ISTITUTO COMPRENSIVO SANT'ELIA
C.F. 90032250608 C.M. FRIC857001
AE651E1 - IC Sant'Elia Fiumerapido Ufficio Protocollo
Prot. 0004154/U del 02/07/2026 08:21 II.5 - Dirigente

ISTITUTO COMPRENSIVO STATALE "SANT'ELIA FIUMERAPIDO"
Cod. Mecc. FRIC857001 | Via IV Novembre SNC – 03040 Sant'Elia Fiumerapido (FR)
C.F. 91023590609 | Tel./Fax 0776 608140 | fric857001@istruzione.it | fric857001@pec.istruzione.it

DISCIPLINARE PER L'UTILIZZO DELLA POSTA ELETTRONICA ISTITUZIONALE E DELLA POSTA ELETTRONICA CERTIFICATA (PEC)

(Approvato dal Consiglio di Istituto con Delibera n. 6 del 22 giugno 2026)

CAPO I – DISPOSIZIONI GENERALI

Art. 1 – Oggetto e finalità

1. Il presente Disciplinare definisce le regole di utilizzo della posta elettronica ordinaria istituzionale (PEO) e della posta elettronica certificata (PEC) dell'Istituto Comprensivo Statale "Sant'Elia Fiumerapido" (di seguito "Istituto"), da parte del personale docente, del personale amministrativo tecnico e ausiliario (ATA) e del Dirigente Scolastico.

2. Scopo del presente Disciplinare è:

- garantire la corretta gestione degli strumenti di comunicazione elettronica istituzionale;
- tutelare la sicurezza informatica dell'Istituto e dei dati personali trattati;
- preservare la reputazione e il decoro dell'Istituto nelle comunicazioni digitali;
- assicurare la conformità alle disposizioni del Codice dell'Amministrazione Digitale (CAD), del Codice di comportamento dei dipendenti pubblici e della normativa in materia di protezione dei dati personali.

Art. 2 – Fonti normative

Il presente Disciplinare è adottato in conformità a:

- D.Lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale – CAD) e successive modificazioni;
- D.P.R. 11 febbraio 2005, n. 68 (Posta elettronica certificata);
- Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 10 agosto 2018, n. 101;
- Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), artt. 4 e 8, come modificati dal D.Lgs. 14 settembre 2015, n. 151;
- D.P.R. 16 aprile 2013, n. 62 (Codice di comportamento dei dipendenti pubblici), come modificato dal D.P.R. 13 giugno 2023, n. 81, in particolare artt. 11-bis e 11-ter;
- Linee Guida del Garante per la protezione dei dati personali su Internet e posta elettronica nel rapporto di lavoro (doc. web n. 1387522);
- Documento di indirizzo del Garante per la protezione dei dati personali del 6 giugno 2024 (doc. web n. 10026277) su programmi e servizi di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati;
- Circolare AgID n. 2/2017 – Misure minime di sicurezza ICT per le pubbliche amministrazioni;
- Linee Guida dell'Agenzia per la Cybersicurezza Nazionale (ACN);
- Nota MIM prot. 4730 del 22 luglio 2025 (allineamento indirizzi PEO/PEC al codice meccanografico);

- Codice di comportamento dell'Istituto vigente pro tempore;
- Piano Triennale per la Prevenzione della Corruzione e della Trasparenza (PTPCT) dell'Istituto.

Art. 3 – Definizioni

Ai fini del presente Disciplinare si intende per:

- "PEO" (Posta Elettronica Ordinaria): casella di posta istituzionale dell'Istituto con indirizzo fric857001@istruzione.it, ai sensi della Nota MIM prot. 4730/2025; casella individuale del personale con formato nome.cognome@scuola.istruzione.it;
- "PEC" (Posta Elettronica Certificata): casella certificata dell'Istituto con indirizzo fric857001@pec.istruzione.it, avente valore legale equiparato alla raccomandata con avviso di ricevimento (D.P.R. n. 68/2005);
- "Metadati": dati relativi all'utilizzo della posta elettronica (mittente, destinatario, oggetto, data/ora di invio e ricezione, dimensione), distinti dal contenuto del messaggio;
- "Amministratore di Sistema": soggetto incaricato della gestione tecnica dei sistemi informatici e della casella istituzionale;
- "Utente": qualsiasi componente del personale dell'Istituto (DS, DSGA, docenti, ATA) che utilizza la PEO o la PEC istituzionale nell'esercizio delle proprie funzioni;
- "Credenziali": username e password (o codice MFA – Multi-Factor Authentication) necessari per accedere alle caselle di posta.

Art. 4 – Ambito di applicazione

1. Il presente Disciplinare si applica a tutto il personale dell'Istituto – docente e ATA, a tempo indeterminato e determinato, in servizio presso qualsiasi plesso – che utilizzi, a qualsiasi titolo e per qualsiasi finalità istituzionale, la PEO o la PEC dell'Istituto.

2. Il Disciplinare si applica altresì ai collaboratori esterni, ai tirocinanti e ai soggetti incaricati di attività in favore dell'Istituto che abbiano accesso agli strumenti di comunicazione istituzionale, nei limiti delle rispettive competenze.

CAPO II – TIPOLOGIE DI STRUMENTI E GESTIONE DELLE CASELLE

Art. 5 – Posta Elettronica Ordinaria istituzionale (PEO)

1. L'Istituto dispone di due tipologie di PEO:

- casella istituzionale dell'Istituto (fric857001@istruzione.it): gestita dal DSGA, utilizzata per le comunicazioni ufficiali dell'Istituto verso l'esterno (MIM, USR, enti pubblici, soggetti privati, famiglie); acceduta dal DSGA e dal DS;
- caselle individuali del personale (nome.cognome@scuola.istruzione.it): assegnate dal MIM al personale con contratto di almeno 60 giorni, ai sensi della Nota MIM prot. 3807/2022 e successive disposizioni; prerequisito obbligatorio per DS, DSGA e personale amministrativo di segreteria per l'abilitazione al SIDI.

2. Le caselle individuali sono strumenti di lavoro a carattere istituzionale e devono essere utilizzate esclusivamente per finalità di servizio connesse alle funzioni svolte presso l'Istituto.

3. Le caselle individuali soggette a disattivazione automatica per inattività superiore a sei mesi o per cessazione del rapporto di lavoro da più di tre mesi. I titolari sono tenuti ad accedere periodicamente alle proprie caselle per evitarne la disattivazione e a comunicare tempestivamente al DSGA qualsiasi variazione del proprio status lavorativo.

4. L'accesso alla PEO istituzionale e alle caselle individuali richiede l'autenticazione a più fattori (MFA) mediante l'applicazione "Microsoft Authenticator" o strumento equivalente indicato dal MIM, in conformità alla Nota MIM prot. 5430/2024.

Art. 6 – Posta Elettronica Certificata (PEC)

1. La PEC dell'Istituto (fric857001@pec.istruzione.it) costituisce lo strumento di comunicazione ufficiale avente valore legale equiparato alla raccomandata con avviso di ricevimento ai sensi del D.P.R. n. 68/2005 e dell'art. 48 del CAD.

2. La PEC istituzionale è gestita esclusivamente dal DSGA e dal Dirigente Scolastico, o da chi ne fa le veci per delega espressa. Nessun altro soggetto è autorizzato ad accedere o a inviare messaggi dalla PEC istituzionale senza specifica autorizzazione scritta del Dirigente Scolastico.

3. La PEC è utilizzata obbligatoriamente per:

- le comunicazioni con MIM, USR, Ambito Territoriale, INPS, INAIL, Ragioneria dello Stato e altri enti pubblici;
- la trasmissione di atti, contratti, decreti e provvedimenti aventi rilevanza giuridica;
- le notifiche e comunicazioni nell'ambito dei procedimenti amministrativi formali;
- le comunicazioni con il Tribunale, la Prefettura, la Procura della Repubblica e gli uffici giudiziari;
- la ricezione di atti aventi valore legale da privati e da soggetti giuridici.

4. La PEC istituzionale NON può essere utilizzata per comunicazioni di carattere informale, per l'invio di circolari interne ordinarie o per finalità non connesse all'attività istituzionale.

5. Il DSGA assicura la consultazione della casella PEC almeno una volta per ogni giorno lavorativo e garantisce la tempestiva lettura dei messaggi pervenuti. In caso di assenza programmata del DSGA, il Dirigente Scolastico individua un sostituto per la gestione della PEC per il periodo di assenza.

Art. 7 – Firma digitale e firma elettronica qualificata nei messaggi

1. I documenti trasmessi via PEC aventi natura di provvedimento amministrativo (decreti, delibere, contratti, atti di accertamento) devono essere firmati digitalmente ai sensi degli artt. 20 e 21 del CAD prima dell'invio.

2. La firma digitale del Dirigente Scolastico e del DSGA deve essere mantenuta in corso di validità e rinnovata tempestivamente alla scadenza. La custodia del dispositivo di firma è personale e intrasferibile.

3. I documenti trasmessi via PEO a fini informativi non richiedono firma digitale, fatta eccezione per i casi in cui la normativa di settore la preveda obbligatoriamente.

CAPO III – REGOLE D'USO

Art. 8 – Principi generali di utilizzo

1. Ai sensi dell'art. 11-bis del D.P.R. n. 62/2013, come modificato dal D.P.R. n. 81/2023, l'utilizzo dell'account istituzionale è consentito soltanto per fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'Istituto.

2. L'utilizzo di caselle di posta elettronica personali per attività o comunicazioni afferenti il servizio è di norma evitato, salvi i casi di forza maggiore dovuti a circostanze eccezionali documentabili, dei quali il dipendente dà comunicazione al Dirigente Scolastico o al DSGA.

3. Le comunicazioni istituzionali devono essere formalmente corrette, chiare, rispettose del decoro dell'Istituto e redatte in italiano, salvo i casi in cui la comunicazione con soggetti esteri richieda l'uso di altra lingua.

✓ USI CONSENTITI	✗ USI VIETATI
Comunicazioni di servizio con personale, famiglie, enti pubblici, fornitori	Utilizzo per fini personali, commerciali o politici
Trasmissione di circolari, note, verbali, atti ufficiali	Invio di catene di messaggi, spam, contenuti satirici non istituzionali

Ricezione e inoltro di comunicazioni MIM, USR, INPS, INAIL, enti previdenziali	Iscrizione a newsletter o servizi privati con l'indirizzo istituzionale
Notifiche e comunicazioni nell'ambito di progetti PNRR, PON, PN	Utilizzo dell'e-mail istituzionale come recapito personale su social media
Corrispondenza con famiglie per comunicazioni scolastiche ufficiali	Apertura di allegati di provenienza sconosciuta o dubbia (phishing)
Invio di documenti firmati digitalmente nell'ambito dei procedimenti istituzionali	Divulgazione a terzi delle credenziali di accesso

Art. 9 – Gestione dei messaggi in entrata

1. Il personale abilitato è tenuto a verificare con regolarità la propria casella di posta istituzionale. In via di prassi, si raccomanda la verifica almeno una volta al giorno nei giorni lavorativi.

2. In caso di messaggi di provenienza sospetta o di tentativi di phishing (richiesta fraudolenta di credenziali o dati personali), l'utente è tenuto a:

- non aprire allegati né cliccare su link contenuti nel messaggio;
- segnalare immediatamente il messaggio al DSGA o al Responsabile della Sicurezza Informatica dell'Istituto;
- non rispondere al mittente;
- conservare il messaggio ai fini di eventuale analisi forense.

3. I messaggi di posta elettronica ricevuti nella casella istituzionale sono documenti informatici a tutti gli effetti e devono essere conservati con le stesse modalità previste per la corrispondenza cartacea, secondo le norme sul protocollo informatico e la gestione documentale.

Art. 10 – Protocollazione della corrispondenza elettronica

1. La corrispondenza in entrata e in uscita tramite PEO e PEC istituzionale è soggetta a protocollazione ai sensi del D.P.R. 28 dicembre 2000, n. 445 e del D.P.C.M. 3 dicembre 2013 (Regole tecniche per il protocollo informatico).

2. Il DSGA assicura la registrazione tempestiva al protocollo informatico di tutti i documenti rilevanti ai fini dei procedimenti amministrativi in corso, indicando per ciascuno: data di ricezione, mittente, oggetto e numero di protocollo assegnato.

3. La protocollazione avviene attraverso il sistema informativo istituzionale adottato dall'Istituto. Non è ammessa la protocollazione manuale di documenti informatici, salvo indisponibilità temporanea del sistema, documentata e comunicata al Dirigente Scolastico.

Art. 11 – Risposta automatica in caso di assenza

1. In caso di assenza programmata (congedo, ferie, missione, malattia di durata prevedibile), i titolari di casella individuale abilitata sono tenuti ad attivare il messaggio di risposta automatica (out-of-office), indicando:

- il periodo di assenza;
- il nominativo e il recapito del soggetto che gestisce la corrispondenza durante l'assenza;
- eventuali modalità alternative di contatto per urgenze.

2. Il mancato rientro nei tempi indicati nel messaggio automatico deve essere comunicato al DSGA affinché possa essere aggiornato il messaggio di risposta.

Art. 12 – Sicurezza delle credenziali e protezione degli accessi

1. Le credenziali di accesso alle caselle di posta (username, password, dispositivo MFA) sono personali, strettamente riservate e non cedibili a terzi.

2. Il personale è tenuto a:

- modificare la password periodicamente (almeno ogni 6 mesi) e comunque ogni qualvolta si sospetti che le credenziali possano essere state compromesse;
- non annotare le credenziali in luoghi accessibili a terzi;
- non comunicare le credenziali nemmeno al personale di supporto tecnico, che non ne ha necessità per finalità di manutenzione;
- segnalare tempestivamente al DSGA e al Dirigente Scolastico qualsiasi sospetto di accesso non autorizzato alla propria casella;
- non accedere alla propria casella da dispositivi pubblici o condivisi senza adottare le necessarie precauzioni (sessione privata, disconnessione al termine).

3. Il Dirigente Scolastico, nel caso di dimissioni, cessazione, pensionamento o trasferimento di un dipendente, dispone tempestivamente la disattivazione della casella individuale ovvero la revoca delle autorizzazioni di accesso, comunicandolo al DSGA.

CAPO IV – PROTEZIONE DEI DATI PERSONALI E METADATI

Art. 13 – Trattamento dei dati personali nelle comunicazioni elettroniche

1. Le comunicazioni elettroniche dell'Istituto possono contenere dati personali di dipendenti, alunni, famiglie e soggetti terzi. Il personale è tenuto a trattare tali dati nel rispetto dei principi del GDPR, con particolare riguardo ai principi di minimizzazione, pertinenza e riservatezza.

2. È vietato:

- inviare via PEO o PEC dati personali di alunni (in particolare dati relativi alla salute, a situazioni di disagio, a procedimenti di tutela) a destinatari non autorizzati o senza adeguata cifratura;
- trasmettere dati sensibili in chiaro (non cifrati) quando siano disponibili modalità di trasmissione sicura;
- inserire in copia visibile (CC) soggetti non legittimati a conoscere i dati contenuti nel messaggio; utilizzare il campo CCN (copia nascosta) quando la comunicazione è personalizzata e riguarda singoli destinatari.

3. Per le comunicazioni a gruppi (famiglie di una classe, personale di un plesso), si utilizza la funzione di invio individuale o di lista di distribuzione chiusa, al fine di non rendere visibili a tutti i destinatari i recapiti altrui.

Art. 14 – Metadati della posta elettronica

1. In conformità al Documento di indirizzo del Garante per la protezione dei dati personali del 6 giugno 2024 (doc. web n. 10026277), l'Istituto informa il personale che i sistemi di gestione della posta elettronica possono raccogliere e conservare automaticamente i metadati delle comunicazioni (mittente, destinatario, oggetto, data/ora, dimensione del messaggio).

2. I metadati sono trattati dall'Istituto per finalità strettamente connesse al corretto funzionamento e alla sicurezza del sistema di posta elettronica, nel rispetto dei principi di necessità e proporzionalità.

3. La conservazione dei metadati avviene per un periodo non superiore a quello strettamente necessario alle finalità di sicurezza informatica e di garanzia dell'integrità del sistema. Il Responsabile della Protezione dei Dati (RPD), ove nominato, è consultato in merito ai periodi di conservazione.

4. I metadati NON sono utilizzati per finalità di monitoraggio sistematico dell'attività lavorativa dei dipendenti, in conformità all'art. 4 della L. n. 300/1970 e al GDPR.

Art. 15 – Controlli sul sistema di posta elettronica

1. Ai sensi dell'art. 4, comma 2, della L. n. 300/1970, la PEO e la PEC, in quanto strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, non sono soggetti alle garanzie procedurali previste dall'art. 4, comma 1 (accordo sindacale o autorizzazione amministrativa), limitatamente ai controlli strettamente necessari per garantire la sicurezza e il corretto funzionamento del sistema.

2. I controlli effettuati dall'Istituto sul sistema di posta hanno esclusivamente finalità di:

- prevenzione e contrasto di attacchi informatici (malware, phishing, ransomware);
- garanzia della continuità operativa del sistema;
- individuazione di anomalie di funzionamento;
- verifica di incidenti di sicurezza.

3. Qualsiasi controllo sul contenuto delle comunicazioni personali dei dipendenti non è ammesso e sarebbe in contrasto con l'art. 4, comma 1, L. n. 300/1970 e con gli artt. 8 e 113 del D.Lgs. n. 196/2003.

4. Ai sensi delle Linee Guida del Garante per la protezione dei dati personali, l'Istituto fornisce al personale adeguata informazione sulle modalità di utilizzo degli strumenti di posta e sulle possibilità di controllo nel rispetto dei limiti di legge, mediante la presente informativa allegata al Disciplinare.

CAPO V – ARCHIVIAZIONE, CONSERVAZIONE E GESTIONE DOCUMENTALE

Art. 16 – Archiviazione dei messaggi

1. La posta elettronica istituzionale (PEO e PEC) è parte integrante del sistema di gestione documentale dell'Istituto. I messaggi aventi rilevanza amministrativa devono essere archiviati in modo ordinato e accessibile.

2. Il DSGA definisce le procedure di archiviazione della casella PEO istituzionale e della PEC, organizzando le cartelle per anno, tipologia di pratica e ufficio di riferimento.

3. La cancellazione definitiva di messaggi aventi rilevanza giuridica o amministrativa è vietata. I messaggi eliminati accidentalmente devono essere recuperati tempestivamente e la circostanza comunicata al DSGA.

4. Al termine di ogni anno scolastico, il DSGA provvede all'archiviazione permanente dei messaggi dell'anno e alla loro conservazione per i termini previsti dalle norme in materia di conservazione degli atti amministrativi.

Art. 17 – Conservazione digitale a norma

1. I messaggi PEC aventi valore legale sono conservati in conformità alle Linee Guida AgID sulla conservazione dei documenti informatici (determina AgID n. 407/2021 e successive).

2. L'Istituto adotta, nei limiti delle risorse disponibili, un sistema di conservazione digitale a norma o si avvale di un conservatore accreditato AgID per i documenti che richiedono conservazione a lungo termine.

3. Il DSGA assicura che i messaggi PEC costituenti ricevute di consegna e avvisi di mancata consegna siano conservati unitamente al messaggio originale, quale prova dell'avvenuta notifica.

CAPO VI – OBBLIGHI, DIVIETI E SANZIONI

Art. 18 – Obblighi specifici del personale

Tutto il personale che utilizza la PEO o la PEC istituzionale è tenuto a:

- utilizzare la posta istituzionale esclusivamente per finalità di servizio;
- verificare regolarmente la propria casella e rispondere tempestivamente alle comunicazioni di servizio;
- adottare comportamenti improntati alla correttezza formale e alla riservatezza;
- segnalare immediatamente al DSGA o al Dirigente Scolastico qualsiasi anomalia, incidente di sicurezza o utilizzo non autorizzato;
- attivare il messaggio automatico di risposta in caso di assenza programmata;

- non installare client di posta o applicazioni non autorizzate per l'accesso alla casella istituzionale;
- mantenere aggiornato il dispositivo MFA per l'autenticazione a due fattori;
- partecipare alle attività di formazione sulla sicurezza informatica organizzate dall'Istituto o dal MIM.

Art. 19 – Divieti specifici

Al personale è in ogni caso vietato:

- utilizzare la PEO o la PEC istituzionale per fini personali, commerciali, politici o sindacali propri;
- iscrivere la casella istituzionale a newsletter, mailing list, servizi commerciali o social media non pertinenti al servizio;
- cedere, prestare o condividere le proprie credenziali di accesso con chiunque;
- inviare catene di e-mail, messaggi satirici, meme o contenuti non pertinenti al servizio;
- utilizzare la casella istituzionale per comunicazioni che possano recare pregiudizio all'immagine, al decoro o alla reputazione dell'Istituto o dell'Amministrazione scolastica;
- trasmettere dati personali di alunni, famiglie o colleghi a soggetti non autorizzati;
- accedere alle caselle di posta di altri dipendenti, anche in caso di autorizzazione informale del titolare;
- inoltrate a caselle personali intere conversazioni o archivi di messaggi istituzionali;
- utilizzare l'indirizzo istituzionale come recapito personale su piattaforme commerciali o social media;
- effettuare registrazioni o screenshot del contenuto delle caselle altrui.

Art. 20 – Responsabilità e conseguenze disciplinari

1. La violazione delle disposizioni del presente Disciplinare costituisce inosservanza degli obblighi di servizio e può integrare illecito disciplinare ai sensi del D.Lgs. 30 marzo 2001, n. 165, del CCNL Scuola vigente, del D.P.R. n. 62/2013 e del Codice di comportamento dell'Istituto.

2. Le violazioni in materia di protezione dei dati personali possono configurare, oltre alla responsabilità disciplinare, anche responsabilità civile, penale e amministrativa, con conseguente applicazione delle sanzioni previste dal GDPR e dal D.Lgs. n. 196/2003.

3. La gravità delle violazioni e le conseguenti misure disciplinari sono valutate tenendo conto di:

- natura e gravità della violazione;
- eventuale reiterazione della condotta;
- danno arrecato all'Istituto, a terzi o ai titolari dei dati personali interessati;
- presenza di dolo o colpa grave.

4. Il Dirigente Scolastico, qualora venga a conoscenza di una violazione, avvia, ove ne ricorrano i presupposti, il procedimento disciplinare previsto dal CCNL e dalla normativa vigente.

CAPO VII – ORGANIZZAZIONE E RUOLI

Art. 21 – Responsabilità organizzative

Ruoli e responsabilità nella gestione della posta elettronica istituzionale
Dirigente Scolastico: responsabile della corretta applicazione del Disciplinare; autorizza l'accesso straordinario alla PEC da parte di soggetti diversi dal DSGA; adotta i provvedimenti disciplinari in caso di violazione; dispone la disattivazione delle caselle in caso di cessazione del rapporto.

DSGA: gestore operativo della PEO istituzionale e della PEC; assicura la consultazione giornaliera della PEC; cura la protocollazione della corrispondenza elettronica; supervisiona l'archiviazione dei messaggi; coordina le procedure di sicurezza informatica con il supporto dell'Amministratore di Sistema.

Referente per la Sicurezza Informatica / Animatore Digitale: collabora con il DSGA nella gestione tecnica delle caselle; provvede alla segnalazione di anomalie o incidenti; supporta il personale nell'utilizzo corretto degli strumenti; cura la formazione interna sulla sicurezza informatica.

RPD (Responsabile della Protezione dei Dati): vigila sul rispetto della normativa in materia di protezione dei dati personali nelle comunicazioni elettroniche; è consultato in merito ai periodi di conservazione dei metadati e alle misure di sicurezza adottate.

Personale docente e ATA: titolari delle caselle individuali; responsabili del corretto utilizzo secondo le presenti disposizioni; tenuti a segnalare tempestivamente incidenti e anomalie.

Art. 22 – Formazione e sensibilizzazione

1. Il Dirigente Scolastico promuove, nell'ambito del Piano di Formazione del personale, iniziative di sensibilizzazione e formazione in materia di:

- sicurezza informatica e prevenzione del phishing;
- corretto utilizzo degli strumenti di comunicazione istituzionale;
- obblighi in materia di protezione dei dati personali nel trattamento delle comunicazioni elettroniche.

2. Le attività formative sono organizzate almeno con cadenza annuale, anche in coordinamento con le iniziative del MIM e dell'ACN in materia di cybersicurezza per le istituzioni scolastiche.

CAPO VIII – DISPOSIZIONI FINALI

Art. 23 – Informativa ai sensi del GDPR e dello Statuto dei Lavoratori

1. Il presente Disciplinare costituisce, ai sensi dell'art. 13 del GDPR e delle Linee Guida del Garante, l'informativa al personale in merito alle modalità di utilizzo degli strumenti di posta elettronica istituzionale e alle possibilità di controllo esercitate nel rispetto dei limiti di legge.

2. Ai sensi dell'art. 4, comma 3, della L. n. 300/1970, le informazioni raccolte nell'ambito dei controlli consentiti dalla legge sono utilizzabili a tutti i fini connessi al rapporto di lavoro, nei limiti delle modalità indicate nel presente Disciplinare.

3. L'informativa completa sul trattamento dei dati personali del personale è disponibile presso la segreteria dell'Istituto e pubblicata sul sito istituzionale.

Art. 24 – Pubblicazione e comunicazione

1. Il presente Disciplinare è pubblicato sul sito istituzionale dell'Istituto nella sezione "Amministrazione Trasparente – Disposizioni generali – Atti generali" e nella sezione "Regolamenti".

2. Il Dirigente Scolastico assicura la comunicazione del Disciplinare a tutto il personale in servizio mediante circolare interna, all'inizio di ogni anno scolastico e in occasione di ogni aggiornamento significativo.

3. Il presente Disciplinare è consegnato in copia a ogni nuovo assunto all'atto della presa di servizio, unitamente all'informativa sul trattamento dei dati personali.

Art. 25 – Aggiornamento

Il presente Disciplinare è soggetto a revisione periodica, in occasione di modifiche normative rilevanti (in materia di protezione dei dati, sicurezza informatica, codice di comportamento) o di variazioni organizzative dell'Istituto. Le modifiche sono approvate dal Consiglio di Istituto.

Art. 26 – Entrata in vigore

Il presente Disciplinare entra in vigore il giorno successivo alla pubblicazione sul sito istituzionale dell'Istituto e sostituisce ogni precedente disposizione interna incompatibile in materia di utilizzo della posta elettronica.

Sant'Elia Fiumerapido, 22 giugno 2026

Il Presidente del Consiglio di Istituto

