SOMMARIO

1 Premessa

L'utilizzo delle risorse informatiche di proprietà dell'I.C. via Pace - Limbiate poste a disposizione dei collaboratori e degli studenti per lo svolgimento dell'attività lavorativa e istituzionale deve avvenire in piena conformità alle norme legislative e regolamentari che disciplinano il rapporto di lavoro nelle Pubbliche Amministrazioni e delle obbligazioni contrattuali del personale dell'I.C. via Pace - Limbiate ai sensi e per gli effetti dell'art. 2104 del C.C, nonché delle norme in materia di trattamento dati che il Titolare del trattamento deve adottare secondo quanto previsto dall'art. 32 del Regolamento UE n. 2016/679 (c.d. "GDPR").
Il presente regolamento è assunto nell'osservanza delle norme di legge sopra richiamate ed avuto riguardo agli indirizzi giurisprudenziali in materia di riservatezza della vita di relazione e, nel contempo, di condanna dell'indebito utilizzo dei mezzi informatici per fini personali e illeciti che cagionano danni patrimoniali all'I.C. via Pace - Limbiate.

2 Scopo e campo di applicazione

Scopo del presente Regolamento è definire le regole relative alle modalità di utilizzo delle risorse informatiche messe a disposizione di tutti i collaboratori e studenti dell'I.C. via Pace - Limbiate , con l'obiettivo di prevenire l'accesso indebito, la modifica o l'alterazione, la cancellazione o la perdita dei dati contenuti negli archivi e consentire un trattamento adeguato dei dati personali degli interessati. Il regolamento descrive altresì le modalità con cui saranno effettuati i controlli sul rispetto delle indicate regole. A tal fine, successivamente alla sua adozione, il presente Regolamento sarà portato a conoscenza dei collaboratori dell'I.C. via Pace - Limbiate.

3 Definizioni

"Trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

"Dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

"Categorie particolari di dati": i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (anche indicati come dati sensibili nel presente documento).

"Archivio": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

"Titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

"Responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

"Consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

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

"Interessato": La definizione di "interessato", non essendocene una diretta, è desumibile dall'articolo 5, comma 1 che, definendo il "dato personale" dispone che: "*si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

4 Classificazione e modalità di trattamento delle informazioni che si possono riferire a dati personali

Confidenziale	Uso interno	Pubblico
Informazioni la cui divulgazione danneggerebbe la riservatezza o l'integrità di un soggetto: - informazioni relative al personale (docenti e ATA) - informazioni relative agli alunni e alle famiglie - dati appartenenti a categorie particolari (es. alunni con disabilità, esigenze di diete particolari)	Informazioni il cui accesso non autorizzato potrebbe influenzare e/o compromettere l'efficacia operativa scolastica: - anagrafiche relative ad alunni e famiglie - anagrafiche relative al personale (docenti e ATA) - informazioni relative ad aspetti operativi delle attività scolastiche	Informazioni che non sono né ad uso interno né confidenziali. La divulgazione di tali dati o informazioni non costituirebbe un danno per la Società, come ad esempio: - contatti dell'Istituto - informazioni reperibili dal sito scolastico; - informazioni reperibili da pubblici registri
L'accesso a queste informazioni è consentito esclusivamente a figure scolastiche specificamente autorizzate o fornitori esterni nominati Responsabili del trattamento, nell'ambito di un incarico o di un mandato.	Le informazioni possono essere comunicate esclusivamente alle persone che necessitano di conoscerle per motivi operativi connessi alle loro mansioni o a fornitori a cui siano necessarie per l'esecuzione del contratto.	Qualsiasi collaboratore, alunno, genitore, fornitore o consulente scolastico. Le informazioni non sono riservate o confidenziali e possono essere divulgate pubblicamente senza alcuna ripercussione per l'Istituto.
È vietato creare copie cartacee di documenti confidenziali, fatta eccezione per quanto previsto dagli obblighi di legge. I documenti confidenziali devono essere archiviati nell'apposito armadio protetto da serratura. È fatto divieto assoluto di lasciare, anche temporaneamente, questi documenti incustoditi sulle scrivanie o negli spazi condivisi. La condivisione di questi file deve essere effettuata tramite file/cartella protetti da password.	I documenti riservati possono essere stampati e vanno archiviati nell'apposito armadio con serratura messo a disposizione. È fatto divieto assoluto di lasciare questi documenti incustoditi sulle scrivanie o negli spazi condivisi. È inoltre fatto divieto assoluto di condivisione delle informazioni riservate in formato cartaceo.	È possibile condividere questi documenti all'esterno dell'Istituto.
La trasmissione per via orale di informazioni confidenziali deve avvenire in appositi spazi (es. sale riunioni), alla presenza delle sole persone interessate.	La trasmissione per via orale di informazioni riservate può avvenire all'interno di spazi scolastici delimitati (es. sale riunioni) in presenza delle persone o fornitori autorizzati al trattamento.	La trasmissione per via orale di informazioni pubbliche è libera e non sottoposta a regolamentazione specifica.

5 Misure di sicurezza

Ai sensi dell'articolo 32 del GDPR, relativo alla "Sicurezza del trattamento", «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio». A tal fine, l'I.C. via Pace - Limbiate adotta le misure adeguate di sicurezza, che si differenziano a seconda della modalità del trattamento dei dati e pertanto sono di seguito individuate.

L'I.C. via Pace - Limbiate si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisito, salvato, o installato in violazione del presente Regolamento.

6 Utilizzo dei sistemi informatici scolastici

L'I.C. via Pace - Limbiate è responsabile delle metodologie per la tutela dei dati gestiti con ausilio di strumenti informatici. Pertanto computer, tablet, ed ogni altro dispositivo mobile, nonché i relativi programmi e/o applicazioni affidati ai collaboratori e agli studenti, sono da considerarsi esclusivamente come strumenti di lavoro o strumenti didattici, pertanto si rammenta quanto segue:

1. tali strumenti devono essere custoditi in modo appropriato adottando le precauzioni necessarie ad evitare il furto del materiale informatico messo disposizione dall'Istituto;
2. devono essere prontamente segnalati al Preside e/o all'Amministratore di Sistema il danneggiamento, lo smarrimento o il furto di tali strumenti;
3. gli strumenti assegnati possono essere utilizzati solo per fini professionali in relazione alle mansioni assegnate e non per scopi personali, tantomeno per scopi illeciti;
4. qualunque anomalia riscontrata nel funzionamento del sistema informatico deve essere tempestivamente segnalata all'Amministratore di Sistema.

Tutte le strumentazioni hardware, incluse le apparecchiature informatiche, sono opportunamente etichettate e catalogate all'interno di un inventario elettronico. I collaboratori e gli studenti devono conservare e utilizzare gli strumenti a loro disposizione in modo da non danneggiare o asportare il contrassegno o l'etichetta.

6.1 Utilizzo di computer, tablet, e dispositivi mobili

Richiamato quanto in premessa ed anche al fine di evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità degli applicativi, non è consentito installare programmi provenienti dall'esterno. In caso di introduzione di virus o programmi che possono rappresentare un rischio per la sicurezza del computer e/o di qualsiasi altro dispositivo in uso si deve contattare l'Amministratore di Sistema, astenendosi dal risolvere il problema per conto proprio. In particolare, si ricorda di avere particolare riguardo durante l'utilizzo del laboratorio informatico.
Si rammenta inoltre quanto segue:

1. Non è consentito l'uso di programmi non distribuiti ufficialmente dall'Istituto.
2. Non è consentito scaricare alcun software se non con l'autorizzazione dell'Amministratore di Sistema.
3. Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
4. Non è consentito modificare le configurazioni impostate sul proprio PC rispetto a quelle autorizzate e predisposte.
5. Non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio modem Wi-Fi e memorie esterne).
6. Non sono consentiti la visualizzazione e il salvataggio di testi, immagini o registrazioni a carattere razzista, pornografico, pedopornografico, sessuale, violento, osceno o di natura simile, indipendentemente da quale ne sia la fonte e/o comunque di qualsiasi materiale che sia vietato dalle norme penali.
7. Al termine della giornata lavorativa o per periodo prolungati di assenza i computer fissi devono essere spenti. In caso di dispositivi mobili assegnati dall'Istituto come strumenti di lavoro, questi devono essere riposti in luogo sicuro o portati con sé. In caso di pause si raccomanda di proteggere il pc o il dispositivo con password o pin al fine di renderlo inaccessibile da parte di persone non autorizzare.

Si ricorda che non è consentito l'utilizzo di dispositivi personali per finalità connesse alle attività scolastiche.
Si raccomanda inoltre di salvare i file nel server dell'Istituto all'interno delle cartelle definite, evitando di salvare i documenti che contengono dati personali in locale.

6.2 Utilizzo di supporti magnetici

I documenti che contengono dati personali devono essere salvati sulle cartelle presenti sul Server dell'Istituto. L'utilizzo di supporti magnetici (ad esempio hard-disk esterni e chiavette usb) deve essere limitato ad esigenze lavorative o didattiche autorizzate e secondo le seguenti modalità:

1. ogni collaboratore è tenuto a custodire i supporti magnetici contenenti dati appartenenti a categorie particolari in armadi chiusi a chiave, al fine di evitare che il loro contenuto possa essere trafugato, alterato e/o distrutto;
2. non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

6.3 Controlli contro malware

L'I.C. via Pace - Limbiate predispone gli strumenti dati in uso ai collaboratori e agli studenti in modo che siano adottate le misure più opportune per proteggere i sistemi da malware, attacchi hacker e intrusioni in genere. L'I.C. via Pace - Limbiate provvede all'installazione di opportuni software quali antivirus e configurazione di firewall.
È obbligo del collaboratore verificare, almeno con cadenza mensile, che questi software siano in funzione e aggiornati. Per qualsiasi informazione riguardo alla modalità di verifica o nel caso si sospettino malfunzionamenti, il collaboratore si può rivolgere all'Amministratore di Sistema, il quale potrà anche intervenire direttamente sul dispositivo.

7 Utilizzo della rete istituzionale

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono essere utilizzate per scopi diversi in alcun modo. Pertanto, qualunque file che non sia collegato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
L'I.C. via Pace - Limbiate si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza del sistema ovvero acquisito o installato in violazione del presente Regolamento.

8 Utilizzo della rete internet e della posta elettronica

8.1 Internet

L'uso di Internet è consentito esclusivamente alle persone autorizzate per gli scopi attinenti alla propria attività lavorativa. Non è consentito scaricare files, inclusi files multimediali, in violazione delle leggi sul Copyright. Si ricorda in particolare che nell'ambito dell'attività lavorativa:

1. Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare dati appartenenti a categorie particolari del collaboratore.
2. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
3. Non è consentita la consultazione o la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Ai fini di garantire una navigazione Internet sicura e prevenire il download e la diffusione di malware, l'I.C. via Pace - Limbiate si avvale di strumenti esterni per il filtraggio del traffico dati. In particolare, è in uso una soluzione di DNS filtering tramite un provider esterno. I dati non rivelano in alcun modo i contenuti delle comunicazioni in rete e sono utilizzati esclusivamente dal provider nel rispetto del regolamento.
I dati sono conservati per 30 giorni al fine di consentirne una analisi periodica.
L'eventuale prolungamento dei suddetti tempi di conservazione è eccezionale e può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

8.2 Posta elettronica

Al singolo collaboratore è assegnato un indirizzo e-mail personale fornito dal MIUR del tipo "nome.cognome@istruzione.it". I collaboratori sono tenuti a mantenere in ordine la propria casella, a prestare attenzione alla dimensione degli allegati inviati e, per la trasmissione di file, a preferire, quando possibile, l'utilizzo delle cartelle di rete condivise.
Si ricorda che la posta elettronica è uno strumento di lavoro e che tutte le caselle contrassegnate dagli indirizzi con estensione "@istruzione.it" ed il contenuto delle stesse sono e restano di proprietà dell'I.C. via Pace - Limbiate , che le concede in uso ai propri collaboratori esclusivamente per finalità di lavoro.

Si ritiene pertanto utile segnalare che:

1. non è consentito utilizzare l'indirizzo di posta elettronica istituzionale (sia in entrata che in uscita) per motivi non attinenti allo svolgimento delle mansioni assegnate;
2. ogni messaggio di posta elettronica deve riportare nome e cognome;
3. è obbligatorio specificare l'oggetto della e-mail nel relativo campo;
4. è opportuno limitare l'uso della funzione "rispondi a tutti" solo ai casi strettamente necessari;
5. essendo vietata la diffusione degli indirizzi e-mail senza il consenso dell'intestatario, si raccomanda di prestare attenzione agli invii a più persone, valutando se del caso, l'utilizzo del campo "CCN:" (o "BCC:" per le postazioni con il software in inglese) al posto di "A:" e/o "CC:";
6. non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa (contenenti testi, immagini o registrazioni a carattere razzista, pornografico, pedopornografico, sessuale, violento, osceno o di natura simile e/o comunque di qualsiasi materiale che sia vietato dalle norme penali e/o che sia discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
7. non è consentito rispondere e/o inoltrare messaggi catalogabili come spam;

8. non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione;
9. i messaggi elettronici in entrata vengono sistematicamente analizzati nella ricerca di virus; i messaggi contenenti virus sono automaticamente eliminati;
10. sono vietati i tentativi di accesso a messaggi elettronici di utenti o terzi;
11. è vietato inviare posta elettronica a nome di un altro utente, salvo sua espressa autorizzazione.

8.3 Gestione dei Social Network e dei programmi di messaggistica

È vietato l'uso di Social Network (quali ad esempio Facebook, Twitter, LinkedIn e Instagram), di qualsiasi altra piattaforma online (quale ad esempio YouTube) e di applicativi di messaggistica (quale ad esempio WhatsApp) non attinenti all'attività lavorativa.
È raccomandato di non inviare comunicazioni a soggetti estranei agli scopi istituzionali o professionali ovvero procedere alla diffusione dei dati non autorizzati.

9 Credenziali di accesso

Le credenziali di accesso alla postazione di lavoro e agli applicativi scolastici dei nuovi utenti sono trasmesse dall'Amministratore di Sistema via e-mail, su richiesta del Preside o del DSGA, in base al profilo di accesso corrispondente al ruolo e alle mansioni affidati all'utente.
Si rammenta che la password è personale e non può essere comunicata ad altre persone, salvo per esigenze connesse all'assenza del collaboratore per cui è possibile individuare una persona delegata (P.11).
È severamente vietato usare la password e lo User-ID di un altro utente.
Le norme sopra elencate si applicano a tutte le credenziali distribuite agli utenti per accedere agli strumenti istituzionali.
Al momento del rilascio delle credenziali verrà impostata una password generica che consentirà il primo accesso che dovrà obbligatoriamente essere cambiata con una ad esclusiva conoscenza dell'assegnatario.
Le password devono essere conformi ai seguenti requisiti minimi di complessità:

1. lunghezza minima di 8 caratteri;
2. almeno un carattere maiuscolo;
3. almeno un carattere minuscolo;
4. almeno due cifre decimali 0-9.

I requisiti di complessità vengono verificati al momento sia della creazione sia della modifica delle password.
Le password scadono ogni 60 giorni. Non è possibile riutilizzare una delle ultime due password.
Le password non devono, per motivo alcuno, essere trascritte o risultare facilmente reperibili (ad esempio, non devono essere riportate su supporti cartacei).
Le postazioni di lavoro, siano Desktop, PC portatili, o Tablet, non possono essere abbandonate senza che l'accesso sia protetto, pertanto sul proprio PC è obbligatorio impostare uno screensaver automatico con password.
L'Istituto provvederà a disabilitare tempestivamente le credenziali, comunque entro 15 giorni, a seguito della conclusione della collaborazione o qualora venga meno la necessità per cui queste sono state create.

10 Riservatezza dei dati nelle comunicazioni con l'esterno

I documenti e i files prodotti all'interno dell'I.C. via Pace - Limbiate durante l'attività lavorativa quali documenti tecnici, anagrafiche, comunicazioni interne/esterne e file di posta sono esclusivamente di proprietà dell'I.C. via Pace - Limbiate. Non è consentito asportare alcun file (tramite salvataggio su supporti esterni, stampa, invio e diffusione ad altri soggetti tramite e-mail) se non espressamente autorizzati o attinenti con l'attività lavorativa.

1. è severamente vietato rivelare informazioni riservate o di carattere confidenziale relative all'I.C. via Pace - Limbiate, ai suoi collaboratori o ad altri soggetti con i quali si intrattengono rapporti professionali;
2. è severamente vietata la diffusione di informazioni confidenziali relative all'I.C. via Pace - Limbiate a soggetti indeterminati;
3. l'utilizzo dei loghi scolastici è consentito solo se previsto nell'ambito delle mansioni e attività assegnate;
4. è vietato il riferimento a qualsiasi fatto, persone, tecnologie e informazioni di carattere generale riconducibili all'I.C. via Pace - Limbiate, a meno che non si tratti di contesto lavorativo.

11 Disponibilità dei dati durante i periodi di assenza

Per necessità legate alla continuità operativa, ogni collaboratore è tenuto ad individuare un fiduciario di posta elettronica autorizzato ad accedere alla propria casella di posta istituzionale in caso di assenza prolungata superiore a tre giorni.
Al collaboratore è inoltre richiesto di impostare un messaggio di risposta che informi il mittente della propria indisponibilità fornendo un contatto alternativo.

12 Cessazione del rapporto di lavoro

Il collaboratore che cessa il rapporto di lavoro con l'Istituto (sia esso docente o personale ATA) è obbligato a consegnare al proprio responsabile gerarchico (segreteria, DGSA, Preside) o all'Amministratore di Sistema tutti gli strumenti istituzionali e i dispositivi in dotazione, inclusi supporti di memoria esterni.
L'Amministratore di Sistema provvederà a disattivare l'accesso ai corrispondenti archivi presenti sul Server, alla casella di posta elettronica e a tutti gli applicativi e servizi web messi a disposizione dall'Istituto. Per consentire la continuità operativa, sulla casella di posta della persona autorizzata dimissionaria sarà impostato un messaggio automatico che avvisa della disattivazione della casella e-mail e fornisce il nominativo di un altro utente.

Ricordando che la posta elettronica e tutti gli strumenti istituzionali sono di proprietà dell'Istituto, si ritiene necessario ricordare che alla cessazione del rapporto di lavoro è obbligatorio restituire integri e completi tutti gli strumenti che l'Istituto ha messo a disposizione, in particolare:

1. la casella di posta elettronica e i messaggi e i documenti in essa contenuti devono essere messi a disposizione dell'Istituto per consentire la continuità operativa;
2. eventuali messaggi privati o non pertinenti l'attività operativa devono essere eliminati;
3. PC portatili e Smartphone devono essere tempestivamente consegnati, senza che il collaboratore ne effettui backup o copie per uso personale;
4. la eventuale scheda Sim corrispondente al numero assegnato deve essere restituita.

Entro 15 giorni dal termine della collaborazione tutto l'hardware sarà formattato in modo da essere illeggibile e non più recuperabile, secondo gli standard internazionali più recenti.

13 Controlli

Poiché in caso di violazioni disciplinari e giuridiche sia l'I.C. via Pace - Limbiate sia il singolo collaboratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'I.C. via Pace - Limbiate verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.
Qualora le misure tecniche e organizzative non fossero idonee ad evitare eventi dannosi o situazioni di pericolo e/o gli strumenti e i dispositivi di controllo segnalino anomalie nel normale utilizzo delle risorse, l'I.C. via Pace - Limbiate provvederà ad effettuare con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le fasi successive.

13.1 Traffico di rete ed internet

Si riportano i controlli sui dati di traffico effettuati per verificare la presenza di eventuali anomalie:

1. analisi aggregata del traffico di rete riferito all'intera struttura scolastica e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni, ecc.) e/o delle categorie di siti visitati;
2. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite;
3. in caso di successivo permanere dell'anomalia, effettuazione di controlli sul traffico generato dalle singole postazioni di lavoro, preservando comunque il rispetto della riservatezza del collaboratore, ad esempio omettendo l'individuazione dei singoli siti visitati, a meno che ciò non sia richiesto dall'Autorità Giudiziaria.

13.2 Occupazione dello spazio di memorizzazione sul Server scolastico

Si riportano i controlli relativi allo spazio occupato sui server dell'Istituto:

1. analisi aggregata dei dati memorizzati sul Server a livello di intera struttura lavorativa, rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
2. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite;
3. analisi aggregata dei dati memorizzati sui server a livello di singoli Settori/Servizi, rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
4. emanazione di un avviso al responsabile gerarchico relativo ad un riscontrato utilizzo anomalo, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite;
5. in caso di successivo permanere dell'anomalia, è possibile procedere con un'analisi puntuale, anche sulle singole cartelle di files.

13.3 Controlli sulle postazioni di lavoro

Qualora a seguito degli accertamenti generali, risultino elementi presuntivi plurimi e concordanti in ordine all'anomalo utilizzo di una postazione di lavoro, il Preside, il DSGA o un altro responsabile procederà alla contestazione delle anomalie al collaboratore titolare della postazione di lavoro, assegnandogli un termine

non inferiore a 5 giorni per la presentazione di controdeduzioni o giustificazioni. Nell'ipotesi in cui le giustificazioni presentate non siano ritenute congrue o scusanti, con provvedimento motivato potrà essere autorizzata la verifica puntuale della postazione di lavoro che dovrà avvenire alla presenza ed in contraddittorio del titolare della postazione di lavoro stessa. Si ribadisce che ogni controllo verrà effettuato nel rispetto dei seguenti principi:

1. proporzionalità: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi;
2. trasparenza: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.

Il soggetto preposto al controllo ed alla verifica del rispetto del presente regolamento è il Titolare del trattamento, nella persona del Preside pro tempore, supportato da altre figure quali il DSGA o l'Amministratore di Sistema.

14 Protezione dei dati - Altre misure di sicurezza

Al fine di tutelare anche i dati trattati su supporto cartaceo, si ricorda infine quanto segue:

1. non trasportare al di fuori dell'Istituto documenti cartacei se non per scopi legati alle attività lavorative e previamente autorizzati dal Preside;
2. i documenti devono essere conservati nei locali dedicati a cura delle persone autorizzate;
3. non diffondere informazioni e documentazione riservate;
4. prestare particolare attenzione alla custodia delle chiavi e dei codici di accesso ai locali dell'Istituto.

I documenti che contengono dati personali o appartenenti a categorie particolari devono essere archiviati e custoditi in armadi provvisti di serratura al fine di evitare accessi non autorizzati, copiatura o sottrazione; le chiavi devono essere affidate a personale individuato e conservate in luogo sicuro a chiusura dell'Istituto.
Stampanti, apparecchiature fax e fotocopiatrici devono essere collocate in luoghi in cui sia agevole la sorveglianza e il controllo da parte degli addetti. Si raccomanda di evitare la diffusione di copie e stampe se non necessario e richiesto ai fini lavorativi.

15 Azioni a fronte dei controlli

Tutte le anomalie riscontrate che possono costituire una violazione a quanto definito nel presente Regolamento devono essere segnalate all'Amministratore di Sistema secondo quanto previsto.
Qualora, ad esito di controllo, vengano rilevate delle anomalie sull'utilizzo dei sopracitati strumenti informatici che possano essere configurate quali attività non conformi al presente codice o comunque in violazione dei doveri connessi al contratto di lavoro, verrà data informazione al Preside per l'adozione dei conseguenti provvedimenti disciplinari.
A seguito dell'accertamento della condotta illecita e, quindi, dell'adozione del provvedimento disciplinare, l'I.C. via Pace - Limbiate procederà altresì, qualora il fatto integri gli estremi di un reato, a segnalare l'abuso all'Autorità competente.

16 Deroghe e modifiche al presente regolamento

Il presente documento è regolarmente aggiornato, messo a disposizione per la consultazione da parte di ogni collaboratore ed è pubblicato all'interna di una specifica area personale. Il Titolare del trattamento, supportato da altre funzioni, quali il DSGA o l'Amministratore di Sistema, provvederà a notificare ai collaboratori la presenza di una eventuale versione aggiornata.
Deroghe o modifiche di uno o più punti del presente Regolamento non rendono invalidi gli altri punti.

17 Appendice

17.1 Istruzioni al personale

Si riportano in sintesi le istruzioni da osservare per la corretta gestione dei dati personali trattati dall'I.C. via Pace - Limbiate , in conformità al Regolamento UE 2016/679 (c.d. "GDPR") e al Codice Privacy (D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018).

Istruzioni al personale di segreteria
a) non portare documenti fuori dalla sede scolastica, neanche temporaneamente; b) non fare copie della documentazione, salvo autorizzazione; c) durante il trattamento mantenere i documenti contenenti dati personali lontani dalla portata di terzi; non lasciare sulla scrivania documenti relativi al personale, ai collaboratori, agli alunni e alle loro famiglie, specie se appartenente a categorie particolari (es. dati relativi alla salute); d) al termine del trattamento custodire i documenti all'interno di archivi muniti di serratura; e) in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di soggetti non autorizzati di accedere a tali dati; f) evitare di fornire telefonicamente dati personali riguardanti collaboratori e alunni, salvo espressa autorizzazione; g) non fornire informazioni in merito alla salute relativi al personale docente e altri collaboratori. h) le comunicazioni agli interessati dovranno avvenire in forma riservata, in particolare se effettuate per iscritto dovranno essere consegnate in busta chiusa; i) all'atto della consegna di documenti, la persona autorizzata dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta; j) prestare attenzione all'utilizzo di documenti cartacei riciclati poiché potrebbero contenere dati personali o di natura sensibile.

Istruzioni ai collaboratori scolastici
a) non divulgare informazioni non attinenti alla propria mansione relative ai dati personali, di qualsiasi natura essi siano; b) non accedere ai locali della segreteria se non si è espressamente chiamati; c) evitare la consultazione e l'utilizzo di qualsiasi documento cartaceo o informatico durante la fase di pulizia dei locali; d) evitare di visualizzare il contenuto di documenti scolastici fotocopiati e trasportati all'interno dell'Istituto; e) non portare fuori dall'Istituto documenti scolastici; f) non diffondere i recapiti telefonici di docenti, collaboratori, alunni e famiglie; g) non diffondere dati appartenenti a categorie particolari degli alunni; h) non fornire informazioni relative alla salute del personale docente e di altri collaboratori; i) all'atto della consegna di documenti, la persona autorizzata dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta. j) prestare attenzione all'utilizzo di documenti cartacei riciclati poiché potrebbero contenere dati personali o di natura sensibile.

Istruzioni al personale docente
a) non portare documenti fuori dalla sede scolastica, neanche temporaneamente; b) non fare copie della documentazione, salvo autorizzazione; c) durante il trattamento mantenere i documenti contenenti dati personali lontani dalla portata di terzi; non lasciare sulla scrivania documenti relativi agli alunni e alle loro famiglie, specie se appartenente a categorie particolari (es. dati relativi alla salute); d) al termine del trattamento custodire i documenti all'interno di archivi muniti di serratura; e) in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di soggetti non autorizzati di accedere a tali dati; f) non diffondere i recapiti telefonici di colleghi, alunni e famiglie; g) non diffondere dati relativi ai giudizi scolastici e appartenenti a categorie particolari degli alunni; h) la consultazione del fascicolo personale dell'alunno è possibile esclusivamente dopo aver fatto richiesta alla segreteria e deve avvenire all'interno dei locali indicati; i) nessun dato può essere comunicato a terzi o diffuso senza la preventiva autorizzazione del Titolare; j) le comunicazioni agli interessati dovranno avvenire in forma riservata, in particolare se effettuate per iscritto dovranno essere consegnate in busta chiusa; k) all'atto della consegna di documenti, la persona autorizzata dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta.

17.2 Definizioni

TITOLARE DEL TRATTAMENTO
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Il Titolare del trattamento è l'Istituto, nella persona del Dirigente Scolastico pro tempore.

AUTORIZZATO AL TRATTAMENTO
Definizione ricavabile dal disposto dell'articolo 4 n. 10 del GDPR che individua "la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare". La persona nominata deve: - trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle funzioni secondo i principi di liceità, correttezza e trasparenza; - effettuare le operazioni di trattamento esclusivamente connesse allo svolgimento delle proprie mansioni; - mantenere assoluta riservatezza riguardo ai dati personali trattati secondo i principi di integrità e riservatezza; - accedere unicamente alle banche dati di cui si dispongono autorizzazioni; - aggiornare periodicamente le banche dati a cui ha accesso; - evitare la creazione o installazione di banche dati o software senza espressa autorizzazione del Titolare; - evitare di produrre copia o asportare supporti cartacei o informatici contenenti dati personali senza autorizzazione del Titolare. Le persone autorizzate al trattamento sono: il DSGA, i collaboratori del Dirigente Scolastico, i docenti, il personale di segreteria, i collaboratori scolastici.

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, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

DATO PERSONALE
Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Esempi: Nome, cognome, indirizzo, codice fiscale, numero di telefono, indirizzo di posta elettronica.

DATO APPARTENENTE A CATEGORIE PARTICOLARI
Dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o 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. Esempi: Patologie, disabilità, certificati medici o DVA, malattie o infortuni sul lavoro, farmaci salvavita - insegnamento della religione - diete particolari connesse allo stato di salute o all'appartenenza religiosa - adesione al sindacato e gestione dello sciopero.

ARCHIVIO
Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Il/La sottoscritto/a _____ dichiara di aver preso visione del presente Regolamento per l'utilizzo dei sistemi informativi dell'Istituto scolastico.

Luogo e data

_____, / /

Firma del Titolare del trattamento

_____

Firma leggibile del collaboratore

_____