



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 PERSONALE DOCENTE

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

1. Premessa

Le presenti linee guida descrivono le misure operative che il docente deve adottare per garantire la sicurezza e la correttezza del trattamento dei dati personali degli alunni e delle famiglie, in aggiunta alle istruzioni operative generali dell'istituzione. Trattamento è qualunque operazione compiuta su dati personali, con o senza strumenti informatici.

2. Principi e regole generali

- Accedere ai soli dati necessari all'esercizio della funzione docente e trattarli in modo lecito, corretto e trasparente.
- Raccogliere e registrare i dati solo per finalità didattiche, educative e di valutazione; non richiedere dati eccedenti.
- Verificare l'esattezza dei dati e aggiornarli quando necessario; conservarli per il tempo strettamente necessario.
- Non comunicare a terzi, fuori dall'ambito lavorativo o in difformità dalle istruzioni, alcun dato personale di alunni o famiglie.

3. Registro elettronico e strumenti digitali

- Accedere al registro elettronico e alle piattaforme con le proprie credenziali personali; non condividerle; effettuare il logout e non lasciare la sessione aperta su postazioni condivise o alla LIM.
- Inserire nel registro solo le annotazioni pertinenti alla didattica e alla valutazione; evitare giudizi o annotazioni non necessari e riferimenti a dati sulla salute o alla vita privata non indispensabili.
- Utilizzare esclusivamente le piattaforme e le applicazioni didattiche approvate dall'istituzione, per le quali è stato definito il rapporto con il fornitore ai sensi dell'art. 28 GDPR; non attivare autonomamente nuovi servizi o app che trattino dati degli alunni.

4. Alunni con BES, DSA e disabilità

- Trattare PEI, PDP, certificazioni e relazioni cliniche con particolare riservatezza; consultarli e condividerli solo tra i docenti del consiglio di classe e i soggetti autorizzati.
- Custodire i documenti in luogo sicuro; non lasciarli incustoditi in aula o in sala docenti; non inviarli su canali non istituzionali.

5. Comunicazioni con le famiglie

- Utilizzare i canali istituzionali (registro elettronico, e-mail dell'istituto, colloqui); non usare gruppi o chat personali (ad esempio WhatsApp) per trasmettere dati personali o valutazioni.
- Nelle comunicazioni a più destinatari non rendere visibili gli indirizzi altrui.

6. Foto, video e riprese

- Effettuare riprese o fotografie di alunni solo nell'ambito di attività autorizzate dall'istituzione e in presenza delle liberatorie raccolte.
- Non pubblicare né diffondere immagini o video di alunni su profili o canali personali; il materiale va gestito solo tramite i canali istituzionali.

7. Uso di strumenti di intelligenza artificiale

- Il personale è tenuto a mantenere una competenza adeguata all'uso degli strumenti di IA (alfabetizzazione, art. 4 del Regolamento UE 2024/1689) secondo la formazione organizzata dall'istituzione.
- Utilizzare solo gli strumenti di IA autorizzati dall'istituzione; non inserire in chatbot o servizi di IA generici dati personali di alunni o famiglie; ove l'uso sia consentito, pseudonimizzare o anonimizzare i dati e verificare sempre gli output.
- Non utilizzare l'IA per assumere valutazioni o decisioni sugli studenti senza supervisione umana; sono in ogni caso vietati i sistemi di riconoscimento delle emozioni in ambito educativo (art. 5 del Regolamento UE 2024/1689).

8. Misure di sicurezza sulla postazione

- Scegliere password robuste e non intuibili, custodirle e non comunicarle; bloccare la sessione e spegnere la postazione a fine attività.
- Non aprire allegati o link di provenienza incerta; segnalare le e-mail sospette al referente per la sicurezza informatica senza inoltrarle, indicando data, ora, oggetto e mittente apparente.
- Non salvare dati personali degli alunni su dispositivi o servizi cloud personali; usare gli strumenti e gli spazi indicati dall'istituzione.
- Al termine delle attività giornaliere consegnare il registro di classe cartaceo, ove in uso, al personale incaricato della custodia.

9. 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).

10. Obblighi permanenti

Gli obblighi di riservatezza e di corretto trattamento permangono anche dopo il termine dell'incarico e la cessazione del rapporto di servizio. La violazione può comportare responsabilità disciplinare, civile e penale. Per quanto non previsto si rinvia al Regolamento UE 2016/679, al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 e alle policy dell'istituzione.

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 : _____