ISTITUTO COMPRENSIVO "GUGLIELMO MARCONI" – CEGGIA (VE)

Scuola dell'Infanzia, Primaria e Secondaria di I grado

Via Folegot, 350 – 30022 Ceggia (VE) | C.F. 84003800277

POLICY GENERALE PER LA PROTEZIONE DEI DATI PERSONALI

Versione	1.0
Approvata con	Ad aggiornamento/integrazione procedura per la gestione delle violazioni dei dati personali dell'Istituto Comprensivo "G. Marconi di Ceggia" p. 5147/2023
Data di approvazione/aggiornamento	[Agosto 2026]
Data di entrata in vigore	[Agosto 2026]
Titolare del trattamento	Istituto Comprensivo "Guglielmo Marconi" di Ceggia, rappresentato dal Dirigente Scolastico pro tempore
Responsabile della Protezione dei Dati (RPD/DPO)	Avv. Andrea Camata

Art. 1 – Oggetto e finalità

La presente Policy definisce i principi generali, le responsabilità e le regole organizzative che devono essere osservati nell'ambito dell'Istituto Comprensivo "Guglielmo Marconi" di Ceggia per garantire la protezione dei dati personali trattati nello svolgimento delle attività istituzionali.

La Policy costituisce documento generale di indirizzo dell'Istituto in materia di protezione dei dati personali e sicurezza delle informazioni e deve essere letta congiuntamente alle procedure, ai regolamenti, alle informative e alle ulteriori policy specifiche adottate dall'Istituto.

L'obiettivo è assicurare che ogni trattamento di dati personali avvenga nel rispetto della normativa e dei Provvedimenti del Garante per la Protezione dei Dati Personali e, in particolare, dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.

La protezione dei dati personali costituisce parte integrante dell'attività amministrativa, organizzativa, educativa e didattica dell'Istituto.

Art. 2 – Riferimenti normativi

La presente Policy è adottata, in particolare, in conformità:

- al Regolamento (UE) 2016/679 (GDPR);
- al Decreto Legislativo 30 giugno 2003, n. 196;

- ai provvedimenti, alle linee guida e alle indicazioni del Garante per la protezione dei dati personali;
- alle indicazioni delle competenti autorità europee in materia di protezione dei dati personali;
- ai regolamenti, alle procedure e agli atti organizzativi interni dell'Istituto.

Costituiscono inoltre riferimento per l'attività dell'Istituto le indicazioni del Garante specificamente rivolte al mondo scolastico, compreso il documento "La scuola a prova di privacy".

Art. 3 – Ambito di applicazione

La presente Policy si applica a tutti i trattamenti di dati personali effettuati dall'Istituto, con strumenti cartacei, informatici, telematici, audiovisivi o mediante qualsiasi altro supporto.

Sono tenuti al rispetto della presente Policy, secondo le rispettive attribuzioni:

- il Dirigente Scolastico;
- il Direttore dei Servizi Generali e Amministrativi;
- il personale docente;
- il personale amministrativo, tecnico e ausiliario;
- i collaboratori e consulenti;
- i soggetti autorizzati al trattamento;
- gli amministratori e referenti dei sistemi informatici, nei limiti delle rispettive attribuzioni;
- ogni altro soggetto che, per ragioni istituzionali o contrattuali, sia autorizzato ad accedere a dati personali trattati dall'Istituto.

I fornitori e gli altri soggetti esterni che trattano dati personali per conto dell'Istituto sono soggetti agli obblighi derivanti dagli atti di designazione, dai contratti, dagli accordi stipulati e dalla normativa applicabile.

Art. 4 – Titolare del trattamento

Il Titolare del trattamento è l'Istituto Comprensivo "Guglielmo Marconi" di Ceggia, rappresentato dal Dirigente Scolastico pro tempore.

Al Titolare competono le decisioni relative alle finalità e ai mezzi dei trattamenti di dati personali effettuati nell'ambito delle attività istituzionali.

Il Titolare adotta misure tecniche e organizzative adeguate al fine di garantire e poter dimostrare che i trattamenti sono effettuati conformemente alla normativa vigente.

Art. 5 – Responsabile della Protezione dei Dati

L'Istituto designa il Responsabile della Protezione dei Dati – RPD/DPO ai sensi degli artt. 37 e seguenti del GDPR.

Il DPO svolge i compiti attribuitigli dalla normativa e, in particolare, informa e fornisce consulenza al Titolare e ai soggetti che effettuano i trattamenti, sorveglia l'osservanza della disciplina in materia di protezione dei dati personali, fornisce pareri nei casi previsti e coopera con il Garante per la protezione dei dati personali.

Il DPO deve essere tempestivamente coinvolto nelle questioni che riguardano la protezione dei dati personali, secondo quanto previsto dal GDPR.

Resta ferma la responsabilità decisionale e organizzativa del Titolare del trattamento.

Art. 6 – Soggetti autorizzati al trattamento

Il personale tratta i dati personali esclusivamente nell'ambito delle proprie funzioni, delle mansioni attribuite e delle istruzioni ricevute dall'Istituto.

L'accesso a dati, documenti, archivi, applicativi e piattaforme deve essere limitato a quanto effettivamente necessario per lo svolgimento delle attività assegnate.

L'eventuale possibilità tecnica di accedere a un dato non costituisce, di per sé, autorizzazione alla sua consultazione o al suo utilizzo.

Ogni soggetto autorizzato è tenuto alla riservatezza anche successivamente alla cessazione del rapporto con l'Istituto.

Art. 7 – Principio di minimizzazione

Devono essere trattati esclusivamente i dati personali adeguati, pertinenti e necessari rispetto alle finalità istituzionali perseguite.

Prima di raccogliere, comunicare, condividere, pubblicare o conservare un dato personale, il personale deve pertanto valutare se tale operazione sia effettivamente necessaria per lo svolgimento della propria attività.

Devono essere evitate raccolte generalizzate, duplicazioni non necessarie di documenti, conservazioni indiscriminate e circolazione di informazioni eccedenti rispetto alla finalità perseguita.

Particolare cautela deve essere adottata quando il trattamento riguarda minori o categorie particolari di dati personali.

Art. 8 – Dati relativi agli alunni

I dati personali degli alunni devono essere trattati esclusivamente per finalità connesse alle funzioni istituzionali dell'Istituto e nei limiti previsti dalla normativa.

Il personale deve prestare particolare attenzione nella gestione di informazioni riguardanti, a titolo esemplificativo:

- condizioni di salute;
- disabilità;
- bisogni educativi;
- situazioni familiari;
- provvedimenti giudiziari;
- condizioni di disagio personale o sociale;
- convinzioni religiose, ove rilevanti;
- immagini e registrazioni audio/video;
- valutazioni e informazioni relative al percorso scolastico;
- PEI, PDP e altra documentazione educativa o sanitaria contenente informazioni riservate.

Tali informazioni non devono essere comunicate a soggetti non legittimati a conoscerle né utilizzate per finalità estranee a quelle istituzionali.

Art. 9 – Comunicazioni contenenti dati personali

Prima di inviare una comunicazione contenente dati personali, il mittente deve verificare con particolare attenzione:

- l'identità dei destinatari;
- gli indirizzi di posta elettronica utilizzati;

- la necessità di utilizzare i campi “A”, “CC” o “CCN”;
- la presenza e il contenuto degli allegati;
- la pertinenza dei dati comunicati;
- l’eventuale presenza di dati riferiti a soggetti diversi dal destinatario.

L’invio di documentazione contenente categorie particolari di dati personali deve essere limitato ai casi necessari e deve avvenire attraverso strumenti e modalità adeguati alla natura delle informazioni trattate.

È vietato utilizzare account personali di posta elettronica per trasferire o conservare documentazione istituzionale contenente dati personali, salvo situazioni eccezionali espressamente autorizzate dall’Istituto.

Art. 10 – Account istituzionali e credenziali

Gli account messi a disposizione dall’Istituto sono strumenti destinati allo svolgimento dell’attività istituzionale.

Le credenziali sono personali e non possono essere comunicate, cedute o condivise con altre persone.

Gli utenti devono:

- custodire diligentemente le proprie credenziali;
- utilizzare password adeguatamente robuste;
- utilizzare i sistemi di autenticazione a più fattori messi a disposizione o prescritti dall’Istituto;
- bloccare il dispositivo quando si allontanano dalla postazione;
- effettuare il logout dalle postazioni condivise;
- segnalare immediatamente il sospetto accesso abusivo o la compromissione delle credenziali.

Art. 11 – Utilizzo di servizi cloud e piattaforme

I dati personali trattati per finalità istituzionali devono essere gestiti esclusivamente attraverso piattaforme, applicativi e servizi autorizzati dall’Istituto.

Il personale non può autonomamente utilizzare applicazioni, servizi cloud, piattaforme web o altri servizi digitali esterni per raccogliere, archiviare o elaborare dati personali degli alunni, delle famiglie o del personale quando tali strumenti non siano stati previamente autorizzati dall’Istituto.

Prima dell’introduzione di nuovi strumenti che comportino il trattamento di dati personali devono essere effettuate le necessarie valutazioni sotto il profilo della protezione dei dati e della sicurezza.

Art. 12 – Google Workspace e condivisione dei documenti

L’utilizzo di Google Workspace deve avvenire nel rispetto del relativo regolamento adottato dall’Istituto e delle specifiche istruzioni impartite al personale.

La condivisione di file deve essere limitata ai soggetti che abbiano effettiva necessità di accedervi.

Salvo specifica autorizzazione e adeguata valutazione, devono essere evitate condivisioni mediante collegamenti pubblicamente accessibili o utilizzabili da chiunque disponga del link.

I permessi di accesso devono essere periodicamente verificati e revocati quando viene meno la necessità della condivisione.

Particolare cautela deve essere adottata nella gestione di documenti contenenti categorie particolari di dati personali o informazioni relative a minori.

Le modalità operative di utilizzo di Workspace e Drive sono disciplinate da apposita Policy dell'Istituto.

Art. 13 – Documenti cartacei

La protezione dei dati personali riguarda anche i documenti cartacei.

Il personale deve:

- evitare di lasciare documenti riservati incustoditi;
- conservare i fascicoli negli spazi individuati dall'Istituto;
- non lasciare documenti contenenti dati personali nelle stampanti o fotocopiatrici;
- evitare l'esposizione di elenchi, prospetti o documenti a soggetti non autorizzati;
- distruggere i documenti da eliminare mediante modalità che impediscano la ricostruzione delle informazioni, ove necessario in relazione alla natura dei dati.

Art. 14 – Dispositivi informatici

Computer, notebook, tablet, smartphone e altri dispositivi utilizzati per trattare dati dell'Istituto devono essere adeguatamente protetti.

Il personale è tenuto a utilizzare le misure di sicurezza stabilite dall'Istituto e, in particolare, a prestare attenzione a:

- protezione mediante credenziali;
- blocco automatico dello schermo;
- aggiornamento dei sistemi;
- protezione da software malevolo;
- conservazione sicura dei dispositivi;
- download e conservazione locale dei documenti;
- utilizzo di supporti rimovibili;
- connessioni a reti non affidabili.

Lo smarrimento o il furto di un dispositivo utilizzato per attività istituzionali deve essere immediatamente segnalato secondo la procedura prevista per gli incidenti di sicurezza.

Art. 15 – Fotografie, video e registrazioni

Fotografie, filmati e registrazioni audio che rendano identificabili alunni, personale o altri soggetti costituiscono dati personali e devono essere trattati nel rispetto della normativa applicabile e delle disposizioni dell'Istituto.

Il personale non deve pubblicare o diffondere attraverso account, social network, sistemi di messaggistica o altri strumenti personali immagini, filmati o registrazioni realizzati nell'ambito dell'attività scolastica, salvo quanto espressamente previsto e autorizzato dall'Istituto.

Art. 16 – Applicazioni di messaggistica e social network

I servizi personali di messaggistica istantanea e i social network non devono essere utilizzati come ordinari strumenti per la trasmissione di documentazione istituzionale contenente dati personali.

Le comunicazioni istituzionali devono avvenire attraverso i canali individuati dall'Istituto.

È vietata la pubblicazione sui propri profili personali di documenti, schermate di applicativi, registri, comunicazioni interne o altre informazioni riservate acquisite nello svolgimento dell'attività lavorativa.

Art. 17 – Strumenti di intelligenza artificiale

L'utilizzo di sistemi di intelligenza artificiale nell'ambito dell'attività scolastica deve rispettare i principi di protezione dei dati personali, riservatezza, sicurezza e minimizzazione.

In particolare, salvo che l'utilizzo dello specifico servizio sia stato previamente valutato e autorizzato dall'Istituto, non devono essere inseriti nei sistemi di intelligenza artificiale generativa:

- nomi e cognomi degli alunni;
- dati delle famiglie;
- dati del personale;
- dati relativi alla salute, disabilità o bisogni educativi;
- PEI, PDP o altra documentazione individuale;
- relazioni contenenti informazioni personali;
- credenziali;
- documenti amministrativi riservati;
- fotografie, registrazioni o altri contenuti che rendano identificabile una persona.

Quando possibile, per attività consentite devono essere utilizzati dati anonimi o adeguatamente privati degli elementi identificativi.

L'utilizzo istituzionale degli strumenti di intelligenza artificiale è disciplinato da specifiche disposizioni dell'Istituto.

Art. 18 – Conservazione e cancellazione

I dati personali devono essere conservati per il periodo necessario alle finalità per le quali sono trattati e secondo i termini derivanti dalla normativa e dagli strumenti di gestione documentale e archivistica applicabili all'Istituto.

Non devono essere conservate copie ulteriori e non necessarie di documenti contenenti dati personali.

La cancellazione di file e documenti deve essere effettuata tenendo conto delle caratteristiche dello strumento utilizzato, comprese eventuali copie presenti nel cestino, nei sistemi di sincronizzazione o negli spazi condivisi.

Art. 19 – Violazioni dei dati personali e incidenti di sicurezza

Chiunque venga a conoscenza di un evento che possa comportare perdita, distruzione, alterazione, divulgazione non autorizzata o accesso non autorizzato a dati personali deve segnalarlo immediatamente, senza attendere di averne accertato personalmente la gravità.

Rientrano, a titolo esemplificativo:

- invio di una e-mail al destinatario errato;
- invio dell'allegato sbagliato;
- perdita o furto di documenti;
- perdita o furto di dispositivi;
- accesso abusivo a un account;
- compromissione delle credenziali;
- attacco informatico;
- apertura accidentale di documenti a soggetti non autorizzati;

- condivisione errata di file o cartelle;
- pubblicazione accidentale di dati;
- cancellazione o alterazione non autorizzata di dati.

La segnalazione deve essere effettuata secondo la Procedura per la gestione delle violazioni dei dati personali dell'Istituto vigente.

Il personale non deve autonomamente decidere se l'incidente costituisca o meno un data breach notificabile al Garante.

La valutazione compete al Titolare del trattamento, con il supporto del DPO e degli altri soggetti individuati dalla procedura interna.

Art. 20 – Phishing e incidenti informatici

Il personale deve prestare particolare attenzione a messaggi sospetti, richieste anomale di credenziali, allegati inattesi e collegamenti di dubbia provenienza.

In presenza di un possibile phishing o di altra compromissione informatica, l'utente deve interrompere l'attività potenzialmente pericolosa e informare tempestivamente i soggetti individuati dall'Istituto.

Qualora siano state inserite credenziali in una pagina sospetta o sia stato aperto un allegato potenzialmente malevolo, la segnalazione deve avvenire immediatamente.

Art. 21 – Privacy by design e by default

Nell'introduzione di nuovi trattamenti, piattaforme, servizi, progetti o procedure che comportino l'utilizzo di dati personali, l'Istituto tiene conto della protezione dei dati fin dalla fase di progettazione.

Devono essere privilegiate, per impostazione predefinita, soluzioni che limitino il trattamento ai dati effettivamente necessari, riducano il numero dei soggetti che possono accedervi e garantiscano un adeguato livello di sicurezza.

Il DPO viene coinvolto nei casi e secondo le modalità previste dalla normativa.

Art. 22 – Fornitori e soggetti esterni

Prima di affidare a soggetti esterni attività che comportino il trattamento di dati personali per conto dell'Istituto deve essere verificata la disciplina applicabile al rapporto e, ove ricorrano i presupposti, il soggetto deve essere designato Responsabile del trattamento ai sensi dell'art. 28 GDPR.

Il personale non è autorizzato ad affidare autonomamente dati personali dell'Istituto a soggetti esterni o a creare account istituzionali presso servizi non autorizzati.

Art. 23 – Formazione e responsabilizzazione

L'Istituto promuove periodicamente attività di informazione e formazione in materia di protezione dei dati personali e sicurezza informatica.

Il personale è tenuto a prendere visione delle policy, delle procedure e delle istruzioni adottate dall'Istituto e a partecipare alle iniziative formative previste.

Il rispetto delle misure di sicurezza e delle istruzioni impartite costituisce parte degli obblighi connessi al corretto trattamento dei dati personali.

Art. 24 – Obbligo di segnalazione

Dubbi, anomalie o situazioni potenzialmente rilevanti sotto il profilo della protezione dei dati devono essere tempestivamente portati all'attenzione dei soggetti competenti secondo l'organizzazione interna.

In particolare, devono essere segnalati:

- accessi non autorizzati;
- perdita di documenti o dispositivi;
- errori nell'invio di comunicazioni;
- condivisioni errate;
- sospetta compromissione delle credenziali;
- richieste anomale di dati personali;
- utilizzo non autorizzato di piattaforme;
- pubblicazione accidentale di informazioni;
- ogni altro evento che possa compromettere riservatezza, integrità o disponibilità dei dati.

Art. 25 – Inosservanza della Policy

La violazione delle disposizioni della presente Policy può comportare l'adozione delle misure previste dall'ordinamento, dalla disciplina del rapporto di lavoro e dai regolamenti applicabili, ferma restando ogni eventuale ulteriore responsabilità prevista dalla legge.

La valutazione delle singole condotte avviene nel rispetto delle competenze, delle procedure e delle garanzie previste dall'ordinamento.

Art. 26 – Rapporti con le policy specifiche

La presente Policy costituisce il quadro generale di riferimento.

Sono disciplinati mediante specifici documenti, tra gli altri:

1. utilizzo della posta elettronica istituzionale;
2. utilizzo di Google Workspace, Drive e sistemi di condivisione;
3. password, autenticazione e sicurezza degli account;
4. utilizzo di dispositivi informatici e dispositivi personali;
5. lavoro da remoto;
6. trattamento della documentazione relativa agli alunni;
7. fotografie, video e attività digitali;
8. utilizzo di servizi cloud e piattaforme esterne;
9. utilizzo di sistemi di intelligenza artificiale;
10. gestione degli incidenti e delle violazioni dei dati personali.

In caso di disposizioni più specifiche contenute nelle singole policy o procedure, queste ultime trovano applicazione con riferimento alla materia disciplinata.

Art. 27 – Diffusione

La presente Policy è portata a conoscenza del personale attraverso gli strumenti istituzionali individuati dall'Istituto.

L’Istituto assicura che il personale possa accedere alla versione vigente della Policy e delle procedure ad essa collegate.

Art. 28 – Aggiornamento e revisione

La Policy è sottoposta a revisione periodica e comunque quando intervengano:

- modifiche normative rilevanti;
- provvedimenti o nuove indicazioni delle autorità competenti;
- modifiche significative dell’organizzazione dell’Istituto;
- introduzione di nuovi sistemi informativi o piattaforme;
- incidenti che evidenzino la necessità di modificare le misure organizzative;
- modifiche rilevanti dei rischi connessi ai trattamenti.

Il DPO può formulare osservazioni e raccomandazioni nell’ambito dei compiti attribuitigli dal GDPR.

Art. 29 – Entrata in vigore

La presente Policy entra in vigore dalla data stabilita nel relativo atto di approvazione.

Dalla medesima data le precedenti disposizioni interne incompatibili con la presente Policy devono essere coordinate o aggiornate.

Restano vigenti, in quanto compatibili, le procedure e i regolamenti già adottati dall’Istituto, compresa la Procedura per la gestione delle violazioni dei dati personali e il Regolamento relativo all’utilizzo della piattaforma Workspace.