Ministero dell'Istruzione e del Merito
Ufficio Scolastico Regionale per il Lazio
"ISTITUTO COMPRENSIVO 2 - via BARBARANELLI"
Via F. Barbaranelli, 3/3-a - 00053 CIVITAVECCHIA (RM) Tel. 0766.031868 Fax: 0766.546961
Cod.Fisc. 91038390588 - Cod.Mecc. RMIC8GN009 – www.iccivitavecchia2.edu.it
E-mail: rmic8gn009@istruzione.it – Pec: rmic8gn009@pec.istruzione.it

Circolare n.146

Civitavecchia, 11/12/2023

A tutto il personale docente e non docente dell'IC CIVITAVECCHIA 2

Agli Atti

Sul sito

Oggetto: Istruzioni operative e contestuale pubblicazione del Disciplinare Tecnico per l'utilizzo degli strumenti informatici della posta elettronica ed internet da parte dei dipendenti.

Le indicazioni sulla sicurezza delle informazioni relative all'utilizzo degli strumenti informatici, della posta elettronica ed internet sono contenute all'interno del Disciplinare Tecnico RGSI_01 rev. 24.11.23. Tale documento riporta la descrizione degli obblighi e delle facoltà per la Scuola, la definizione degli obblighi del lavoratore e le istruzioni operative ai dipendenti su: utilizzo di personal computer e device mobili in dotazione e personali, gestione delle password, uso della rete locale, accesso da remoto, uso della rete internet, utilizzo di account istituzionali e piattaforme cloud, utilizzo della posta elettronica, protezione degli strumenti, utilizzo di stampanti multifunzione e fotocopiatrici, utilizzo delle attrezzature dei laboratori, e costituisce parte integrante di questa circolare. Tutti i dipendenti sono invitati a prenderne visione tenendo presente che questa circolare comprende anche l'accettazione del Disciplinare, la cui presa visione comporta pertanto presa visione e accettazione delle istruzioni. Di seguito se ne riporta un estratto.

Gestione degli strumenti elettronici

I Personal Computer affidati in dotazione per lo svolgimento della prestazione lavorativa appartengono alla Scuola. Gli stessi sono strumenti di lavoro ed il loro utilizzo è consentito esclusivamente per lo svolgimento delle proprie mansioni e, in ogni caso, per finalità strettamente connesse con l'attività svolta. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione, e, soprattutto, minacce alla sicurezza dei dati personali e dell'Istituto. Di conseguenza gli utenti sono tenuti al rispetto delle seguenti regole:

- non usare impropriamente il sistema informativo e i dispositivi dell'Istituto (per esempio per diffusione o memorizzazione di inserzioni commerciali o personali, petizioni, pubblicità o per qualsiasi altro uso non autorizzato, come l'uso di strumenti non autorizzati per lo scambio di dati personali);

- non accedere o tentare l'accesso alle informazioni per le quali non si hanno privilegi;
- non è consentito l'utilizzo di programmi informatici, software ed altri applicativi diversi da quelli distribuiti ed installati ufficialmente dagli amministratori di sistema o dagli assistenti tecnici della Scuola;
- non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del Dirigente scolastico;
- non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro, se non con autorizzazione esplicita del Dirigente scolastico;
- per tutti i dati di interesse lavorativo, per cui si renda necessaria la garanzia della conservazione, deve essere utilizzata l'area condivisa sul server o, comunque, su tale area i dati devono essere copiati periodicamente. Nel caso in cui tale suggerimento non fosse seguito, è responsabilità dell'utente predisporre opportune misure di sicurezza per il salvataggio dei dati. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante;
- effettuare la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili.

Inoltre per la gestione della sessione di lavoro sul computer è necessario che:

- venga spento il PC al termine delle ore di servizio, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici devono essere necessariamente chiusi a chiave;
- in caso di assenza momentanea dalla propria postazione, accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone mediante chiusura della sessione di lavoro sul PC facendo il logout;
- nel caso in cui l'utente sia costretto ad assentarsi dall'ufficio o nel caso in cui egli ritenga di non essere in grado di presidiare l'accesso alla postazione dei lavoro, al fine di evitare che persone estranee effettuino accessi non permessi, deve essere quindi attivato sul computer un programma salvaschermo (screen saver) protetto da password;
- effettuare il logout dai programmi utilizzati e spegnere correttamente il computer al termine della sessione di lavoro, sia per garantire la protezione dei dati da accessi non autorizzati che per mantenere il corretto funzionamento del PC.

Utilizzo della posta elettronica

La casella di posta elettronica, assegnata dall'Istituto all'utente, è uno strumento di lavoro, pertanto la posta elettronica istituzionale deve essere utilizzata esclusivamente per lo svolgimento dell'attività lavorativa. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Con l'utilizzo della posta elettronica gli utenti assegnatari rappresentano l'Istituto all'esterno e, pertanto, sono tenuti ad osservare un comportamento professionale a tutela dell'immagine della Scuola.

Pertanto l'utente è tenuto a:

- prestare la massima attenzione nell'apertura dei file allegati alle e-mail (per esempio Word, Excel, PDF, ZIP, Immagini) poiché possibili veicoli di virus o ransomware;
- prestare la massima attenzione nell'apertura di link presenti nel corpo della e-mail, poiché potrebbero indirizzare a siti malevoli;
- non diffondere notizie a carattere riservato, né inviare documenti di lavoro a indirizzi di posta elettronica esterni alla rete informatica dell'Istituto, se non necessario per l'attività lavorativa, in considerazione del fatto che la posta può essere intercettata da chiunque;
- non utilizzare la casella di posta elettronica assegnata per l'invio di messaggi personali e completamente estranei al rapporto di lavoro o alle relazioni tra colleghi, per scaricare allegati contenenti video/brani musicali non funzionali all'attività lavorativa, per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione.

È buona norma:

- mantenere la casella di posta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti;
- nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari, rendere preventivamente questi allegati illeggibili attraverso la crittografia comunicando al destinatario la password di cifratura attraverso un Canale separato (per es. Sms, dettata al telefono, ecc).

Utilizzo di internet

L'utilizzo di internet è consentito esclusivamente per lo svolgimento dell'attività lavorativa ed è vietato ogni utilizzo difforme dagli scopi istituzionali o che possa arrecare danno all'immagine dell'Istituto. Per l'utilizzo della rete Internet possono essere impiegati esclusivamente gli applicativi "browser" (es. Internet Explorer, Mozilla Firefox, Chrome, ecc.) installati sulle postazioni di lavoro dal personale autorizzato dal DS. Non è consentito agli operatori effettuare sulle postazioni

l'installazione di qualsiasi altro applicativo per l'accesso alla rete pubblica, anche quando tale installazione risultasse tecnicamente possibile.

In generale, l'utente è tenuto a:

- utilizzare l'accesso alla rete internet senza mettere a rischio l'integrità, la riservatezza e la disponibilità dei dati, delle informazioni e dell'intero sistema informatico dell'Istituto;
- non visitare siti non attendibili poiché, dopo la posta elettronica, la navigazione internet rappresenta il veicolo principale per le minacce di sicurezza.

Si raccomanda di osservare le seguenti regole di comportamento:

- non è consentito scaricare software gratuito (freeware) e software gratuito per un certo periodo di prova (shareware) prelevato da siti Internet, file musicali o video da siti internet, se non espressamente autorizzato dal titolare;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano correlati all'attività lavorativa;
- è fatto divieto all'utente accedere a siti che offrano contenuti audio/video tramite streaming (stazioni radio – televisione on line, ecc.) se non espressamente autorizzati dal DS;
- non è consentita la partecipazione, per motivi non professionali, a forum, chat-line, bacheche elettroniche, nonché registrazioni in guest book anche utilizzando pseudonimi;
- è vietato l'utilizzo di servizi di comunicazione e condivisione file;
- non è consentita l'effettuazione di transizioni finanziarie, comprese le operazioni di remote banking, acquisti online e simili;
- non è consentito l'utilizzo di applicativi di messaggistica istantanea e di social network (es. whatsApp) per lo scambio di informazioni e dati di natura professionale; tali informazioni possono essere scambiate esclusivamente attraverso eventuali sistemi messi a disposizione dall'Istituto.

Utilizzo di account istituzionali

L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'Istituto. Pertanto è vietato:

- utilizzare l'account istituzionale per registrarsi ad un servizio, applicazioni e siti web, che hanno natura e finalità non riconducibili all'attività istituzionale della Scuola e/o che hanno scopi pubblicitari e commerciali;
- consentire ad altri, a vario titolo, l'utilizzo delle piattaforme digitali per l'amministrazione e la didattica adottate dall'Istituto utilizzando il proprio account istituzionale;
- diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano gli stessi servizi digitali della Scuola;
- utilizzare gli account istituzionali e le relative piattaforme in modo da danneggiare, molestare o insultare altre persone;
- tramite gli account istituzionali creare e trasmettere: immagini, dati o materiali offensivi, osceni o indecenti e materiale pubblicitario.

L'utente autorizzato è tenuto a:

- modificare la password unica fornita e impostarne una nuova personale;
- sostituire con periodicità la password;
- conservare la password personale e non consentirne l'uso ad altre persone;
- non memorizzare la password per utilizzi successivi della piattaforma o per altre applicazioni che lo propongono ed al termine delle operazioni effettuare sempre il logout;
- comunicare immediatamente all'amministratore di sistema ed al team animatore digitale l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;
- utilizzare i servizi offerti solo ad uso esclusivo per le attività amministrative e didattiche della scuola.

Uso dei dispositivi mobili

I dispositivi mobili forniti dalla Scuola rappresentano di fatto delle estensioni del network dell'Istituto al di fuori del suo perimetro fisico. Pertanto, se vulnerabili, possono esporre l'Istituto a rischi di sicurezza informatica. Come i PC nelle postazioni fisse anche i device sono strumenti di lavoro ed il loro utilizzo è consentito esclusivamente per lo svolgimento delle proprie mansioni e, in ogni caso, per finalità strettamente connesse con l'attività svolta. Eventuali utilizzi che non rientrano nella mansione lavorativa possono contribuire ad innescare problemi al servizio, costi di manutenzione, e, soprattutto, minacce per la protezione dei dati personali. Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete locale, con le seguenti ulteriori raccomandazioni:

- non lasciarli mai incustoditi sia nei locali dell'ente che all'esterno;
- in caso di assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno (es. cassaforte);

Ministero dell'Istruzione e del Merito
Ufficio Scolastico Regionale per il Lazio
"ISTITUTO COMPRENSIVO 2 - via BARBARANELLI"
Via F. Barbaranelli, 3/3-a - 00053 CIVITAVECCHIA (RM) Tel. 0766.031868 Fax: 0766.546961
Cod.Fisc. 91038390588 - Cod.Mecc. RMIC8GN009 – www.iccivitavecchia2.edu.it
E-mail: rmic8gn009@istruzione.it – Pec: rmic8gn009@pec.istruzione.it

- in caso di furto di uno strumento è necessario avvertire tempestivamente il Dirigente Scolastico che, sentito il DPO, valuterà il rischio per le libertà ed i diritti delle persone interessate connesso al relativo data breach ed adotterà le necessarie misure per prevenire ulteriori conseguenze sulla sicurezza della rete locale;
- avere sempre cura della strumentazione affidata garantendone la custodia temporanea anche per lo svolgimento di attività lavorative al di fuori della sede dell'Istituto (corsi di formazione, smart working, ecc..);
- eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile;
- evitare di connettersi a reti wi-fi pubbliche e comunque non adeguatamente protette e in assenza di condizioni ambientali di sicurezza (es. utilizzo di un collegamento VPN, protezione del dispositivo mediante password adeguata).

La Dirigente Scolastica
Prof.ssa De Luca Francesca
(Firma autografa sostitutiva a mezzo stampa
ai sensi dell'art. 3co.2 del D.lgs. n. 39/93)

ISTITUTO COMPRENSIVO CIVITAVECCHIA 2

Via Barbaranelli 3-3A - 00053 Civitavecchia (RM)

Cod.Fisc.91038390588 - Cod.Mecc. RMIC8GN009 - www.iccivitavecchia2.edu.it

E-mail:rmic8gn009@istruzione.it – Pec: rmic8gn009@pec.istruzione.it

Disciplinare interno per l'utilizzo degli strumenti informatici della posta elettronica ed internet

Regolamento UE 2016/679

Identificazione del documento

Codice: RGSI_01
Titolo: Disciplinare interno per l'utilizzo degli strumenti informatici della posta elettronica ed internet

Stato delle edizioni

	Rev.	*Motivo della edizione*	Data
Edizione n°1	1	Prima emissione	29.11.23

Redazione e verifica

		Firma
Redatto e verificato	Responsabile Protezione dati Ing. Manuela Buratti	Firmato digitalmente da: MANUELA BURATTI Data: 29/11/2023 19:56:03 *Manuela Buratti*

Validazione e Approvazione

		Firma
Validato e approvato	Titolare del trattamento Istituto Comprensivo Civitavecchia 2 Firma del DS	Firmato dal Dirigente Scolastico Prof.ssa Francesca De Luca 04/12/2023 13:56:20

"Policy sull'utilizzo delle attrezzature informatiche, posta elettronica ed internet"

Una policy interna sull'utilizzo delle attrezzature informatiche rappresenta uno strumento organizzativo utile al titolare del trattamento al fine di fornire alle persone autorizzate (addetti) un'adeguata formazione nell'ambito del trattamento dei dati

Sommario

1. Premessa

Tale regolamento è volto a conformare i comportamenti degli utenti ai principi generali di diligenza e correttezza, per evitare e prevenire condotte, anche inconsapevoli, che potrebbero minacciare la sicurezza nel trattamento dei dati o comportare rischi alla sicurezza del sistema informatico e all'immagine della Scuola. L'Istituzione scolastica, in quanto datore di lavoro, è tenuta ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi. D'altro canto ai dipendenti è riservato l'obbligo, sancito da norme di legge (anche di rilevanza penale) e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli ai beni mobili ed agli strumenti ad essi affidati, tra i quali vi sono le attrezzature ICT ed i sistemi informativi messi a disposizione dall'Istituto. Al riguardo, si ritiene opportuno ricordare, oltre alle disposizioni del Codice disciplinare contenuto nei contratti collettivi di comparto (che dispongono sanzioni in caso di *"negligenza nella cura dei locali e dei beni mobili o strumenti a lui affidati o sui quali, in relazione alle sue responsabilità, debba espletare azione di vigilanza"*), anche il dettato del Codice di comportamento dei dipendenti delle pubbliche amministrazioni di cui al Decreto del Ministro per la funzione pubblica del 28 novembre 2000 che, ove richiamato dal Codice disciplinare dei CCNL dei diversi comparti, costituisce, oltre che norma di valenza etico-comportamentale, anche vero e proprio obbligo la cui inosservanza da parte dei dipendenti è passibile di sanzione. In particolare, l'art. 10, comma 3, del Codice di comportamento dispone che *"Il dipendente non utilizza a fini privati materiale o attrezzature di cui dispone per ragioni di ufficio."* Pertanto, l'utilizzo delle risorse ICT da parte dei dipendenti, oltre a non dover compromettere la sicurezza e la riservatezza del Sistema informativo, non deve pregiudicare ed ostacolare le attività della Scuola od essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.

Anche il Garante per protezione dei dati personali ha fornito specifiche linee guida per l'utilizzo dei sistemi aziendali nei luoghi di lavoro (deliberazione del 1° marzo 2007, n. 13 (pubblicato in G.U. n. 58 del 10 marzo 2007 riguardante le linee guida per l'utilizzo della posta elettronica e di internet) che, lasciando da parte i profili di illecito penale e/o disciplinare sopra richiamati, costituiscono un sicuro punto di riferimento e regolamentazione delle modalità di utilizzo del Sistema informativo delle pubbliche amministrazioni da parte dei dipendenti nell'ambito del rapporto di lavoro. La deliberazione, nel definire, per i datori di lavoro, le regole in materia di trattamento dei dati personali raccolti in occasione delle attività di verifica del corretto utilizzo della rete Internet e del sistema di posta elettronica da parte dei lavoratori, fissa dei principi che non riguardano esclusivamente la tutela della privacy ma riprendono anche le disposizioni contenute nel "Codice dell'amministrazione digitale".

In sintesi, come definito anche dalle linee guida del Garante, il datore di lavoro (secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104), può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro. Nell'esercizio di tali prerogative, tuttavia, deve rispettare la libertà e la dignità dei lavoratori, tenendo presente, al riguardo, quanto disposto dalle norme poste a tutela del lavoratore (ci si riferisce, in particolare, al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* di cui all'art. 4 della legge n. 300 del 1970).

2. Finalità e ambito di applicazione

Il presente documento definisce e detta agli utenti specifiche regole e condizioni di utilizzo degli strumenti informatici in uso attraverso:

- la definizione di regole e procedure uniformi da applicarsi in tutte le aree operative;
- l'indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;
- la definizione dell'ambito, delle modalità e dei limiti del monitoraggio e dei controlli attuabili dall'agenzia nel rispetto della normativa vigente nonché delle regole e delle procedure interne;

- l'individuazione delle responsabilità degli utenti in caso di inosservanza di regole e prescrizioni.

Pertanto scopo del presente regolamento interno è quello di fornire determinate istruzioni operative sull'utilizzo degli strumenti informatici da parte degli addetti autorizzati al trattamento dei dati personali (dipendenti, collaboratori, consulenti ed in generale tutte le persone che sono assegnatarie di risorse informatiche dell'ente e che sono autorizzate ad accedere ai dati personali ed a svolgere operazioni di trattamento relative ai dati personali). Tale policy inoltre è finalizzata a far condividere al personale le scelte attuate dal titolare per consentire di migliorare la sicurezza del sistema adottato per la protezione dei dati. Infatti nessuna misura di sicurezza può essere ritenuta efficace, se agli operatori autorizzati non vengono forniti gli strumenti fondamentali per la sua realizzazione. Inoltre mediante la condivisione delle semplici regole contenute nella presente policy si promuove anche la sensibilizzazione degli addetti autorizzati sul tema più generale della sicurezza delle informazioni e della protezione dei dati personali, ponendo l'attenzione delle persone autorizzate nei confronti dell'utilizzo delle apparecchiature informatiche, sia nella vita professionale ma anche in ambito personale.

3. Glossario e definizioni

Ai fini del presente documento si intende per:

- **Amministratori di sistema**: figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;

- **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);

- **Dati personali relativi a condanne penali e reati** ("dati giudiziari"): dati che rendono identificabile la condizione di imputato o indagato dell'interessato e/o dati relativi a provvedimenti penali di condanna;

- **Categorie particolari di dati personali** ("dati sensibili"): dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare, in modo univoco, una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

- **Interessato:** la persona fisica cui si riferiscono i dati personali;

- **Credenziali di autenticazione**: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

- **Dispositivi mobili**: apparecchi di telecomunicazione portatili (tablet, smartphone, etc.);

- **File di log**: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;

- **ICT e strumenti ICT:** tecnologie dell'informazione e della comunicazione, si intendono tutti i processi e le pratiche connesse alla trasmissione, ricezione ed elaborazione dei dati e delle informazioni

– Tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni;

- **Postazione di lavoro (PdL):** personal computer (desktop o portatile) messo a disposizione dall'Agenzia a ciascun Utente per l'espletamento dell'attività lavorativa;
- **Strumenti informatici**: personal computer fissi o portatili, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
- **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali;
- **Responsabile del trattamento**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- **Titolare del trattamento**: persona fisica o giuridica, autorità pubblica o altro organismo che determina le finalità e i mezzi del trattamento di dati personali;
- **Addetti autorizzati del trattamento**: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile – sono addetti autorizzati tutti i docenti, gli assistenti amministrativi e tecnici ed i collaboratori scolastici – l'addetto autorizzato in base alla propria funzione ed ai compiti assegnati riceve dalla Scuola l'autorizzazione a svolgere determinate operazioni (e complessi di operazioni) che hanno per oggetto dati personali di terzi (trattamento di dati);
- **Utenti**: personale dipendente, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro in essere a qualsiasi titolo con la Scuola, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione dall'Istituto;
- **Violazione di dati personali**: violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.

4. Normativa di riferimento

Hanno supportato la stesura del presente documento le seguenti normative di riferimento:

— Normativa in materia di protezione dei dati personali, che comprende in particolare il Regolamento UE 679/2016, il D.lgs.101/2018, ed alcuni Provvedimenti Generali del Garante per la Protezione dei Dati Personali, tra cui soprattutto la deliberazione del 1° marzo 2007, n. 13 (pubblicato in G.U. n. 58 del 10 marzo 2007 riguardante le linee guida per l'utilizzo della posta elettronica e di internet);
— Legge n.300 del 20 maggio 1970 "Statuto dei lavoratori" e la Legge n.183/2014 (c.d. Jobs act) e ss.mm.ii. che garantiscono il rispetto dei diritti dei lavoratori sul posto di lavoro e l'assenza di qualsiasi controllo invasivo;

- D. lgs. 10.9.2003, n. 276 Attuazione delle deleghe in materia di occupazione e mercato del lavoro, di cui alla legge 14 febbraio 2003, n. 30;
- Decreto Legislativo 14 settembre 2015, n. 151 Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183;
- DPR 81/2023 Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165»;
- DPR 62/2013 (Codice di comportamento dei dipendenti pubblici) Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165.

5. Obblighi e facoltà per la Scuola

L'Istituzione scolastica ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali. In base all'art.12 c.3-bis del D.lgs.82/2005 l'Amministrazione favorisce l'uso di dispositivi elettronici personali da parte dei lavoratori al fine esclusivo di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo.

La facoltà per il titolare di accedere ai dati (principalmente file di LOG) creati nel corso dell´attività lavorativa e cancellarli, nonché la facoltà di accedere, raccogliere, conservare (individuando tempi di conservazione proporzionati allo scopo della raccolta), comunicare e cancellare le informazioni comunque presenti all´interno degli strumenti utilizzati (dunque, in ipotesi, anche di natura privata), in occasione del verificarsi di eventi determinati (es. richieste dell'autorità giudiziaria o della polizia giudiziaria, evento dannoso o di pericolo che richieda un immediato intervento, utilizzo anomalo degli strumenti da parte degli utenti, evidenza o comunque fondato sospetto che sia in corso o sia stato posto in essere un illecito) ed in presenza delle necessarie misure di garanzia, dovrà essere conforme ai principi di liceità, necessità, pertinenza e non eccedenza dei trattamenti.

A tale scopo la Scuola adotterà ogni misura atta a garantire la sicurezza e la protezione delle informazioni e dei dati, tenendo conto delle migliori pratiche e degli standard nazionali, europei e internazionali per la protezione delle proprie reti, nonché sull'uso sicuro dei dispositivi, attraverso un'adeguata informazione al lavoratore e anche con la diffusione di apposite linee guida, e disciplinando l'uso di specifici strumenti, dal cui utilizzo improprio possono derivare sia un controllo illegittimo sull'attività del lavoratore che maggiori rischi per la tutela della riservatezza (es webcam e microfoni).

6. Obblighi per il lavoratore

Nei paragrafi che seguono vengono specificati gli obblighi e le norme di condotta obbligatorie per ciascun lavoratore e per tutti coloro che, in virtù di un rapporto di lavoro o fornitura, trattano informazioni ovvero utilizzano sistemi informativi o apparecchiature elettroniche di proprietà della Scuola.

Il presente regolamento si applica anche nel caso di Lavoro agile (o Smart working): istituto disciplinato dalla legge 22 maggio 2017 n. 81 (Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato), al Capo II, ed in particolare dall'art. 18 all'art. 23. Lo Smart Working è una: «tipologia di lavoro senza precisi vincoli di orario o di luogo di

lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa». Nel caso di utilizzo di strumenti messi a disposizione dalla Scuola, che consentano di lavorare da remoto, il dipendente in Smart Working è personalmente responsabile della sicurezza, custodia e conservazione in buono stato, salvo l'ordinaria usura derivante dall'utilizzo, delle dotazioni informatiche eventualmente fornitegli dall'Istituto scolastico. Le dotazioni informatiche della Scuola devono essere utilizzate esclusivamente per ragioni di servizio e non devono subire alterazioni della configurazione di sistema, ivi inclusa la parte relativa alla sicurezza, e su queste non devono essere effettuate installazioni di software non autorizzate.

In generale ai lavoratori è consentito utilizzare anche i propri dispositivi personali come smartphone, tablet o pc portatili sul posto di lavoro per avere accesso alle informazioni necessarie a svolgere le funzioni assegnate al proprio ruolo ovvero per svolgere l'attività lavorativa. Quindi solo per finalità strettamente connesse alla didattica la Scuola concede ai dipendenti ed ai collaboratori di accedere alla rete wi-fi interna e in nessun caso è consentito accedervi per finalità contrastanti con quelle della Scuola. Inoltre l'utilizzo di tali dispositivi dovrà avvenire in modo da garantire la sicurezza dei dati personali ivi contenuti e di rispettare la riservatezza dei dipendenti stessi.

Infatti tutti questi strumenti informatici, in particolare smartphone e tablet, che oltre alle chiamate vocali ed ai messaggi di testo, offrono la possibilità di utilizzare i servizi Internet (social network, condivisione di contenuti, ecc.) e dispongono di molti sensori che forniscono una crescente quantità di informazioni, hanno un grande impatto su diversi aspetti relativi ai dati personali, ovvero, ad esempio, la conservazione, la trasmissione e, soprattutto, la sicurezza, andando a creare altre fonti di rischio per l'Amministrazione scolastica che deve costantemente monitorarli.

In particolare riguardo alla sicurezza si evidenziano le seguenti criticità:

- gli utenti che utilizzano dispositivi mobili per motivi di lavoro spesso non sono consapevoli che un'azione sul dispositivo mobile può comportare un trattamento di dati personali, soggetto quindi alle condizioni e ai limiti del Regolamento UE 2016/679 ("GDPR");
- i dispositivi mobili consentono l'uso di applicazioni che comunicano dati, talvolta, senza che gli utenti o l'Istituto scolastico ne siano a conoscenza;
- pertanto gli utenti possono perdere o divulgare dati gestiti dall'Istituto involontariamente (caso di furto o perdita del dispositivo non adeguatamente protetto, disponibilità permanente dei dati in seguito a dimissioni o cessazione del rapporto di lavoro, sostituzione del dispositivo senza aver eseguito la cancellazione efficace dei dati, promiscuità dell'uso del dispositivo che può comportare la diffusione di dati o l'introduzione di virus che possono danneggiare i dati);
- nel momento in cui i dipendenti utilizzano i propri dispositivi privati per scopi professionali si presentano ulteriori problemi di protezione dei dati personali, in quanto viene utilizzato lo stesso dispositivo sia per comunicazioni sia personali e sia della Scuola - L'Istituto non può esercitare lo stesso livello di controllo, che applicano sui dispositivi aziendali, sui dispositivi privati.

Al fine di assicurare la compliance alla normativa e garantire il rispetto dei principi fondamentali, il lavoratore che intende svolgere attività lavorative con il proprio device dovrà attenersi alle seguenti regole:

- seguire le procedure adottate dalla Scuola per la gestione delle autorizzazioni di accesso alla rete informatica interna con il proprio device mobile;
- utilizzare PIN/password per l'accesso al dispositivo mobile e ad applicazioni specifiche;
- utilizzare firewall e applicazioni anti-malware sul dispositivo mobile;
- effettuare gli aggiornamenti tempestivi del software del dispositivo mobile e delle applicazioni installate su di esso;
- effettuare il backup periodico delle informazioni di carattere lavorativo ed istituzionali nel dispositivo mobile;

- verificare che il dispositivo sia in grado di connettersi alla rete prima di accedere alle risorse aziendali (verifica di conformità);
- per talune categorie di dati che per loro natura sono estremamente sensibili (dati sulla salute) crittografare i dati nel dispositivo ed assicurarsi che anche i dati in transito siano protetti (crittografia delle comunicazioni);

inoltre dovrà accertarsi di:

— aver ricevuto la convalida alla connessione di rete con il proprio dispositivo mobile, essendo stato previamente autorizzato, attraverso l'esecuzione dell'apposita procedura approvata dall'Istituto;
— aver ricevuto credenziali di autenticazione alla rete wi-fi al fine di monitorare gli accessi degli utenti e garantire l'uso corretto di internet;
— aver firmato per ricevuta il relativo verbale di convalida alla connessione e di ricezione delle credenziali di autenticazione.

7. Entrata in vigore della policy e la pubblicità

Il presente Regolamento è soggetto a revisione ed aggiornamento quando necessario; entra in vigore con la sua formale adozione da parte del DS, previo accordo con i rappresentanti dei lavoratori. La Policy è portata a conoscenza degli utenti e disponibile per la consultazione tramite i mezzi di comunicazione interna utilizzati dall'Istituto (circolare, sito). Ai nuovi assunti saranno comunicate le modalità per la sua consultazione contestualmente alla data di assunzione.

8. Utilizzo del personal computer

I Personal Computer affidati in dotazione per lo svolgimento della prestazione lavorativa appartengono alla Scuola. Gli stessi sono strumenti di lavoro ed il loro utilizzo è consentito esclusivamente per lo svolgimento delle proprie mansioni e, in ogni caso, per finalità strettamente connesse con l'attività svolta. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione, e, soprattutto, minacce alla sicurezza dei dati personali e dell'Istituto.

Di conseguenza gli utenti sono tenuti al rispetto delle seguenti regole:

- Non è consentito l'utilizzo di programmi informatici, software ed altri applicativi diversi da quelli distribuiti ed installati ufficialmente dagli amministratori di sistema o dagli assistenti tecnici della Scuola.
- Solo il personale incaricato, che opera come tecnico autorizzato alla gestione della sicurezza dei sistemi, può compiere interventi nel sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.). L'inosservanza della presente disposizione espone inoltre la stessa Scuola a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.
- Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del Dirigente scolastico.
- Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro, se non con autorizzazione esplicita del Dirigente scolastico.
- Ogni utente deve prestare la massima attenzione ai supporti di origine esterna (il cui utilizzo deve essere evitato il più possibile e deve essere limitato a casi strettamente autorizzati dal DS), avvertendo

immediatamente l'amministratore di sistema e gli assistenti tecnici nel caso in cui vengano rilevati malware e virus.

- Per tutti i dati di interesse lavorativo, per cui si renda necessaria la garanzia della conservazione, deve essere utilizzata l'area condivisa sul server o, comunque, su tale area i dati devono essere copiati periodicamente. Nel caso in cui tale suggerimento non fosse seguito, è responsabilità dell'utente predisporre opportune misure di sicurezza per il salvataggio dei dati. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante.
- Effettuare la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili.

8.1 Per la gestione della sessione di lavoro sul computer è necessario:

- Il PC deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo.
- Spegnere il PC al termine delle ore di servizio, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici devono essere necessariamente chiusi a chiave.
- In caso di assenza momentanea dalla propria postazione, accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone mediante chiusura della sessione di lavoro sul PC facendo il logout.
- Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità o di provarne in seguito l'indebito uso. Pertanto l'utente è tenuto a scollegarsi dal sistema/rete ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima al fine di evitare che persone estranee effettuino accessi non permessi. Deve essere quindi attivato sul computer un programma salvaschermo (screen saver) protetto da password.
- Effettuare il logout dai programmi utilizzati e spegnere correttamente il computer al termine della sessione di lavoro, sia per garantire la protezione dei dati da accessi non autorizzati che per mantenere il corretto funzionamento del PC.

8.2 Per i controlli tecnici e gli interventi di manutenzione:

Il personale incaricato dell'assistenza tecnica ai sistemi informativi ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

9. Utilizzo di PC portatili

I device (smartphone, tablet, stampanti, notebook, ecc....) affidati in dotazione all'utente sono di esclusiva proprietà dell'Istituto. Come i PC nelle postazioni fisse anche i device sono strumenti di lavoro ed il loro utilizzo è consentito esclusivamente per lo svolgimento delle proprie mansioni e, in ogni caso, per finalità strettamente connesse con l'attività svolta. Eventuali utilizzi che non rientrano nella mansione lavorativa possono contribuire ad innescare problemi al servizio, costi di manutenzione, e, soprattutto, minacce per la protezione dei dati personali.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete locale, con le seguenti ulteriori raccomandazioni:

- non lasciarli mai incustoditi sia nei locali dell'ente che all'esterno;
- in caso di assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno (es.cassaforte);
- in caso di furto di uno strumento è necessario avvertire tempestivamente il Dirigente Scolastico che, sentito il DPO, valuterà il rischio per le libertà ed i diritti delle persone interessate connesso al relativo data breach ed adotterà le necessarie misure per prevenire ulteriori conseguenze sulla sicurezza della rete locale;
- avere sempre cura della strumentazione affidata garantendone la custodia temporanea anche per lo svolgimento di attività lavorative al di fuori della sede dell'Istituto (corsi di formazione, smart working, ecc..);
- eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile;
- evitare di connettersi a reti wi-fi pubbliche e comunque non adeguatamente protette e in assenza di condizioni ambientali di sicurezza (es. utilizzo di un collegamento VPN, protezione del dispositivo mediante password adeguata).

10. Gestione ed assegnazioni delle password

Ogni utente autorizzato accede alla rete locale della Scuola ed al proprio personal computer mediante un sistema di autenticazione che richiede all'utente di inserire un codice (user ID) ed una parola chiave (password).

Ciascun utente deve:

- ✓ modificare, alla prima connessione, la password generata dall'amministratore di sistema;
- ✓ cambiare la password ogni 3 mesi oppure immediatamente nel caso in cui sospetti che la password abbia perso la segretezza, dando comunicazione dell'incidente all'amministratore di sistema, e, comunque, ogni qual volta viene richiesto per impostazione predefinita ed in modo automatico dal sistema di autenticazione associato all'utilizzo di un software o di un applicativo;
- ✓ utilizzare password di almeno 8 caratteri (e comunque di lunghezza pari a quella massima consentita dal software utilizzato) costituiti da una combinazione di numeri e/o caratteri speciali, lettere (almeno una maiuscola ed una minuscola) – tenendo presente che una password complessa è costituita da almeno 14 caratteri;
- ✓ scegliere password che non contengono riferimenti ad informazioni agevolmente riconducibili all'utente o ai suoi familiari, come ad esempio il nome ed il cognome;
- ✓ evitare password uguali alle precedenti utilizzate;
- ✓ proteggere la riservatezza della password conservandola in luogo sicuro, non rilevandola o condividendola con i colleghi di lavoro, familiari e amici;
- ✓ non trascrivere la password su supporti facilmente accessibili a terzi soprattutto in prossimità della postazione di lavoro utilizzata (ad esempio le password non devono essere annotate su foglietti custoditi nei pressi della postazione o sotto la testiera);
- ✓ non utilizzare la funzione di salvataggio automatico della password per successivi utilizzi delle applicazioni;
- ✓ non usare la stessa password per l'accesso a sistemi ed applicativi differenti.

11. Uso della rete locale

La rete telematica locale è l'insieme delle tecnologie – apparati e programmi – mediante le quali si realizza la connettività interna tra i vari componenti del sistema informatico interno. La perfetta e continuativa disponibilità della stessa è quindi fattore strategico per il funzionamento operativo dell'Istituto. Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi da quelli per cui sono state predisposte. Pertanto, qualunque applicazione o file ad essa correlato che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in dette unità di rete. Su di esse, inoltre, vengono regolarmente svolte attività di controllo, amministrazione e backup. La Scuola effettua il backup dei dati in modo automatico, prevedendo per gli utenti esclusivamente la copia di sicurezza della cartella "condivisa" del server. Pertanto gli addetti sono tenuti ad utilizzare puntualmente le informazioni presenti sui server e non sui terminali, in modo da garantire un accesso ed un salvataggio sicuro delle informazioni. Ciascun file di lavoro salvato all'esterno della suddetta cartella non verrà salvato e, in caso di malfunzionamenti, potrebbe essere irrimediabilmente perso. Perciò, è fatto specifico obbligo a ciascun dipendente di salvare i file inerenti alle attività di lavoro esclusivamente nella cartella "condivisa" del server. Le password d'ingresso alla rete e ai programmi di rete sono segrete e vanno comunicate e gestite secondo le procedure in precedenza impartite. È fatto assoluto divieto di entrare nella rete interna e nei programmi utilizzando credenziali di autenticazione di qualsiasi altro utente. L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di ogni applicazione che dovesse ritenere pericolosa per la sicurezza, sia sui PC degli addetti autorizzati che sulle unità di rete. È cura del lavoratore effettuare la stampa dei dati solo se strettamente necessaria alle esigenze di lavoro e di ritirarla prontamente dai vassoi delle stampanti di rete messe in comune. Nel caso si debbano stampare informazioni riservate, è fatto obbligo di presidiare personalmente l'area ove avviene la stampa. Per quanto attiene la cura degli strumenti di stampa, il lavoratore è tenuto a segnalare prontamente qualsiasi malfunzionamento direttamente agli assistenti tecnici incaricati della gestione della sicurezza dei sistemi informatici. È buona regola, infine, evitare di stampare su stampanti comuni documenti o file non adatti. In caso di necessità, la stampa in corso può essere cancellata.

Alla luce di ciò, è fatto esplicito divieto di:

- utilizzare la rete interna dell'Istituto per fini non espressamente previsti e/o autorizzati;
- connettere in rete locale apparecchiature elettroniche (PC, stampanti, ecc.) o altri qualsiasi altro genere di apparato (router, switch, ecc.) che possa alterare la configurazione della rete interna e/o danneggiare le applicazioni.

La Scuola si riserva il diritto di rimuovere, senza alcun preavviso, qualsiasi tipologia di apparecchiatura elettronica o di software installato sulla rete interna e che non sia stato in precedenza autorizzato.

12. Accesso da remoto

É vietato agli utenti collegare alla rete informatica della Scuola (sia in modalità wired che wireless) strumenti Informatici che non siano stati configurati e/o preventivamente autorizzati dalla Scuola. É fatto divieto agli utenti di installare qualsiasi tipologia di dispositivo di rete all'infrastruttura dell'Istituto scolastico. Gli strumenti Informatici non devono mai essere connessi contemporaneamente alla rete aziendale e a reti esterne. Nell'utilizzo degli strumenti informatici di proprietà della Scuola, qualora non automaticamente impedito dal sistema, non è consentito utilizzare reti WIFI pubbliche (hotel, stazioni, hot spot gratuiti e a pagamento). Il collegamento alla rete informatica interna alla Scuola di strumenti informatici personali è consentito

esclusivamente previo esplicita autorizzazione della Dirigenza, dopo aver consultato l'amministratore di sistema ed i tecnici responsabili della gestione della sicurezza informatica.

13. Disposizioni per il lavoro agile (smart working)

- Il lavoratore deve disporre di idonea dotazione tecnologica.
- Per le attività da remoto devono essere utilizzate le postazioni di lavoro fornite dall'amministrazione, in grado di garantire la protezione delle risorse aziendali a cui il lavoratore deve accedere.
- L'Istituzione scolastica deve assicurare il costante aggiornamento dei meccanismi di sicurezza, nonché il monitoraggio del rispetto dei livelli minimi di sicurezza.
- In alternativa, previo accordo con il datore di lavoro, possono essere utilizzate anche dotazioni tecnologiche del lavoratore che rispettino i requisiti di sicurezza di cui al periodo precedente.
- L'accesso alle risorse digitali ed alle applicazioni dell'amministrazione raggiungibili tramite la rete internet deve avvenire attraverso sistemi di gestione dell'identità digitale (sistemi Multi factor authentication, tra i quali, ad esempio, CIE e SPID), in grado di assicurare un livello di sicurezza adeguato e tramite sistemi di accesso alla rete predisposti sulla postazione di lavoro in dotazione in grado di assicurare la protezione da qualsiasi minaccia proveniente dalla rete (c.d. zero trust network).
- Inoltre si dovrà ricorrere all'attivazione di una VPN (Virtual Private Network, una rete privata virtuale che garantisce privacy, anonimato e sicurezza) verso l'ente.

Inoltre, al fine di garantire adeguati livelli di sicurezza e protezione della rete ed in base alle raccomandazioni del Cert-PA dell'Agenzia per l'Italia Digitale (AgID), i lavoratori che hanno adottato la modalità di lavoro agile e che per lo svolgimento delle attività lavorative sono autorizzati ad utilizzare i propri dispositivi personali (pc, smartphone, tablet) sono obbligati a:

1. Seguire prioritariamente le policy e le raccomandazioni dettate dall'Amministrazione scolastica di appartenenza;
2. Utilizzare i sistemi operativi per i quali attualmente è garantito il supporto;
3. Effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo in uso;
4. Assicurarsi che i software di protezione del proprio sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati;
5. Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla propria Amministrazione;
6. Non installare software proveniente da fonti/repository non ufficiali;
7. Bloccare l'accesso al sistema e/o configurazione della modalità di blocco automatico in caso di allontanamento dalla postazione di lavoro;
8. Non cliccare su link o allegati contenuti in email sospette;
9. Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;
10. Collegarsi a dispositivi mobili (pen-drive, hd-esterno, etc) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione);

11. Effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa la propria sessione lavorativa;
12. Evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di prestazione fuori sede;
13. Bloccare l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
14. Qualora non si utilizzino dispositivi forniti dal titolare del trattamento si proceda ad installare almeno un buon sistema antivirus e ad effettuare un'accurata scansione preventiva;
15. Evitare l'uso dei social network, o altre applicazioni social facilmente hackerabili;
16. Adoperare "misure di sicurezza" nell'utilizzo di pc o tablet come paraschermi (privacy-screen) che impediscano la visuale laterale del vicino, per proteggere le informazioni trattate da accessi non autorizzati;
17. Evitare il collegamento a reti non sicure o sulle quali non si abbiano adeguate garanzie.

14. Uso della rete internet

La postazione di lavoro dell'utente è abilitata alla navigazione in internet. L'utilizzo di internet è consentito esclusivamente per lo svolgimento dell'attività lavorativa ed è vietato ogni utilizzo difforme dagli scopi istituzionali o che possa arrecare danno all'immagine dell'Istituto. La vasta gamma di attività istituzionali non permette la possibilità di definire un elenco di siti autorizzati.

L'Istituto si riserva, tuttavia, la facoltà di implementare, tramite l'amministratore di sistema, sistemi di filtraggio mediante i quali può essere inibita la navigazione su siti o categorie di siti i cui contenuti non sono consentiti (Firewall).

È vietato, comunque, l'accesso a qualunque altro sito che, pur consentito dal sistema, non sia collegato o collegabile alle attività istituzionali della Scuola.

Per l'utilizzo della rete Internet possono essere impiegati esclusivamente gli applicativi "browser" (es. Internet Explorer, Mozilla Firefox, Chrome, ecc.) installati sulle postazioni di lavoro dal personale autorizzato dal DS. Non è consentito agli operatori effettuare sulle postazioni l'installazione di qualsiasi altro applicativo per l'accesso alla rete pubblica, anche quando tale installazione risultasse tecnicamente possibile.

Si raccomanda di osservare le seguenti regole di comportamento:

- Non è consentito scaricare software gratuito (freeware) e software gratuito per un certo periodo di prova (shareware) prelevato da siti Internet, file musicali o video da siti internet, se non espressamente autorizzato dal titolare;
- È fatto divieto all'utente accedere a siti che offrano contenuti audio/video tramite streaming (stazioni radio – televisione on line, ecc.) se non espressamente autorizzati dal DS;
- È vietata ogni forma di registrazione a siti i cui contenuti non siano correlati all'attività lavorativa;
- non è consentita la partecipazione, per motivi non professionali, a forum, chat-line, bacheche elettroniche, nonché registrazioni in guest book anche utilizzando pseudonimi;

- È vietato l'utilizzo di servizi di comunicazione e condivisione file;
- Non è consentita l'effettuazione di transizioni finanziarie, comprese le operazioni di remote banking, acquisti online e simili - ne è però ammesso l'utilizzo, che dovrà essere espressamente autorizzato dal DS, per assolvere proprie incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari ed assicurativi) - Tale modalità di utilizzazione di Internet deve essere contenuta nei tempi strettamente necessari allo svolgimento delle transazioni/comunicazioni e privilegiando, quando possibile, l'utilizzo delle pause di lavoro - Il fine è quello di contribuire a ridurre gli spostamenti della persone e gli oneri logistici e di personale a carico dell'Istituzione scolastica che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi;
- Non è consentito l'utilizzo delle risorse del server per la memorizzazione di materiale privato, personale o non attinente all'attività lavorativa;
- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria;
- Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- Non è consentito l'utilizzo di applicativi di messaggistica istantanea e di social network (es whatsApp) per lo scambio di informazioni e dati di natura professionale; tali informazioni possono essere scambiate esclusivamente attraverso eventuali sistemi messi a disposizione dall'Istituto;
- L'accesso alle risorse del sistema intranet dall'esterno è consentito esclusivamente tramite un collegamento che necessita di autenticazione VPN (Virtual Private Network) ovvero solo gli utenti autorizzati vi possano accedere. L'abilitazione e le credenziali di accesso vengono forniti dall'amministratore di sistema, laddove presente, o dal personale tecnico autorizzato alla gestione della sicurezza dei sistemi informativi, previa richiesta formale con assunzione di responsabilità, verificati i requisiti di sicurezza.

Accesso alla rete wi-fi dell'Istituto

La Scuola rende disponibile un servizio gratuito di navigazione internet attraverso connessione wi-fi abilitato su proprie postazioni e su device personali di proprietà del personale in servizio (Notebook, Tablet, Smartphone, ecc.). Tutto il personale che intende utilizzare la rete scolastica dovrà impegnarsi a rispettare scrupolosamente le seguenti regole:

- Prima di poter accedere alla rete, il personale autorizzato deve aver ricevuto la convalida alla connessione di rete con il proprio dispositivo mobile, essendo stato previamente abilitato, attraverso l'esecuzione dell'apposita procedura approvata dall'Istituto - Tale procedura prevede la sottoscrizione dell'apposito Regolamento per l'accesso e l'utilizzo della wi-fi dell'Istituto da parte dell'utente e la sua formale richiesta di credenziali per il servizio di navigazione internet dell'Istituto;
- l'utente autorizzato potrà avere accesso alla rete wi-fi solo se in possesso delle necessarie credenziali, al fine di garantire l'uso corretto della rete, evitando l'accesso e l'utilizzo da parte di soggetti non autorizzati;
- l'utente autorizzato dovrà firmare per ricevuta il relativo verbale di convalida alla connessione e di ricezione delle credenziali di accesso.

15. Uso dei supporti removibili

Nel caso in cui non si crei una limitazione informatica nelle impostazioni di sistema o utilizzando software specifici che impediscono il riconoscimento di supporti removibili come chiavette USB, dischi esterni, smartphone al fine di impedire la sottrazione di dati o il rischio di contaminazione da supporti veicolanti qualsiasi forma di virus, gli addetti autorizzati sono tenuti al rispetto delle seguenti regole.

L'utilizzo di supporti di memorizzazione rimovibili deve essere effettuato con molta cautela ed esclusivamente per le attività lavorative.

Al momento della connessione di un dispositivo esterno viene avviata la scansione automatica antivirus, per permettere al sistema di completare la verifica di sicurezza che non può essere interrotta dall'Utente. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, per non danneggiare e rendere illeggibili i dati.

L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza o per trasportare file di grandi dimensioni, rimane in ogni caso sotto la responsabilità dell'utilizzatore, che è tenuto a rivolgersi al personale tecnico autorizzato della gestione dei sistemi informativi, per le opportune configurazioni di sicurezza e/o crittografia del dispositivo.

I supporti removibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, ecc.).

Quando tali supporti non sono più utilizzati devono essere distrutti o resi inutilizzabili, oppure possono essere riutilizzati da altri incaricati soltanto dopo essere stati formattati utilizzando la cancellazione sicura dei dati personali.

Le operazioni sopra menzionate vengono effettuate da personale specializzato impiegato in Società/Ditte appositamente incaricate dalla Scuola

È vietato consegnare a terzi supporti già utilizzati per la memorizzazione di informazioni o di dati personali, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo l'intervenuta cancellazione.

Il trasferimento di file contenenti dati personali, dati particolari e giudiziari su supporti rimovibili è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari ed i dati giudiziari devono essere crittografati.

L'Utente è tenuto a informare immediatamente il DS, il DSGA e il Responsabile della Protezione dei Dati, anche ai sensi della procedura di gestione delle violazioni di dati personali, di qualsiasi danno, furto o perdita di apparati, software e/o dati in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti.

16. Utilizzo di account istituzionali

L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'Istituto.

Pertanto è vietato:

- utilizzare l'account istituzionale per registrarsi ad un servizio, applicazioni e siti web, che hanno natura e finalità non riconducibili all'attività istituzionale della Scuola e/o che hanno scopi pubblicitari e commerciali;
- consentire ad altri, a vario titolo, l'utilizzo delle piattaforme digitali per l'amministrazione e la didattica adottate dall'Istituto utilizzando il proprio account istituzionale;
- diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano gli stessi servizi digitali della Scuola;
- utilizzare gli account istituzionali e le relative piattaforme in modo da danneggiare, molestare o insultare altre persone;
- tramite gli account istituzionali creare e trasmettere immagini, dati o materiali offensivi, osceni o indecenti;
- tramite gli account istituzionali creare e trasmettere materiale offensivo per altre persone o enti;
- tramite gli account istituzionali creare e trasmettere materiale commerciale o pubblicitario.

L'utente autorizzato è tenuto a:

- modificare la password unica fornita e impostarne una nuova personale;
- sostituire con periodicità la password;
- conservare la password personale e non consentirne l'uso ad altre persone;
- non memorizzare la password per utilizzi successivi della piattaforma o per altre applicazioni che lo propongono ed al termine delle operazioni effettuare sempre il logout;
- comunicare immediatamente all'amministratore di sistema ed al team animatore digitale l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;
- utilizzare i servizi offerti solo ad uso esclusivo per le attività amministrative e didattiche della scuola.

Procedura di sospensione e di disattivazione dell'account

Quando cessa il rapporto di lavoro gli account riconducibili a persone identificate o identificabili devono essere rimossi (dunque cancellati), previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento. Sono altresì necessari accorgimenti tecnici per impedire la visualizzazione dei messaggi in arrivo nelle more di tempo necessario per la cancellazione dell'account stesso.

Pertanto, in conformità ai principi in materia di protezione dei dati personali, dopo la cessazione del rapporto di lavoro, il titolare del trattamento deve provvedere affinché: I) venga rimosso l'account del dipendente cessato; ii) siano informati i terzi con meccanismi automatizzati della disattivazione dell'account e vengano comunicati indirizzi alternativi a cui rivolgersi; iii) vengano adottate misure idonee ad impedire la visualizzazione dei messaggi in arrivo durante il periodo in cui tale sistema automatico è in funzione.

In particolare alla cessazione del rapporto di lavoro l'account istituzionale assegnato all'addetto autorizzato viene immediatamente sospeso, con l'impossibilità di qualsiasi accesso successivo da parte dell'addetto. Entro 90 giorni dalla sospensione, l'account istituzionale viene definitivamente disattivato. In questo periodo, prima della disattivazione definitiva dell'account vengono comunicati, laddove necessario, gli indirizzi alternativi cui rivolgersi.

Al fine di snellire le operazioni di dismissione/disattivazione degli account di tutto il personale docente in servizio, solo ai docenti che svolgono supplenza per un periodo inferiore a 5 giorni non saranno assegnati account istituzionali sulla piattaforma Google Workspace for Education in uso nella Scuola.

17. Sistemi e Servizi in Cloud

Per tutti i servizi in Cloud resi disponibili e approvati dalla Scuola, ne è concesso il pieno utilizzo agli utenti, per tutti e soli gli scopi previsti per lo svolgimento dell'attività lavorativa. Non è consentito agli utenti l'utilizzo dei sistemi o piattaforme Cloud, diverse da quelle adottate dalla Scuola, per finalità personali e/o per condivisione di informazioni (file sharing e collaboration) con entità interne o esterne.

18. Utilizzo della posta elettronica

La casella di posta elettronica, assegnata dall'Istituto all'utente, è uno strumento di lavoro.

Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Con l'utilizzo della posta elettronica gli utenti assegnatari rappresentano l'Istituto all'esterno e, pertanto, sono tenuti ad osservare un comportamento professionale a tutela dell'immagine della Scuola.

Si precisa che l'account di posta elettronica è di proprietà dell'Istituto e deve essere utilizzato esclusivamente per lo svolgimento dell'attività lavorativa.

A ciascun utente possono essere assegnate, oltre ad una casella nominativa, anche caselle di posta elettronica associate a gruppi di lavoro e/o unità operative/uffici.

Tali caselle condivise devono essere utilizzate solo per la ricezione dei messaggi, mentre per i messaggi di risposte e in uscita è necessario utilizzare l'account nominativo assegnato.

È vietato utilizzare la casella di posta elettronica assegnata:

- per l'invio di messaggi personali e completamente estranei al rapporto di lavoro o alle relazioni tra colleghi;
- per scaricare allegati contenenti video/brani musicali non funzionali all'attività lavorativa;
- per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione.

Inoltre è da evitare l'utilizzo di caselle di posta elettronica personali per attività o comunicazioni afferenti al servizio, savi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti o salvandoli in una apposita cartella di servizio creata sul proprio PC o nelle partizioni NAS assegnate: il dipendente ha il dovere di verificare periodicamente (settimanalmente) lo spazio a disposizione nella casella di posta propria e/o della propria struttura/ufficio, evitando così di non ricevere messaggi per mancanza di spazio disponibile.

Dal momento che i messaggi di posta elettronica sono un veicolo incredibilmente efficace di virus e attacchi di social engineering è fondamentale che l'addetto autorizzato sia a conoscenza dei rischi per la sicurezza

informatica e per la protezione dei dati e dei mezzi per poter contrastare tali rischi, attraverso una formazione adeguata ed il recepimento di informative e linee guida operative specifiche. Per questo è fondamentale per l'addetto partecipare a tutti gli eventi formativi organizzati dalla Scuola su queste tematiche. Inoltre è importante seguire sempre alcune regole di comportamento nell'utilizzo della posta elettronica.

È buona norma:

- utilizzare password complesse e difficilmente conoscibili, preferibilmente utilizzando programmi generatori di password;
- conservare la password con la massima diligenza e in modo da assicurarne la massima riservatezza;
- mantenere la casella di posta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti;
- utilizzare la ricevuta di ritorno per avere conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- evitare l'invio di messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione;
- controllare i file allegati di posta prima del loro utilizzo, evitando, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità;
- accertarsi dell'identità del mittente e controllare attraverso software antivirus i file allegati prima del loro utilizzo;
- collegarsi a siti internet contenuti nei messaggi solo quando vi è la comprovata sicurezza sul contenuto degli stessi;
- nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli. Analogamente, messaggi provenienti da mittenti conosciuti che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd) non devono essere aperti.
- nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari, rendere preventivamente questi allegati illeggibili attraverso ola crittografia comunicando al destinatario la password di cifratura attraverso un Canale separato (per es. Sms, dettata al telefono, ecc).

È vietato l'invio di messaggi di posta elettronica all'interno o all'esterno della Scuola, che siano oltraggiosi, discriminatori o che possono essere in qualunque modo fonte di responsabilità dell'Istituzione scolastica.

È vietato l'invio automatico di e-mail all'indirizzo privato (ad esempio attivando un "inoltro" automatico delle e-mail entranti) anche durante i periodi di assenza (ad esempio ferie, malattia, infortunio, ecc.).

In quest'ultima ipotesi la Scuola metterà a disposizione appositi sistemi che consentano di inviare automaticamente messaggi di risposta che indichino un indirizzo di mail alternativo da utilizzare per inviare messaggi di contenuto professionale.

In caso di eventuale assenza improvvisa o prolungata di un dipendente e per improrogabili necessità, qualora il dipendente non possa attivare la predetta funzionalità, la Scuola potrà disporre per il tramite di un assistente tecnico o dell'amministratore di sistema l'attivazione di analoga funzione di risposta automatica e re-indirizzamento, avvertendo il lavoratore assente.

In caso di imprescindibili esigenze organizzative e produttive , per la sicurezza del lavoro e per la tutela del patrimonio scolastico ovvero per motivi di sicurezza del sistema informatico, la Scuola potrà, accedere all'account di posta elettronica, prendendo visione dei messaggi , salvando o cancellando file; in tal caso il titolare della casella di posta elettronica potrà designare un altro dipendente (fiduciario) per verificare il contenuto dei messaggi e per inoltrare al titolare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del DSGA assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile.

Disattivazione/rimozione account di posta alla cessazione del rapporto di lavoro

Subito dopo la cessazione del rapporto di lavoro con l'utente la casella di posta assegnata all'autorizzato viene disattivata entro e non oltre 30 giorni con contestuale adozione di un messaggio automatico volto ad informare i terzi e ad indicare un account alternativo per contattare il titolare; l'account verrà definitivamente rimosso e cancellato entro 90 giorni.

Regole per redazione delle email

Poiché il dipendente autorizzato è responsabile del contenuto dei messaggi inviati con il servizio di posta elettronica (Codice di comportamento dei dipendenti pubblici di cui al DPR 62/2013 con le modifiche apportate dal D.lgs.81/2023), gli addetti autorizzati sono tenuti a rispettare le modalità di firma dei messaggi di posta individuate dall'Istituzione scolastica. In particolare, ciascun messaggio in uscita deve consentire l'identificazione dell'addetto mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

Pertanto quando si crea una email l'addetto autorizzato deve:

a) individuare i destinatari, selezionandoli accuratamente e senza eccessi, sia quelli diretti, sia quelli per conoscenza (non è mai il caso di realizzare un piccolo spam);
b) avere cura di non diffondere senza giustificazione gli indirizzi di posta elettronica dei destinatari (perciò usare il campo della copia nascosta);
c) inserire un oggetto sintetico e chiaro;
d) nel corpo della mail preferire frasi brevi e la tecnica della elencazione per punti;
e) spiegare la funzione di eventuali allegati:
f) essere definito e preciso nello spiegare la ragione dell'invio della mail e nell'indicare se è richiesta una risposta;
g) evidenziare tempi attesi della risposta e recapiti per l'inoltro della stessa.

Inoltre la creazione di una email "ex novo" è sempre la forma da preferire alle email attivate con la funzione "rispondi" - peraltro quando si decide di schiacciare il tasto "rispondi", oltre a quanto sopra indicato, bisogna valutare se eliminare in tutto o in parte la comunicazione originaria, la quale a sua volta potrebbe riportare un lunga sequenza di precedenti comunicazioni, magari del tutto slegate dall'argomento trattato nella ultima e-mail.

Solo eccezionalmente si può considerare la funzione "rispondi a tutti" , dal momento che induce a non selezionare i destinatari, con la probabilità che la comunicazione sia inviata a soggetti del tutto disinteressarti, trascinati senza ragione dentro la lunga filiera della email, con notevoli rischi di diffusione non giustificata di dati personali e la conseguente prospettiva delle sanzioni previste per violazione della privacy.

Cosa è il Phishing

Il Phishing è un tipo di frode, veicolata principalmente tramite la posta elettronica, attraverso la quale un malintenzionato cerca di ingannare la vittima inconsapevole convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile o una persona nota all'interno di una comunicazione digitale.

Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale. Per evitare di incorrere in questa tipologia di truffa, è bene attenersi sempre ai seguenti accorgimenti:

a) verificare sempre il vero indirizzo del mittente, di solito riportato vicino al nome;

b) non rispondere mai alle e-mail sospette;

c) non cliccare mai sui link proposti all'interno di mail sospette. Contattare eventualmente l'ente coinvolto che sembra richiedere le informazioni;

d) prestare massima cautela ed attenzione nell'apertura degli allegati presenti all'interno di mail sospette.

19. Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacchi al sistema informatico mediante virus o mediante ogni altro software aggressivo. Ad esempio: non aprire mail e/o relativi allegati sospetti, non navigare su siti non istituzionali o non attinenti al lavoro, ecc. L'Istituto è inoltre dotato di sistemi di protezione contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale. Ogni utente è tenuto a controllare la presenza ed il regolare funzionamento del software antivirus in dotazione. Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso – staccando il cavo di rete senza spegnere il computer - e segnalare l'accaduto al tecnico incaricato della gestione della sicurezza dei sistemi informativi. In generale è da evitare l'uso di supporti di memorizzazione esterni, ma nei casi strettamente necessari ed autorizzati dal DS, eventuali dispositivi magnetici di provenienza esterna alla Scuola o eventuali supporti di memorizzazione utilizzati dovranno essere verificati mediante il programma antivirus prima del loro utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovranno essere utilizzati. In caso in cui l'utente venga avvisato da segnalazioni di anomalie provenienti dal software antivirus presente sul pc o su qualunque device assegnato per lo svolgimento dell'attività lavorativa deve immediatamente avvisare il personale tecnico incaricato della gestione della sicurezza dei sistemi informativi e, laddove presente, anche il proprio amministratore di sistema che analizzerà l'accaduto e individuerà le possibili misure d'intervento.

20. Utilizzo di stampanti multifunzione e fotocopiatrici

Le macchine (stampanti multifunzione e fotocopiatrici) sono di proprietà della Scuola e rientrano tra gli strumenti di lavoro. Gli addetti autorizzati pertanto sono tenuti ad utilizzarli in modo corretto e conforme alle istruzioni d'uso. Eventuali utilizzi che non rientrano nella mansione lavorativa o che non sono conformi ai regolamenti di uso e manutenzione, possono contribuire ad innescare problemi al servizio, costi di manutenzione, e, soprattutto, minacce per la protezione dei dati personali. Tali strumenti possono essere utilizzati per lo svolgimento delle attività didattiche, e per le esigenze di ufficio di segreteria e di Presidenza ed in generale per tutte le attività propedeutiche alla gestione degli alunni e dei genitori, personale ATA e docenti, contabilità e finanza, protocollo e archivio corrispondenza ordinaria.

In generale è necessario prestare attenzione a documenti lasciati incustoditi in stampanti in uso condiviso e alle scansioni effettuate su stampanti multifunzione che indirizzano i documenti in cartelle comuni visibili a tutti i colleghi. I documenti che passano attraverso le stampanti contengono numerose informazioni, spesso confidenziali, e dati personali che devono essere protetti e resi sicuri. Al fine di minimizzare il rischio di diffusione non autorizzata di informazioni le stampe sono consentite esclusivamente attraverso l'utilizzo di credenziali assegnate a ciascun addetto. In tal modo solo le persone autorizzate possono accedere ai documenti, stamparli o effettuare scansioni.

Pertanto, allo scopo di informare il personale sul corretto e responsabile uso delle apparecchiature e garantire la riservatezza dei dati presenti sui documenti mandati in stampa e nei file conservati dal dispositivo, si indicano di seguito le regole che il personale deve rispettare:

1. Il loro utilizzo per fini personali e/o privati è vietato, salvo preventiva autorizzazione da parte del DS.
2. Le apparecchiature tecnologiche sono gestite dalle ditte incaricate della manutenzione e dall'amministratore di sistema.
3. Il personale autorizzato deve, prima di lanciare una stampa, verificare che le impostazioni di stampa e la carta presente nel cassetto della stampante siano adeguate alle esigenze.
4. Qualora, a stampa iniziata, il personale dovesse riscontrare anomalie ad esempio perché essa no risponde alle sure aspettative, il medesimo deve annullare prontamente il prosieguo premendo il tasto annulla sulla stampante stessa.
5. Una volta inviato in stampa il file il personale deve recarsi prontamente presso la stampante e raccogliere il documento.
6. Nel caso in cui la stampante non dovesse funzionare correttamente il personale non può allontanarsi dalla sua postazione senza prima aver cancellato la coda di stampa.
7. È vietato lasciare nel cassetto di uscita della stampante il documento inviato.
8. Per garantire la riservatezza dei documenti mandati in stampa e nei file conservati nel dispositivo, Qualora la stampante multifunzione in rete non fosse collocata in una stanza presidiata dagli addetti di segreteria o altro personale incaricato , si dovrà adottare un sistema di protezione mediante l'uso di un codice pin. Ad Ogni utente autorizzato sarà assegnato un codice che dovrà inserire nel pannello di gestione della stampante al fine di attivare la stampa del documento inserita in coda dalla propria postazione.
9. Ogni responsabilità relativa al corretto uso delle macchine è attribuito al personale scolastico utilizzatore.
10. Il personale è tenuto a segnalare prontamente eventuali guasti delle attrezzature contattando il personale tecnico di competenza.

21. Regolamento per l'accesso e l'utilizzo delle attrezzature dei laboratori

Sebbene le attrezzature presenti nei laboratori informatici non debbano essere utilizzate per la conservazione, raccolta o registrazione dei dati, la loro corretta configurazione e il loro appropriato utilizzo sono fondamentali per lo svolgimento delle finalità didattiche e formative. A tal proposito si individuano di seguito le principali istruzioni operative:

1. Utilizzare le postazioni PC, videoproiettori, LIM monitor interattivi e schermi TV, presenti nei laboratori solo per attività didattiche e non personali.
2. Configurare le macchine con un doppio account (amministratore e utente standard limitato) per evitare manomissioni delle attrezzature informatiche.

3. Installazione e aggiornamenti automatizzati di un sistema antivirus preferibilmente con caratteristiche avanzate del tipo endpoint che assicura la protezione della rete attraverso il monitoraggio e il tracking di ogni dispositivo connesso per minimizzare gli attacchi informatici.
4. Impostare gli aggiornamenti automatici dei sistemi operativi al fine di assicurare la funzionalità e le prestazioni della macchina, riducendo i rischi relativi a bugs (difetti della programmazione del software) delle versioni precedenti.
5. Assicurarsi di aver eseguito il log out da qualsiasi piattaforma web, e non, prima di lasciare incustodito il PC.
6. Evitare di salvare documenti contenenti dati personali, e non, sulla memoria del computer ma utilizzare dispositivi di memoria rimovibili.
7. Evitare di scaricare o salvare file potenzialmente dannosi o di origine incerta sul PC o di aprire e condividere e-mail da mittenti sconosciuti o appartenenti a catene e mail list.
8. Effettuare il log out dai programmi utilizzati e spegnere correttamente tutte le attrezzature utilizzate (PC, LIM, notebook, tablet, proiettori, monitor, ecc.) al termine della sessione di lavoro, non solo per evitare accessi non autorizzati ma anche per garantire il corretto funzionamento delle stesse.
9. Sottoporre le macchine ad una verifica periodica di software e hardware da parte dell'amministratore di sistema nonché registrare qualsiasi operazione effettuata sui dispositivi di lavoro.
10. Impedire l'accesso non autorizzato ai laboratori e supervisionare gli studenti durante le attività didattiche.
11. Riporre tutte le attrezzature mobili in armadietti chiusi a chiave al termine dell'attività di laboratorio.
12. Non lasciare incustodito il laboratorio durante le attività e accertarsi che sia chiuso al termine delle stesse.
13. Informare tutti gli utenti dei laboratori delle regole di utilizzo delle attrezzature approvate dall'Istituto.

14. Utilizzo dei mezzi di informazione e dei social media

Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla Scuola.

In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'Istituto.

Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'Istituzione scolastica e in difformità alle disposizioni di legge di cui al D.lgs.33/2013 e alla Legge 241/1990, documenti, anche istruttori e informazioni di cui essi abbiano la disponibilità.

Durante gli orari di lavoro gli utenti non possono far transitare attraverso i propri account privati immagini e informazioni di carattere lavorativo che riguardano le attività che vengono svolte presso gli uffici e le aule del plesso scolastico.

15. Strumenti di firma digitale

L'uso del kit di firma digitale, anche remota, è strettamente personale e non cedibile a terzi.

16. Comportamenti non consentiti

Sono vietati a tutti gli Utenti i seguenti comportamenti:

a) l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo della smart card di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche della Scuola e/o lo scambio di comunicazioni mediante falsa identità;

b) l'installazione, sulla PdL in dotazione, di software non coperto da licenza o, comunque, non preventivamente autorizzato dal Servizio Infrastrutture ICT Interne;

c) l'utilizzo, per comunicazioni personali, di chat, social network o altri strumenti di comunicazione istituzionale messi a disposizione dalla Scuola;

d) l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata di file e di ogni altra risorsa informatica;

e) l'allontanamento dalle PdL senza la preventiva adozione di opportune precauzioni di sicurezza (ad es. il blocco della PdL);

f) il mantenimento delle PdL accese al termine della giornata lavorativa;

g) la modifica delle configurazioni di base dei dispositivi assegnati dall'Agenzia senza l'autorizzazione preventiva del Servizio Infrastrutture ICT Interne (non è possibile, ad esempio, configurare account privati nel client di posta);

h) l'utilizzo di strumenti volti a eludere i sistemi di protezione.

17. Protezione contro furti e danneggiamenti

Tutte le PdL, portatili e i dispositivi mobili devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in esse contenuti. L'Utente è tenuto a informare immediatamente il DS, il DSGA, e, qualora vi sia la possibilità di una violazione di dati personali, altresì il DPO di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

18. Continuità attività lavorativa

Ciascun operatore può, anche da postazioni esterne alla Scuola, utilizzare specifiche funzionalità di posta elettronica per inviare automaticamente, in caso di assenza, messaggi di risposta che informino il mittente della propria indisponibilità, e funzioni di inoltro automatico dei messaggi ricevuti verso indirizzi di altro personale dipendente o della struttura organizzativa competente.

Evitare di utilizzare un inoltro automatico ad un altro indirizzo di posta, questo per un'ulteriore tutela del lavoratore che, contravvenendo alle regole lavorative interne può aver diffuso il proprio indirizzo mail istituzionale anche per fini privati.

Nel caso in cui un dipendente si assenti senza aver provveduto ad attivare i suddetti sistemi di inoltro automatico, un fiduciario, da lui preventivamente nominato, o, in sua assenza, il DSGA, potrà accedere alla casella di posta al fine di garantire la continuità dell'attività lavorativa.

Nei casi di assenza non programmata o impossibilità, temporanea o protratta nel tempo, se non è possibile attivare la procedura sopra citata, per garantire l'ordinaria operatività aziendale, il dipendente deve delegare ad un collega a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e di inoltrare al DSGA quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Qualora il dipendente non abbia delegato un collega (fiduciario), il DSGA può richiedere (attraverso l'apposita procedura richiedendo all'amministratore di sistema e/o al custode delle credenziali di autenticazione) di accedere alla casella di posta elettronica del dipendente assente, in modo da prendere visione dei messaggi di posta. In questo caso il DSGA deve informare il dipendente appena possibile, fornendo adeguata spiegazione e riportando l'evento su apposito verbale. La stessa procedura deve essere attuata qualora, per garantire l'ordinaria operatività sul lavoro, sia necessario accedere a informazioni o documenti di lavoro presenti sul PC del dipendente assente.

La nomina del fiduciario deve essere redatta in forma scritta, riportare la sottoscrizione del fiduciante e del fiduciario e consegnata al DSGA.

19. Attività degli amministratori del sistema

Per quanto attiene le postazioni di lavoro informatiche dei dipendenti designati come Amministratore del Sistema, oltre a tutto quanto finora evidenziato, anche in questo caso saranno adottati idonei sistemi di registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) avranno le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità in ragione dello scopo di controllo per cui sono richieste e ricomprenderanno, inoltre, i riferimenti temporali e la descrizione dell'evento che le ha generate per un periodo che sia congruo, comunque non inferiore a 6 (sei) mesi, come per legge. Occorre infine rendere noto che, ai fini dell'assolvimento dell'obbligo di registrazione degli accessi logici da parte degli Amministratori del Sistema, saranno registrati anche gli accessi da questi effettuati sui client, intesi come "postazioni di lavoro informatizzate", e non solo sui server. Ogni lavoratore qualificato come Amministratore del Sistema potrà far valere i propri diritti di interessato di cui agli artt. da 15 e ss. Del Regolamento UE 2016/679, rivolgendo direttamente al Titolare del trattamento e senza formalità una specifica richiesta scritta.

20. Monitoraggio e controlli

Nel rispetto delle normative vigenti, l'Istituzione scolastica, proprietaria degli strumenti informatici, e titolare del trattamento dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

a) tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;

b) evitare il verificarsi di illeciti o per esigenze di carattere difensivo anche preventivo;

c) verificare la funzionalità del sistema o dei dispositivi Informatici.

Le attività sull'uso del servizio di accesso a internet sono automaticamente registrate in files di LOG, che riportano i dettagli della navigazione, i siti e i documenti consultati. Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima e/o aggregata (riferita alla singola Struttura). I file di LOG verranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza. I dati personali contenuti nei LOG possono essere trattati esclusivamente nei seguenti casi:

- per rispondere ad eventuali richieste dell'autorità giudiziaria o della polizia giudiziaria;
- su richiesta del DS qualora si verifichi un evento dannoso o di pericolo che richieda un immediato intervento;
- su richiesta del DS qualora si verifichi un utilizzo anomalo degli strumenti da parte degli utenti di una specifica Struttura;
- qualora vi sia l'evidenza o comunque il fondato sospetto che sia in corso o sia stato posto in essere un illecito.

Il sistema informatico è programmato e configurato per cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico la cui conservazione non sia necessaria. Verranno prolungati i tempi di conservazione (limitatamente comunque alle sole informazioni indispensabili per perseguire finalità preventivamente determinate) solo in caso di:

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

Qualora le misure tecniche preventive non siano sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'Istituto effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- analisi aggregata del traffico di rete riferito all'intero Istituto o a sue Strutture e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni);
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro o su base individuale.

L'utente è direttamente e totalmente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine internet ai quali abbia stabilito collegamento tramite link. Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server della Scuola attraverso le seguenti fasi:

- analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (ufficio, area di attività, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;

- in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

21. Non osservanza delle norme

Le disposizioni di cui al presente regolamento rivestono carattere di obbligatorietà e la loro non osservanza costituisce illecito che, quando rilevato, può portare all'instaurazione di procedimenti disciplinari a carico dell'utilizzatore che lo ha posto in essere e, ricorrendone gli estremi, alla segnalazione dello stesso alle autorità competenti.