



Cambridge International School

COESIONE
ITALIA 21-27



SCUOLA ASSOCIATI



FUTURA
LA SCUOLA
PER L'ITALIA DI DOMANI



VADEMECUM



Gestione dei Dati Sensibili e Categorie Particolari

Il trattamento di dati relativi alla **salute** (certificazioni DSA, BES, disabilità, allergie), alle **condizioni familiari** (situazioni di disagio, affidamento) e alle **convinzioni religiose** richiede massima cautela.

- **Minimizzazione:** La scuola deve raccogliere solo i dati strettamente necessari per l'attività didattica o amministrativa. Questi dati devono essere trattati solo da personale autorizzato e conservati con misure tecniche e organizzative adeguate.
- **Voti e Scrutini:** I voti delle interrogazioni e dei compiti in classe devono essere comunicati individualmente con il Registro elettronico che prevede credenziali personali e tracciabilità degli accessi. I tabelloni degli scrutini finali possono essere pubblicati solo se previsto dalle norme ministeriali, evitando comunque riferimenti a dati sanitari (es. non deve apparire il motivo di un esonero dalle prove).
- **Disabilità, DSA e BES:** Le diagnosi e i Piani Didattici Personalizzati (PDP) o Piani Educativi Individualizzati (PEI) devono essere accessibili **solo** ai docenti della classe, al personale amministrativo dedicato e alla famiglia.
- **Assenze e Motivazioni Sanitarie:** Il registro elettronico deve riportare solo l'assenza. La motivazione clinica specifica (es. "visita oncologica") deve essere gestita esclusivamente tramite canali riservati (segreteria) e non deve essere visibile nell'area comune del registro o ai docenti non direttamente interessati.

- **Patologie - Accesso Selettivo:** La documentazione medica (certificati, diagnosi cliniche) deve essere conservata in **faldoni chiusi** o **archivi digitali**. Solo il Dirigente Scolastico e il personale amministrativo autorizzato possono accedere al fascicolo completo.
- **Comunicazione ai Docenti:** I professori del Consiglio di Classe devono essere informati solo delle **ricadute didattiche** della patologia (es. "lo studente necessita di pause frequenti" o "non può svolgere attività fisica intensa") e non necessariamente della diagnosi clinica esatta, a meno che non sia indispensabile per la sicurezza dello studente.

Gestione delle Emergenze Sanitarie



Protocolli di Somministrazione Farmaci: Per gli studenti che soffrono di patologie croniche (es. diabete, epilessia, asma grave) e che richiedono farmaci salvavita, la scuola predispone un protocollo riservato. Solo il personale formato deve conoscere le modalità di intervento.

- **Piani di Emergenza:** La condizione di salute può essere indicata nel piano di evacuazione, ma l'informazione deve essere gestita in modo da non essere visibile a persone estranee o compagni di classe (es. codici interni).

Gestione delle Assenze per Terapie e richiesta DDI /DAD



- **Giustificazioni:** Se lo studente deve assentarsi periodicamente per terapie o ospedalizzazioni, la famiglia può presentare una certificazione cumulativa.
- **Registro Elettronico:** Sul registro deve apparire esclusivamente la dicitura "Assente". Eventuali dettagli sulle motivazioni sanitarie non devono mai essere inseriti nelle "Note" visibili ad altri genitori o studenti.
- **Richiesta Didattica Digitale integrata DDI/ Didattica a Distanza DAD:** Dietro richiesta genitoriale, è possibile attivare la DDI/DAD compilando, a cura dell'intero corpo genitori della classe, un modello di consenso informato.



Obbligo di Attivazione in caso di Violazione

Se un dato sanitario viene diffuso indebitamente (es. un docente menziona la patologia di un alunno davanti alla classe o un dato sensibile appare sul sito web):

1. **Segnalazione Immediata:** Chiunque rilevi la violazione deve avvisare il **DPO (Responsabile Protezione Dati)** della scuola.



COESIONE
ITALIA 21-27



FUTURA
LA SCUOLA
PER L'ITALIA DI DOMANI



2. **Notifica al Garante:** Se la violazione comporta un rischio per i diritti dello studente, il Dirigente deve notificare il Garante della Privacy entro 72 ore (procedura di *Data Breach*).
3. **Misure Correttive:** La scuola deve rimuovere immediatamente l'informazione e informare la famiglia dell'accaduto e delle misure prese per rimediare.

Vita digitale degli studenti: Rischi Emergenti e Nuove Frontiere



La digitalizzazione avanzata ha introdotto nuovi pericoli:

- **Deepfake e IA Generativa:** Il rischio principale riguarda la creazione di immagini o video falsificati (anche a carattere sessuale) tramite intelligenza artificiale. La scuola informa che la creazione o diffusione di tali contenuti è un reato grave.
- **Profilazione e Algoritmi:** Gli studenti devono essere consapevoli che ogni "like", ricerca o interazione contribuisce a creare un profilo commerciale e sociale che potrebbe influenzare il loro futuro (es. ammissioni universitarie o selezioni lavorative).
- **Sexting e Revenge Porn:** La condivisione di immagini intime, anche se consensuale all'inizio, espone al rischio di ricatti e diffusione non controllata.
- **Cyberbullismo:** Sono previste sanzioni civili, penali e disciplinari nei casi accertati di insulti, minacce, esclusioni mirate, diffusione di materiale denigratorio.

Consapevolezza: La "Reputazione Digitale"



- **Diritto all'Oblio:** Sebbene esistano procedure per richiedere la rimozione di dati, ciò che finisce in rete è difficile da cancellare totalmente. Gli studenti devono imparare a valutare l'opportunità di pubblicare contenuti prima di farlo.
- **Gestione delle Credenziali:** La consapevolezza passa anche dalla sicurezza tecnica: uso di password robuste, autenticazione a due fattori e protezione degli accessi al registro elettronico e alle piattaforme didattiche.

Uso Etico dei Dispositivi in Classe



- **Finalità Didattica:** L'uso di smartphone e tablet è un diritto-dovere solo se finalizzato all'apprendimento. Registrare un docente o un compagno "per scherzo" senza consenso costituisce una violazione della privacy passibile di sospensione e, nei casi gravi, di denuncia.
- **Rispetto del Silenzio Digitale:** Durante le verifiche e le attività critiche, il diritto alla privacy dei dati scolastici impone la limitazione dell'uso di strumenti di registrazione.
- **Pubblicazioni online:** Foto o video di studenti su siti web o social della scuola richiedono un consenso esplicito e informato dai genitori (o dallo studente se maggiorenne).

Uso Corretto di Chat e Gruppi (WhatsApp, FACEBOOK, INSTAGRAM)



- **Finalità:** I gruppi di classe devono servire esclusivamente per scopi organizzativi e didattici.
- **Rispetto della Privacy:** È vietato condividere nelle chat audio, foto di compagni o screenshot di conversazioni private senza autorizzazione.
- **Non si devono usare le chat per offese, denigrazioni o pressioni verso i docenti, compagni o famiglie.**
- **Diritto alla disconnessione:** Docenti e studenti hanno il diritto di non rispondere a comunicazioni fuori dall'orario scolastico per preservare il benessere digitale.
- Le chat **non sono strumenti istituzionali** della scuola.
- Ciascun membro del gruppo è **responsabile** del proprio comportamento e del rispetto della normativa sulla protezione dei dati.

Ruolo del Registro Elettronico



Il registro è uno strumento istituzionale che sostituisce integralmente i documenti cartacei.

- **Accesso riservato:** Le credenziali sono personali. I genitori devono visionare solo il profilo del proprio figlio.



COESIONE
ITALIA 21-27



FUTURA
LA SCUOLA
PER L'ITALIA DI DOMANI



- **Trasparenza:** Le note disciplinari e le assenze devono essere inserite tempestivamente per garantire il monitoraggio della famiglia, ma con un linguaggio che rispetti la dignità dello studente.
- **Sicurezza:** La scuola è tenuta a garantire la protezione dei dati nel registro contro accessi non autorizzati o perdite accidentali.
- **Gestione:** E' possibile scaricare comunicazioni ufficiali, circolari e avvisi.

Shareting: condivisione da parte dei genitori di foto, video e informazioni dei figli sui social



- La scuola, con figure esperte esterne, può dedicare momenti di incontro/formazione sul tema dei rischi dello shareting, precisando che ogni contenuto pubblicato contribuisce a determinare l'identità digitale del minore e che può essere riutilizzato in contesti distorti o lesivi.

Responsabilità Condivisa



- **La Scuola:** È il "Titolare del trattamento", designa un Responsabile della Protezione dei Dati (DPO) e forma il personale su come gestire i dati degli studenti.
- **La Famiglia:** Deve collaborare nell'educazione al digitale e vigilare sull'uso dei dispositivi personali. È civilmente responsabile dei danni causati dai figli.
- **Lo Studente:** È chiamato a un uso etico della tecnologia. Nel 2026, la consapevolezza che "il digitale è reale" è parte integrante della valutazione del comportamento.
- **Formazione:** E' prerogativa della scuola garantire una cultura condivisa della privacy e dell'uso responsabile delle tecnologie attraverso una formazione continua che coinvolga personale scolastico, famiglie e studenti.

Codice Min.: **CEPM03000D**
Codice fiscale: C.F. e P.I. 93034560610
Codice univoco di fatturazione: UF71YN

P.zza Umberto I – 81043 CAPUA CE
Email: **cepm03000d@istruzione.it**
Email PEC: **cepm03000d@pec.istruzione.it**

Tel: **0823/961077**
Fax: **0823/625640**
www.liceopizzi.edu.it