Ministero dell'Istruzione e del Merito

C.P.I.A.3

Centro Provinciale per l'Istruzione degli Adulti
Via Roccafranca, 7/b (entrata nord) -25032 – Chiari (Bs)
C.M.: BSMM206003 - C.F.: 91028640174
e-mail: bsmm206003@istruzione.it
Pec: bsmm206003@pec.istruzione.it
Sito web: www.cpiachiari.edu.it – telefono: 030 7009707

REGOLAMENTO D'ISTITUTO PER L'UTILIZZO DEI DATI PERSONALI E DEGLI STRUMENTI DI TRATTAMENTO

(Disciplinare Tecnico-Organizzativo di Sicurezza ai sensi degli artt. 24, 29 e 32 del Regolamento UE 2016/679 - GDPR, del D.Lgs. 196/2003 e ss.mm.ii. e delle Linee Guida AgID)

Codice Documento: REG-SEC-2026_01

Allegato generale a: Decreti di Autorizzazione per le Unità Organizzative e Atti Integrativi

Destinatari: Personale Docente, Personale Amministrativo (ATA), Collaboratori Scolastici, Collaboratori del DS, Membri del Consiglio di Istituto e soggetti a qualsiasi titolo autorizzati al trattamento.

1. PRINCIPI GENERALI E OBBLIGHI DI RISERVATEZZA

1. **Ambito di Autorizzazione:** Tutto il personale opera sotto la diretta autorità del Dirigente Scolastico (Titolare del trattamento) e del DSGA per i servizi amministrativi, ed è autorizzato a trattare i soli dati personali strettamente necessari alle proprie funzioni istituzionali (principio di minimizzazione e finalità, ex art. 5 GDPR), nel rispetto del Registro delle Attività di Trattamento d'Istituto (TR-01 – TR-06).
2. **Segreto d'Ufficio e Riservatezza Permanente:** L'obbligo di mantenere il più rigoroso riserbo sui dati personali, sulle notizie riservate e sui fatti inerenti gli studenti, le famiglie e il personale conosciuti durante il servizio permane a tempo indeterminato, anche dopo la cessazione del rapporto di lavoro (art. 326 c.p. e art. 28 L. 241/1990).
3. **Tutela delle Comunicazioni Verbali:** È fatto divieto di discutere di situazioni personali o sanitarie di studenti o dipendenti in presenza di terzi (estranei, altri alunni o colleghi non autorizzati), sia di persona che al telefono.

2. REGOLE PER LA GESTIONE DEI DOCUMENTI CARTACEI E DEGLI SPAZI FISICI

1. **Regola della Scrivania Pulita (*Clean Desk*):** Durante l'orario di lavoro, i fascicoli contenenti dati personali non devono essere lasciati incustoditi sulle scrivanie in presenza di visitatori o colleghi non autorizzati. Al termine della giornata lavorativa, tutti i documenti cartacei devono essere riposti negli appositi armadi o cassettiere.

2. **Custodia di Dati Particolari (Sanitari, Diagnosi, L. 104, Giudiziari):** I documenti cartacei contenenti categorie particolari di dati (certificazioni mediche, PEI, PDP, verbali di scrutinio, fascicoli personali) devono essere conservati separatamente dagli atti ordinari, all'interno di archivi o armadi muniti di serratura, le cui chiavi sono affidate esclusivamente al personale di settore autorizzato.
3. **Distruzione Sicura degli Scarti:** Fogli di lavoro, minute, bozze o stampe provvisorie non più necessarie contenenti dati personali non possono essere gettati nel cestino indifferenziato, ma devono essere resi preventivamente illeggibili tramite distruggi-documenti (tritadocumenti).
4. **Accesso ai Locali Operativi:** L'accesso del pubblico e dei visitatori agli uffici di segreteria e di presidenza è limitato all'area di accoglienza/sportello. È vietato l'accesso non presidiato all'area retrostante i banchi operativi o ai locali archivio.

3. UTILIZZO DEGLI STRUMENTI DIGITALI, RETE E CLOUD ISTITUZIONALE

3.1 Ecosistema Cloud Istituzionale e Segregazione dei Dati

- Repository Autorizzati: Tutte le attività di redazione, elaborazione, archiviazione e condivisione di documenti digitali contenenti dati personali devono avvenire esclusivamente all'interno delle piattaforme cloud qualificate e contrattualizzate dall'Istituto (Registro Elettronico, piattaforme gestionali di segreteria, Google Workspace for Education / Microsoft 365 Education di dominio @istituto.edu.it).
- Divieto di Archiviazione Locale su Postazioni Condivise: È severamente vietato salvare file contenenti dati personali (elenchi classi, verbali, valutazioni, PEI, circolari riservate) sul desktop o nelle cartelle locali (*Documenti*, *Download*) di personal computer accessibili a più utenti (LIM d'aula, postazioni dei laboratori didattici, PC delle sale docenti, computer aperti al pubblico o a tirocinanti). Tali postazioni devono intendersi come meri terminali di transito: l'eventuale file temporaneo scaricato deve essere rimosso e il cestino svuotato al termine della sessione di lavoro.
- Permessi di Condivisione Cloud: Quando si creano o condividono file e cartelle sui drive istituzionali, l'operatore deve applicare il principio del minimo privilegio. L'accesso deve essere nominale o circoscritto a gruppi definiti (es. singolo Consiglio di Classe, gruppo dipartimentale, ufficio di competenza). È fatto esplicito divieto di impostare link di condivisione aperti a *«Chiunque abbia il link»* o accessibili al di fuori del dominio istituzionale per documenti recanti dati personali.

3.2 Gestione dei Supporti di Memoria Rimovibili (USB, Hard Disk Esterni, SD Card)

- Regola Generale di Divieto: In virtù della disponibilità degli spazi cloud protetti d'Istituto, l'uso di memorie USB o dischi esterni rimovibili per il trasporto o la conservazione di dati personali è di norma vietato.
- Deroga Tecnica e Cifratura Obbligatoria: Qualora sussista un'inderogabile necessità operativa (es. temporanea assenza di connettività di rete, trasferimento di archivi storici, backup di sicurezza predisposti dall'amministratore di sistema), l'uso di memorie rimovibili è subordinato all'attivazione di sistemi di cifratura hardware o software robusta (es. BitLocker To Go, VeraCrypt, partizioni protette con algoritmo AES a 256 bit) configurati dall'amministratore di sistema o secondo le sue istruzioni. I supporti privi di cifratura non possono in alcun caso ospitare dati identificativi di studenti, famiglie o personale.
- Smaltimento e Riuso di Supporti: Prima di destinare una memoria rimovibile ad altro uso o procedere allo smaltimento dell'hardware obsoleto, deve essere eseguita una procedura di

cancellazione sicura permanente (*wiping* o distruzione fisica del supporto) che impedisca il recupero forense dei file precedentemente memorizzati.

3.3 Utilizzo della Connettività Internet di Plesso (Cablata e Wi-Fi)

- Finalità Istituzionale Esclusiva: Le reti locali d'Istituto (LAN cablata e wireless) e la relativa connettività Internet sono destinate esclusivamente allo svolgimento delle mansioni didattiche, amministrative e gestionali. Non è consentito saturare la banda per scopi personali, intrattenimento, streaming non didattico o attività ludiche.
- Separazione delle Reti (VLAN e SSID Dedicati): L'accesso alla rete Wi-Fi istituzionale è segmentato:
    - *Rete Amministrazione/Docenti:* riservata ai dispositivi di servizio e protetta da autenticazione dedicata (WPA2/WPA3 Enterprise o credenziali nominali);
    - *Rete Didattica/Studenti:* protetta e filtrata per le attività laboratoriali;
    - *Rete Ospiti (Guest):* totalmente isolata dai server scolastici e destinata a visitatori occasionali o eventi collegiali. È fatto divieto di collegare apparati personali non autorizzati alla rete riservata all'amministrazione o accedere alle risorse di rete scavalcando le configurazioni di sicurezza.
- Filtri di Rete e Divieto di Bypassing: L'Istituto adotta sistemi di filtraggio dei contenuti (firewall, DNS filtering, content filtering) a tutela della sicurezza della rete e dei minori. È vietato installare, configurare o utilizzare software di tunneling, VPN commerciali, proxy server o nodi Tor per eludere i blocchi di sicurezza o mascherare il traffico telematico originato dalle postazioni d'Istituto.

3.4 Integrità Software, Download e Divieto di Modifiche di Sistema

- Policy sul Software: Gli utenti abilitati non possono installare autonomamente programmi, applicativi eseguibili (.exe, .msi), script o estensioni per browser non preventivamente collaudati e autorizzati dal Dirigente Scolastico, sentito il parere dell'Amministratore di Sistema o dell'Animatore Digitale.
- Diritti Amministrativi Locali: Dove tecnicamente configurabile, i privilegi di amministratore locale (*root/admin*) sulle macchine d'Istituto sono rimossi dalle utenze ordinarie per prevenire l'infezione da ransomware o la compromissione involontaria del sistema operativo.
- Divieto P2P e Download Massivi: È formalmente interdetto l'uso di software di condivisione peer-to-peer (es. BitTorrent), client di download massivo o strumenti di file sharing non istituzionale sui dispositivi e sulle reti dell'Istituto.

4. GESTIONE DELLE CREDENZIALI DI ACCESSO E SICUREZZA LOGICA

4.1 Principio di Univocità e Segretezza delle Credenziali

- Identificazione Univoca: Ciascun soggetto autorizzato accede ai sistemi informatici dell'Istituto unicamente mediante credenziali personali e nominali che consentono di attribuire ogni singola operazione al rispettivo operatore.
- Divieto Assoluto di Cessione o Condivisione: Le credenziali d'accesso (username, password, PIN, certificati digitali, token OTP) sono strettamente personali e riservate. È fatto espresso divieto di:

    - Comunicare le proprie password a colleghi, assistenti, studenti o soggetti esterni all'istituto, per qualsiasi motivazione anche eccezionale o contingente (es. ferie, urgenze d'ufficio, supplenze brevi);
    - Utilizzare profili generici o condivisi (*"docente"*, *"segreteria"*, *"amministrazione"*) per compiere atti amministrativi, verbalizzazioni, inserimento voti o rilascio di atti;
    - Consentire a terzi di operare su un applicativo lasciando la propria sessione aperta.
- Inviolabilità verso le Figure Apicali e Tecniche: Nessun amministratore di sistema, tecnico di laboratorio o dirigente scolastico è autorizzato a richiedere la password personale a un utente. L'assistenza tecnica o la gestione operativa delegata deve avvenire mediante strumenti di delega amministrativa, reset della password o reindirizzamento dei privilegi, mai tramite l'impossessamento della password dell'interessato.

4.2 Autenticazione Forte (MFA) e Identità Digitali Federate

- Adozione Obbligatoria dell'Autenticazione a Più Fattori: L'accesso all'account di posta istituzionale (@istituto.edu.it), alla console di amministrazione cloud, al Registro Elettronico e alle piattaforme che contengono dati personali deve essere obbligatoriamente presidiato da un meccanismo di Autenticazione a Più Fattori (MFA / 2FA).
- Canali di Autenticazione: L'autenticazione secondaria deve essere garantita mediante app authenticator su dispositivo mobile protetto (es. Google Authenticator, Microsoft Authenticator) o chiave di sicurezza hardware FIDO2. L'uso di SMS è consentito solo in assenza di alternative tecniche superiori.
- Accesso con Identità Federate (SPID / CIE): Qualora i portali ministeriali (SIDI, Portale Acquisti, PagoInRete) o il Registro Elettronico supportino l'accesso tramite SPID (almeno Livello 2) o CIE, tale canale costituisce il metodo primario e raccomandato di autenticazione per garantire la certezza dell'identità dell'operatore.

4.3 Criteri di Costruzione, Lunghezza e Gestione del Ciclo di Vita delle Password

- Costruzione e Lunghezza Minima: Nei contesti in cui è previsto l'uso di password alfanumeriche interne all'istituto, la parola d'ordine deve possedere una lunghezza non inferiore a 12 caratteri (raccomandati 14 o formulazione a *passphrase*, ossia frasi di facile memorizzazione ma complesse da decifrare per attacchi a dizionario) e contenere almeno tre delle seguenti categorie: lettere maiuscole, minuscole, cifre numeriche, simboli grafici/punteggiatura.
- Divieto di Sequenze Banali e Riferimenti Evidenti: La password non deve consistere in sequenze ovvie (es. 12345678, qwerty), combinazioni associate al nome della scuola, all'anno scolastico in corso, né contenere il nome, cognome, data di nascita dell'operatore o parole del vocabolario comune.
- Modifica al Primo Accesso: Le password temporanee rilasciate d'ufficio o generate a seguito di procedura di reset devono essere obbligatoriamente sostituite dall'utente al momento del primo accesso.
- Superamento della Scadenza Frequente Forzata: In linea con gli standard tecnici moderni (NIST SP 800-63B, AgID), la password non è soggetta a scadenza temporale obbligatoria a breve termine (es. ogni 90 giorni), al fine di evitare che gli utenti ricorrano a pattern ripetitivi o variazioni minime. Il cambio password resta invece obbligatorio e immediato:
    - Al primo utilizzo della credenziale temporanea;

- In presenza di indizi, sospetti o notifiche di compromissione, data breach, tentativi di phishing o accesso anomalo;
- Su richiesta motivata del Dirigente Scolastico o del Responsabile della Protezione dei Dati a fronte di incidenti di sicurezza.

4.4 Misure di Protezione della Sessione: Blocco Schermo e Browser Hygiene

- Regola del Blocco Schermo (*Clean Screen*): È fatto obbligo a qualunque dipendente che si allontani dalla propria postazione informatica – anche solo per una frazione di minuto – di provvedere al blocco immediato della sessione di lavoro **(utilizzando la combinazione di tasti Windows + L sui sistemi Windows, o l'equivalente comando di blocco su macOS/Linux)** o al log-out dall'applicativo in uso. Le postazioni d'ufficio devono essere configurate per attivare lo screensaver con blocco automatico dopo un periodo massimo di 5-10 minuti di inattività.
- Divieto di Memorizzazione Password sui Browser: È severamente vietato salvare o acconsentire alla memorizzazione automatica delle password sui browser web (funzione *"Ricorda la password"* o salvataggio nelle impostazioni di Chrome, Edge, Firefox) installati su personal computer ad uso promiscuo, condiviso, d'aula o di laboratorio. L'eventuale memorizzazione delle credenziali è tollerata unicamente su dispositivi ad assegnazione individuale esclusiva, a condizione che l'intero disco o il profilo utente del sistema operativo sia protetto da autenticazione forte.
- Chiusura della Sessione (*Log-out*): Al termine dell'orario di lavoro o al completamento delle registrazioni (in particolare sul Registro Elettronico d'aula o sui software contabili), l'utente deve terminare la sessione cliccando sull'apposito pulsante di *Log-out/Disconnetti*, chiudere le schede del browser e provvedere al corretto spegnimento del personal computer, qualora non vi siano processi di backup notturni centralizzati predisposti.

5. DISCIPLINA DELLA POSTA ELETTRONICA ISTITUZIONALE

1. **Casella Nominale Istituzionale (@istituto.edu.it):** La casella di posta assegnata al dipendente è uno strumento di lavoro. Tutte le comunicazioni con studenti, famiglie, colleghi ed enti esterni devono transitare esclusivamente tramite questo account.
2. **Utilizzo Obbligatorio del CCN:** Nelle comunicazioni rivolte a elenchi di destinatari (classi, gruppi di genitori, fornitori), è obbligatorio inserire gli indirizzi nel campo **CCN** (Copia Conoscenza Nascosta) per impedire la diffusione non autorizzata di recapiti.
3. **Gestione Assenze e Continuità del Servizio:** In conformità ai provvedimenti del Garante sull'uso dell'email aziendale, in caso di assenza programmata o prolungata, il dipendente deve attivare un messaggio di risposta automatica che indichi i recapiti di segreteria o del sostituto. L'Istituto non accede alla casella del dipendente salvo eventi eccezionali e urgenti, mediante procedura tracciata e congiunta (DS/DSGA e RPD).
4. **Informativa ai Destinatari (Disclaimer):** In calce alle email istituzionali è impostato il disclaimer predefinito che attesta la natura istituzionale e non personale del messaggio e le avvertenze sulla riservatezza.

    1. *L'Istituto precisa, in accordo con i propri operatori, che le caselle di posta elettronica utilizzate, sia generiche (es. info, amministrazione) che nominali (cognome.nome) non devono essere utilizzate per messaggi di natura personale o riservata in quanto i messaggi ricevuti o inviati possono essere analizzati dalle funzioni a ciò preposte per ragioni di sicurezza. In caso di assenza prolungata di un operatore i messaggi a lui indirizzati vengono*

letti da altre funzioni. In caso sia necessario attivare canali di comunicazione riservati si prega di contattare direttamente l'operatore interessato.

6. UTILIZZO DI DISPOSITIVI PERSONALI (BYOD) E LAVORO A DISTANZA

1. **Modalità di Accesso Consentita:** L'accesso al Registro Elettronico e alle piattaforme scolastiche da dispositivi personali (smartphone, tablet, PC portatili privati) è consentito unicamente tramite browser web protetto o app ufficiali fornite dai vendor (es. app Registro Elettronico).
2. **Divieto di Archiviazione Locale:** È fatto espresso divieto di scaricare, memorizzare in locale in modo permanente o trasferire su memorie private non cifrate documenti contenenti dati sanitari, certificazioni L. 104/DSA, note disciplinari o graduatorie con dati personali.
3. **Requisiti del Dispositivo Privato:** Qualora il personale utilizzi propri apparati, ha l'onere di garantire che il dispositivo sia dotato di:
    - Meccanismo di blocco automatico tramite PIN, password o biometria;
    - Sistema operativo e antivirus regolarmente aggiornati;
    - Assenza di software contraffatto o di modifiche di sistema (rooting/jailbreak) che ne abbassino la sicurezza.

7. RIPRESE FOTOGRAFICHE, AUDIO/VIDEO E GESTIONE DELLA DIFFUSIONE

1. **Produzione e Conservazione per Finalità Istituzionali e Didattiche:**
    - L'Istituzione Scolastica è pienamente titolata a produrre, raccogliere e conservare immagini, registrazioni audio e filmati ritraenti studenti e personale nell'ambito delle ordinarie attività didattiche, formative, laboratoriali, sportive e progettuali previste dal PTOF.
    - Tale trattamento persegue finalità istituzionali di pubblico interesse connesse all'istruzione e alla documentazione dell'attività educativa (art. 6, par. 1, lett. e) del GDPR e D.Lgs. 297/1994). Per la mera produzione, consultazione e conservazione a uso interno non è richiesta alcuna preventiva autorizzazione o consenso da parte delle famiglie o degli alunni.
2. **Regime di Diffusione Esterna (Sito Web, Social Media d'Istituto, Stampa, Canali Aperti):**
    - Qualora si renda necessaria o opportuna la diffusione esterna di immagini o filmati (es. pubblicazione sul portale web d'Istituto, bacheche accessibili al pubblico, profili social della scuola, mostre aperte alla cittadinanza o testate giornalistiche), il trattamento esula dalla normale documentazione interna.
    - La diffusione non può mai avvenire sulla base di deleghe o consensi generici. Ogni operazione di pubblicazione deve essere gestita di volta in volta, predisponendo una specifica informativa e liberatoria (ai sensi degli artt. 13 GDPR e 96 della Legge 633/1941 sul diritto d'autore) da sottoporre agli interessati (o ai titolari della responsabilità genitoriale in caso di minori), nella quale siano chiaramente descritti:
        - Le specifiche finalità dell'iniziativa o dell'evento;
        - I mezzi, i formati e i canali di diffusione prescelti (es. sito istituzionale, canale video scolastico, pubblicazione a stampa);

        - I tempi e le modalità di conservazione o permanenza online della pubblicazione.

3. **Misure di Sicurezza e Divieto di Utilizzo di Canali Personali:**
    - Le riprese e i materiali multimediali didattici devono essere acquisiti mediante dispositivi della scuola oppure conferiti tempestivamente negli spazi di archiviazione protetti d'Istituto (Google Workspace / Microsoft 365 di dominio), cancellando i file originari da memorie temporanee o da dispositivi eventualmente utilizzati per la cattura.
    - È severamente vietata la diffusione, trasmissione o pubblicazione di fotografie o video ritraenti allievi o colleghi attraverso canali privati del docente (profili social personali, chat WhatsApp/Telegram non ufficiali, siti internet propri).

8. SEGNALAZIONE DI INCIDENTI E GESTIONE DATA BREACH

1. Qualsiasi evento anomalo suscettibile di compromettere la riservatezza, integrità o disponibilità dei dati (es. furto/smarrimento di dispositivi, attacco malware/ransomware, ricezione di email phishing con inserimento credenziali, invio accidentale di documenti riservati a terzi) deve essere **segnalato entro 2-4 ore** al Dirigente Scolastico, al DSGA o all'indirizzo del Responsabile della Protezione dei Dati (rpd@vincenzi.com).
2. La gestione dell'evento seguirà la specifica *Procedura Operativa per la Gestione e Notifica delle Violazioni di Dati Personali* d'Istituto (artt. 33 e 34 GDPR).

9. PRINCIPI, LIMITI E MODALITÀ DI ESECUZIONE DEI CONTROLLI SUGLI STRUMENTI INFORMATICI

9.1 Quadro Normativo e Garanzie Statutarie

1. **Conformità all'Art. 4 dello Statuto dei Lavoratori:** Gli strumenti elettronici, i software applicativi, le caselle di posta elettronica e la rete telematica sono messi a disposizione del personale esclusivamente per rendere la prestazione lavorativa. Ai sensi dell'art. 4 della Legge n. 300/1970 (come modificato dal D.Lgs. 151/2015), tali strumenti non sono preordinati, né possono essere in alcun caso utilizzati, per finalità di controllo a distanza dell'attività lavorativa dei dipendenti.
2. **Divieto di Controlli Indiscriminati, Massivi e Costanti:** L'Istituto non effettua, né direttamente né tramite amministratori di sistema o fornitori esterni, controlli continui, prolungati o a tappeto sulla navigazione Internet, sui contenuti dei messaggi di posta elettronica o sull'utilizzo delle postazioni informatiche da parte del personale. È fatto espresso divieto di impiegare sistemi di tracciamento occulto, *keylogger*, registratori di schermate o strumenti di monitoraggio dell'attività in tempo reale.

9.2 Finalità Esclusive dei Controlli Tecnici Le verifiche sui sistemi e sulle reti sono consentite unicamente per:

- **Sicurezza delle Reti e dei Sistemi:** Tutela dell'integrità del patrimonio informativo dell'Istituto, prevenzione e contrasto di infezioni malware/ransomware, tentativi di intrusione o accessi anomali;
- **Continuità Operativa:** Ripristino della funzionalità dei servizi, diagnostica tecnica per guasti o malfunzionamenti hardware/software, allocazione corretta della banda di rete;
- **Difesa dei Diritti dell'Istituto:** Accertamento di illeciti o abusi gravi nei casi consentiti dalla legge, a fronte di specifiche e documentate anomalie.

9.3 Criterio di Gradualità e Proporzionalità Qualora emerga un'anomalia tecnica (es. traffico di rete anomalo, saturazione della banda, notifiche del firewall o dell'antivirus), le attività di verifica devono rigorosamente rispettare il principio di proporzionalità e gradualità articolandosi nei seguenti livelli:

1. **Livello 1 - Verifiche Aggregate e Anonime:** L'analisi tecnica deve essere condotta esclusivamente a livello macroscopico, anonimo o aggregato (es. monitoraggio del volume complessivo del traffico telematico di plesso o del consumo di risorse di sistema), senza fare riferimento al singolo operatore o alla specifica postazione.
2. **Livello 2 - Alert e Richiamo Organizzativo Generale:** Qualora vengano rilevati utilizzi non conformi o potenziali vulnerabilità a livello generale, il Dirigente Scolastico dirama un richiamo operativo o una circolare interna alle Unità Organizzative interessate, ricordando l'osservanza del presente Regolamento.
3. **Livello 3 - Accertamenti Mirati su Dati Specifici:** L'accesso a log o dati riferibili a singoli apparati o account è ammesso **esclusivamente** come misura di *extrema ratio*, qualora le verifiche anonime non abbiano consentito di rimuovere la minaccia alla sicurezza informatica, oppure in presenza di una formale notifica di *data breach* o di un'espressa richiesta dell'Autorità Giudiziaria.

9.4 Conservazione dei Log e Gestione dei Metadati

1. **Log di Connessione e Accesso:** I dati di traffico telematico interno e i file di log generati dai sistemi (firewall, server, console cloud) sono registrati e conservati per il tempo strettamente necessario a garantire la sicurezza delle reti e l'adempimento degli obblighi di legge, nel rispetto dei principi di minimizzazione e pseudonimizzazione.
2. **Metadati della Posta Elettronica:** In conformità agli orientamenti del Garante per la Protezione dei Dati Personali, i metadati tecnici relativi alla trasmissione e ricezione dei messaggi di posta elettronica (indirizzi mittente/destinatario, data, ora, oggetto, dimensione allegati) sono conservati dai sistemi centralizzati per un periodo limitato, di norma non superiore a pochi giorni (salve comprovate e documentate esigenze tecniche o organizzative dell'Istituto), trascorso il quale vengono cancellati automaticamente.
3. **Divieto di Esame dei Contenuti Privati:** L'attività di manutenzione ordinaria e gestione delle reti non autorizza in alcun caso l'apertura, la lettura o l'estrazione dei contenuti testuali dei messaggi di posta elettronica o dei file presenti negli spazi cloud individuali degli operatori, salvo esplicito e tracciato mandato nei limiti di legge.

9.5 Garanzie di Trasparenza verso il Lavoratore L'adozione del presente Regolamento, la sua notifica all'atto della presa di servizio e la pubblicazione all'Albo Online costituiscono formale adempimento degli obblighi di informazione previsti dall'art. 4, comma 3, della Legge 300/1970 e dall'art. 13 del GDPR. Le informazioni e i dati tecnici legittimamente raccolti nel rispetto delle procedure sopra descritte sono utilizzabili a tutti i fini connessi al rapporto di lavoro, ivi compresi i procedimenti a tutela del patrimonio scolastico o disciplinari, esclusivamente nei casi e con le modalità previsti dalla legge e dai contratti collettivi nazionali di lavoro.

Revisione 2609