violare la legge o i diritti di terzi, o compromettere il decoro dell'amministrazione. A titolo esplicativo ma non esaustivo, è vietato utilizzare la connessione internet dell'Istituto per:

- visitare siti pornografici o con contenuti osceni;
- accedere a siti che promuovono gioco d'azzardo, violenza, xenofobia, razzismo o odio;
- partecipare a forum/chat con linguaggio ingiurioso;
- scaricare materiale protetto da copyright (es. film, musica, software pirata) in violazione delle norme sul diritto d'autore;
- utilizzare servizi di **file sharing** o torrent che non siano espressamente autorizzati e funzionali all'attività lavorativa;
- effettuare transazioni o acquisti online personali;
- installare estensioni del browser o plugin non autorizzati.

Inoltre, è fatto divieto di utilizzare i social network durante l'orario di lavoro per scopi personali; l'accesso a social media o servizi di messaggistica web è consentito solo se strumentale alle mansioni (es. gestione della pagina social ufficiale della scuola da parte di personale autorizzato, oppure utilizzo di applicazioni di messaggistica per comunicazioni di servizio). In ogni caso, l'utilizzo di qualunque piattaforma online deve avvenire in conformità con le linee guida fornite dall'Amministrazione e assicurando la protezione dei dati: ad esempio, per l'archiviazione e condivisione di documenti didattici o amministrativi in cloud, vanno impiegati esclusivamente i servizi **certificati o convenzionati** dall'Istituto (Google Workspace for Education, Microsoft 365 o altri, se approvati e nominati responsabili del trattamento dei dati personali ai sensi dell'art. 28 GDPR). **Non** devono essere caricati documenti contenenti dati personali di alunni o colleghi su servizi cloud esterni non autorizzati o account personali del dipendente.

La navigazione web è soggetta ai controlli di sicurezza dell'Istituto: determinati siti o servizi potrebbero essere filtrati o bloccati automaticamente dai sistemi di protezione (firewall, filtri web) in quanto ritenuti non sicuri o non appropriati. Qualora l'utente ritenga che un sito necessario per lavoro sia stato indebitamente bloccato, potrà segnalarlo all'Amministratore di Sistema per le opportune valutazioni (senza tentare aggiramenti non consentiti dei filtri). **Analogamente, il traffico Internet è monitorato ai soli fini di sicurezza informatica e ottimizzazione della rete:** un utilizzo anomalo o eccessivo della banda (es. download massicci non giustificati) potrebbe essere individuato e limitato per garantire le prestazioni a tutti gli utenti.

Disposizioni per il lavoro da remoto (telelavoro o smart working)

Qualora al personale scolastico venga concessa la possibilità di svolgere la prestazione lavorativa in modalità **agile** (smart working) o **da remoto** (es. telelavoro domiciliare, didattica a distanza in caso di necessità, lavoro da casa per emergenze sanitarie o altri progetti specifici), si applicano tutte le regole di utilizzo corretto degli strumenti informatici previste nel presente disciplinare, con i necessari adattamenti al contesto esterno. In altre parole, le medesime cautele e responsabilità valgono anche fuori dai locali della scuola. Di seguito si richiamano e integrano le principali disposizioni per garantire sicurezza e conformità durante il lavoro da remoto:

- **Riservatezza dei dati e documenti:** il dipendente in lavoro agile è tenuto a garantire la tutela della riservatezza dei dati e delle informazioni d'ufficio anche nell'ambiente domestico. Evitare di lasciare incustoditi documenti cartacei riservati o di far visionare a persone non autorizzate (es. familiari, estranei) lo schermo del PC mentre sono aperti dati dell'Istituto. Le credenziali di accesso e i dispositivi di autenticazione (es. token, smart card) vanno custoditi con cura e non divulgati. Nel partecipare a riunioni online o videoconferenze di lavoro, assicurarsi di farlo in un luogo adeguato, dove terzi non possano ascoltare conversazioni riservate.
- **Dotazioni informatiche e connessione:** l'Istituto potrà fornire al dipendente attrezzature per il lavoro da remoto (PC portatile, tablet, account VPN, ecc.) oppure autorizzare l'uso di dispositivi personali. In entrambi i casi, è imperativo operare su strumenti dotati di adeguate misure di sicurezza. Se si utilizza un **PC personale**, prima di impiegarlo per lavoro è necessario verificare che sia presente un software antivirus aggiornato ed effettuare una scansione completa per escludere la presenza di malware. Il sistema operativo deve essere mantenuto aggiornato con le ultime patch di sicurezza e non deve essere scaduto il supporto del produttore (no a sistemi obsoleti non più aggiornati). È opportuno creare, quando possibile, un **account utente separato** dedicato alle attività lavorative sul PC personale, distinto dagli account ad uso privato, così da isolare i dati di lavoro ed evitare interferenze con programmi o file personali.
- **Sicurezza della rete domestica:** per collegarsi ai sistemi dell'Istituto, il dipendente dovrà disporre di una connessione Internet adeguata e sicura. Assicurarsi che il **router domestico** abbia password di accesso robuste (non lasciare la password predefinita fornita dal costruttore) e che la rete **Wi-Fi** sia protetta da crittografia (WPA2 o superiore) con una chiave di sicurezza complessa. Non utilizzare reti Wi-Fi pubbliche o non protette per accedere a sistemi dell'ente, se non tramite l'utilizzo di canali sicuri (come una **VPN** istituzionale) che cifrino il traffico. In caso l'Istituto fornisca l'accesso via VPN o altre soluzioni di accesso remoto, il dipendente dovrà utilizzarle secondo le istruzioni ricevute, evitando di connettersi attraverso canali non autorizzati.
- **Comportamenti prudenti online:** durante il lavoro da remoto, vanno ancor più osservate le prassi di prudenza nell'uso di Internet e della posta elettronica già descritte. Non cliccare su link sospetti ricevuti via email o tramite messaggistica, poiché attacchi di phishing e truffe informatiche sono in aumento verso chi lavora da casa. Prestare attenzione a **falsi avvisi** o richieste di aggiornamento software che compaiono durante la navigazione: in caso di dubbio, consultare l'Amministratore di Sistema prima di installare qualunque cosa. Evitare di utilizzare, per scopi lavorativi, computer di altri familiari o condivisi che non si ha certezza siano sicuri. Si raccomanda di non abilitare memorizzazioni automatiche di password o documenti di lavoro su servizi cloud personali non autorizzati.
- **Strumenti di collaborazione e cloud:** per trasferire file, comunicare con colleghi o salvare documenti durante il lavoro agile, utilizzare esclusivamente gli strumenti indicati o autorizzati dall'Amministrazione (es: spazio cloud istituzionale, piattaforme di videoconferenza o chat aziendali fornite dalla scuola, ecc.). Evitare di ricorrere a canali alternativi non controllati (es: account personali

di Google Drive, Dropbox, WhatsApp privato) per condividere dati di servizio, soprattutto se contengono informazioni riservate o personali. L'uso di servizi esterni è ammesso solo previa autorizzazione e, se del caso, formalizzazione di un accordo di protezione dati con il fornitore.

- **Supporto tecnico e segnalazioni:** il dipendente in modalità agile deve mantenersi in contatto con l'Amministrazione per segnalare tempestivamente eventuali problemi tecnici che impediscano o pregiudichino il lavoro (guasti al computer fornito, difficoltà di accesso ai sistemi, incidenti di sicurezza informatica, ecc.). L'Istituto cercherà di offrire supporto a distanza tramite i propri tecnici o fornitori. In caso di incidente di sicurezza grave (es. furto del device, sospetta violazione informatica), il lavoratore da remoto ne deve dare immediata comunicazione al Dirigente Scolastico e all'Amministratore di Sistema, fornendo tutte le informazioni utili a circoscrivere l'evento (ad esempio, ultimo accesso eseguito, tipo di dati potenzialmente coinvolti, etc.).
- **Disciplina lavorativa:** si ricorda che anche durante il lavoro agile o telelavoro il dipendente è tenuto al rispetto dell'orario di lavoro concordato e delle direttive ricevute. L'uso degli strumenti informatici in tali contesti deve concentrarsi sulle attività concordate nel progetto di lavoro agile, evitando distrazioni o usi personali non consentiti durante l'orario di servizio. Le verifiche sulle performance e sui risultati seguiranno le medesime regole di trasparenza e rispetto della privacy previste in presenza (non sono ammessi controlli occulti tramite webcam o software spia sul computer, salvo quanto eventualmente consentito dalle norme con adeguate garanzie). Il dipendente in lavoro agile deve altresì rispettare il diritto alla **disconnessione** fuori dall'orario di lavoro: terminato l'orario, non è tenuto a rimanere connesso ai sistemi o reperibile, se non secondo quanto previsto dagli accordi sul lavoro agile vigenti.

Sanzioni per violazioni

Tutti i lavoratori sono tenuti a conoscere e osservare le disposizioni del presente disciplinare, nonché qualunque ulteriore istruzione in materia di sicurezza informatica emanata dall'Amministrazione. La violazione delle regole stabilite è passibile di provvedimenti disciplinari e altre azioni previste dall'ordinamento. In particolare, il mancato rispetto delle norme d'uso di Internet, della posta elettronica e degli strumenti informatici potrà dar luogo a sanzioni disciplinari secondo la gravità dell'infrazione, in conformità a quanto previsto dal **CCNL Comparto Istruzione e Ricerca** vigente e dal D.Lgs. 165/2001 (Testo Unico sul pubblico impiego), oltreché dai Codici di comportamento applicabili ai dipendenti pubblici.

Oltre alle conseguenze disciplinari interne, alcune condotte potrebbero configurare illeciti civili o penali: ad esempio, l'utilizzo di software senza licenza, la diffusione di dati personali senza autorizzazione, l'accesso abusivo a sistemi informatici, la detenzione e propagazione di materiale pedopornografico, la molestia o diffamazione a mezzo internet sono fatti che la legge punisce gravemente. In presenza di violazioni di legge, l'Istituto si riserva di segnalare l'accaduto alle autorità competenti e di intraprendere azioni legali a tutela propria e dei soggetti coinvolti. Il dipendente potrà inoltre essere chiamato a rispondere dei **danni erariali o patrimoniali** causati da un uso doloso o gravemente negligente degli strumenti informatici (ad esempio, danni ai sistemi, perdita di dati, sanzioni comminate all'Ente per violazioni normative riconducibili a comportamenti del dipendente).

Nell'irrogare eventuali sanzioni disciplinari, il Dirigente Scolastico terrà conto di tutti gli elementi del caso (intenzionalità della condotta, grado di negligenza, precedenti, conseguenze prodotte, etc.), nel rispetto delle procedure di contestazione e difesa previste dalla normativa. Resta inteso che la finalità principale del presente regolamento è **preventiva ed educativa**: l'auspicio è che, attraverso la chiara definizione delle regole, si evitino comportamenti scorretti e non si debba ricorrere a misure sanzionatorie.

Esclusioni dai controlli sistematici e tutela della privacy del personale

L'Istituto, pur attuando misure di monitoraggio della rete e delle comunicazioni per garantire la sicurezza informatica, **non effettua controlli massivi, prolungati o indiscriminati** sull'attività online o sulla corrispondenza elettronica dei dipendenti. In ottemperanza ai princìpi dello Statuto dei Lavoratori e della normativa sulla privacy, ogni forma di controllo è esercitata con proporzionalità e trasparenza, evitando di ledere la dignità e la riservatezza del personale. In particolare, sono **esclusi** i seguenti trattamenti invasivi, salvo i casi espressamente ammessi dalla legge e con le garanzie ivi previste:

- ***Lettura o sorveglianza sistematica delle comunicazioni personali:*** l'amministrazione non accede né effettua una lettura preventiva continuativa dei contenuti dei messaggi di posta elettronica **personali** eventualmente inviati o ricevuti dai lavoratori (qualora un uso personale limitato sia tollerato, come da disposizioni sopra), né monitora in modo costante i cosiddetti dati esteriori delle email (metadati quali destinatari, orari, indirizzi IP) oltre quanto tecnicamente necessario al funzionamento dei sistemi. L'eventuale accesso ai contenuti della posta elettronica istituzionale del dipendente potrà avvenire solo per motivate ragioni di servizio e nel rispetto delle procedure di legge (ad esempio, previo coinvolgimento dell'interessato o, in casi di assenza/impedimento, secondo policy di emergenza comunicate, fermo restando il divieto di accesso a comunicazioni di natura privata).
- ***Strumenti di controllo occulti (spyware):*** non sono tollerati e non verranno installati sui dispositivi in uso ai dipendenti strumenti software o hardware destinati a controlli occulti e massivi, quali keylogger (registratori dei tasti digitati), microfoni o telecamere nascoste, software di screenshot/video cattura eseguiti all'insaputa dell'utente, o analoghi meccanismi mirati unicamente alla sorveglianza del lavoratore. Eventuali strumenti di protezione (es. antivirus con funzionalità anti-intrusione, software di inventory per la gestione IT, soluzioni di Mobile Device Management) potrebbero raccogliere informazioni sugli endpoint, ma sempre con finalità di sicurezza/organizzazione e non per spiare l'attività, e saranno comunque portati a conoscenza degli interessati tramite informative adeguate.

Va esplicitato che l'Istituto adotta sistemi di filtraggio dei contenuti web e firewall che **registrano i log** della navigazione Internet e degli accessi alla rete, così come i server di posta elettronica conservano nei log tecnici taluni dati relativi ai messaggi (mittente, destinatario, data/ora, dimensione, ecc.). Tali registrazioni avvengono in modo **automatico** e hanno lo scopo primario di garantire la sicurezza delle infrastrutture, prevenire intrusioni informatiche, virus e usi impropri delle risorse. Il Dirigente Scolastico e l'Amministratore di Sistema – o altri soggetti espressamente delegati a ciò – potranno consultare ed analizzare tali log **solo ove necessario**, ad esempio in caso di segnalazioni di anomalie, sospetto di attività illecite, violazioni del presente regolamento o per esigenze di verifica tecnica. Questa facoltà di controllo sarà esercitata nel rigoroso rispetto delle leggi vigenti: saranno trattati preferibilmente dati aggregati o anonimi ove sufficienti e la consultazione di log dettagliati riconducibili a singoli individui avverrà solo a fronte di concreti motivi e se necessario a prevenire condotte illecite o non in linea con il presente regolamento.

In ottica di correttezza, l'Istituto ispira la propria attività al principio della **gradualità dei controlli**: in caso di utilizzi anomali degli strumenti informatici, si privilegierà – ove possibile – un primo intervento di carattere generale. Ad esempio, qualora dai dati aggregati di utilizzo della rete risultassero comportamenti difformi (un eccessivo consumo di banda, accessi a orari insoliti, ecc.), si procederà inizialmente con un **richiamo collettivo** o verso il reparto interessato, ricordando le regole e invitando a un uso corretto. Se le irregolarità dovessero persistere o assumere carattere di gravità tale da far ipotizzare infrazioni deliberate, si potrà passare a controlli mirati su base individuale. Tali controlli individuali saranno attivati con l'autorizzazione del Dirigente Scolastico e coinvolgeranno l'Amministratore di Sistema per gli aspetti tecnici; avverranno in maniera **non occulta** (cioè gli interessati ne verranno messi a conoscenza nelle forme opportune, salvo i casi

di indagine per illeciti dove ciò potrebbe vanificare l'accertamento) e saranno circoscritti ai soli elementi necessari a verificare le violazioni ipotizzate. In qualunque momento, il dipendente ha diritto di accedere ai dati personali eventualmente raccolti che lo riguardino, secondo quanto previsto dall'art. 15 del GDPR, e di ottenere chiarimenti sul trattamento degli stessi.

Aggiornamento, entrata in vigore e diffusione del disciplinare

Il presente disciplinare interno entra in vigore dalla data di approvazione con disposizione del Dirigente Scolastico. Esso sarà pubblicato tramite i canali istituzionali dell'Istituto (albo online ed area del sito web contenente i regolamenti) e comunicato a tutti i dipendenti per opportuna conoscenza. Ciascun membro del personale è tenuto a prenderne visione e ad attenersi scrupolosamente alle norme in esso contenute.

Il disciplinare sarà oggetto di **aggiornamenti periodici**: almeno una volta all'anno l'Amministrazione ne riesaminerà i contenuti per verificarne l'attualità rispetto all'evoluzione normativa, tecnologica e organizzativa. Eventuali modifiche o integrazioni saranno tempestivamente sottoposte a verifica di conformità legale (coinvolgendo se necessario il DPO e le rappresentanze sindacali, in relazione agli aspetti di controllo a distanza) e quindi comunicate al personale con le stesse modalità del presente atto. In caso di innovazioni significative (ad esempio derivanti da nuove linee guida nazionali, da investimenti digitali del PNRR implementati nella scuola, da aggiornamenti del Piano Triennale ICT del Ministero, ecc.), l'Istituto provvederà a revisionare il disciplinare anche prima della scadenza annuale, per assicurare un costante allineamento alle **best practice** e alle prescrizioni vigenti.

La versione attuale del disciplinare annulla e sostituisce ogni precedente regolamentazione interna sull'uso di Internet, posta elettronica e strumenti informatici da parte del personale. Il Dirigente Scolastico vigilerà sulla corretta applicazione di quanto stabilito e promuoverà una cultura della sicurezza digitale e della legalità nell'uso delle tecnologie, a beneficio dell'intera comunità scolastica. Il presente documento viene adottato con **provvedimento del Dirigente Scolastico** ed è pronto per essere incluso nel novero dei regolamenti ufficiali dell'Istituto.

IL DIRIGENTE SCOLASTICO
Prof.ssa Stefania Acquaviva