



Ministero dell'Istruzione e del Merito

52° Distretto Scolastico

ISTITUTO COMPRENSIVO S. LUCIA

Scuola dell'Infanzia, Primaria e Secondaria di I grado



We prepare for

Cambridge

English Qualifications

Piazza F. Baldi - Fraz. S. Lucia 84013 Cava de' Tirreni (SA)

Sito Web: www.icsantaluciacava.edu.it

e-mail: saic8b100c@istruzione.it Pec: saic8b100c@pec.istruzione.it

Tel. 089 2966809

CF 95178990651

Linea guida per il trattamento e la protezione dei dati personali

Assistenti amministrativi

(istruzioni agli autorizzati del trattamento – art. 29 del Regolamento UE 2016/679 e art. 2-quaterdecies del D.Lgs. 196/2003)

1. Premessa

La presente linea guida descrive le misure operative che l'assistente amministrativo deve osservare per la sicurezza e la correttezza del trattamento dei dati personali, in aggiunta alle istruzioni operative generali dell'istituzione. Costituisce trattamento qualunque operazione svolta su dati personali, con o senza strumenti informatici.

2. Raccolta e registrazione dei dati

- Raccogliere e registrare solo i dati necessari alle attività della segreteria e per finalità determinate e legittime.
- Consegnare o rendere disponibile l'informativa (artt. 13-14 GDPR) all'interessato prima o al momento della raccolta, utilizzando i modelli dell'istituzione, verificare la presenza del consenso quando il trattamento lo richiede.

3. Accesso, conservazione e scambio di documenti

- Accedere ai soli fascicoli e archivi di competenza; conservare i documenti in cartelline non trasparenti e in armadi dotati di serratura.
- Non lasciare incustoditi elenchi con recapiti di alunni, famiglie e personale; non trascriverne il contenuto su fogli di lavoro.
- Al ricevimento e alla consegna allo sportello, accertare l'identità dell'interessato e, in caso di ritiro da parte di terzi, l'esistenza di delega scritta; consegnare la documentazione in busta chiusa non trasparente.
- Presidiare stampanti, fotocopiatrici e scanner: ritirare subito le copie e non lasciare documenti con dati personali a disposizione di estranei.
- Distruggere con trita-documenti le copie e le bozze non più necessarie; non gettare documenti con dati personali nella carta comune.

4. Comunicazioni telefoniche, e-mail e PEC

- Non fornire dati per telefono o fax senza certezza dell'identità e della legittimazione del richiedente; in caso di richieste dell'Autorità giudiziaria o della polizia giudiziaria, richiamare il numero istituzionale del richiedente per verificarne l'identità.

- Utilizzare le caselle istituzionali (PEO/PEC); controllare gli indirizzi dei destinatari prima dell'invio di messaggi con dati personali; per invii a più destinatari esterni usare il campo copia nascosta.
- Non aprire allegati o link di provenienza incerta; segnalare le e-mail sospette al referente per la sicurezza informatica senza inoltrarle.

5. Portali e sistemi gestionali

- Accedere ai portali e ai gestionali (registro elettronico lato segreteria, sistemi del Ministero, NoiPA, INPS, piattaforme di e-procurement, protocollo informatico) esclusivamente con le proprie credenziali e per le pratiche assegnate.
- Non condividere le credenziali; bloccare la sessione quando ci si allontana; effettuare il logout a fine attività.
- Trattare le istanze di accesso documentale, accesso civico e accesso generalizzato secondo le procedure dell'istituzione, valutando la presenza di controinteressati e i limiti a tutela dei dati personali.

6. Misure di sicurezza informatica

- Scegliere password robuste e non intuibili, custodirle e modificarle con la periodicità stabilita; non riutilizzare le credenziali di lavoro su servizi personali o esterni.
- Non installare software non autorizzato; salvare i file solo nelle cartelle e nei sistemi indicati dall'istituzione; non usare dispositivi o cloud personali per dati dell'istituzione.
- Utilizzare supporti rimovibili solo se autorizzati e cifrati; cancellare in modo sicuro i dati prima della dismissione.

7. Uso di strumenti di intelligenza artificiale

- Non utilizzare strumenti di IA non autorizzati per attività che comportino il trattamento di dati personali o di documenti riservati.
- Non inserire in chatbot o servizi di IA generici dati di alunni, famiglie o personale; se uno strumento è autorizzato, pseudonimizzare o anonimizzare i dati prima dell'inserimento e verificare sempre gli output.

8. Gestione degli incidenti

Segnalare senza ritardo al referente privacy / al Dirigente Scolastico e al RPD ogni perdita, furto, accesso non autorizzato, invio errato o sospetta violazione di dati personali, per consentire la valutazione e l'eventuale notifica al Garante entro 72 ore (artt. 33-34 GDPR).

9. Obblighi permanenti

Gli obblighi di riservatezza e di corretto trattamento permangono anche dopo il cambio di incarico e la cessazione del rapporto di servizio. La violazione può comportare responsabilità disciplinare, civile e penale.

Il Titolare

Il Dirigente Scolastico

Prof.^{ssa} Gabriella LIBERTI

*documento firmato digitalmente ai sensi del c.d.
Codice dell'Amministrazione Digitale e normativa connessa*

Il/La sottoscritto/a dichiara di aver preso visione.

COGNOME	NOME	RUOLO

Data: _____

Firma : _____

