



ISTITUTO COMPRENSIVO STATALE

"B. ZUMBINI"

Scuola dell'Infanzia, Scuola Primaria, Scuola Secondaria di I Grado con indirizzo Musicale

Via Misasi – 87100 Cosenza
Tel. 0984 21859

Cod. Meccanografico CSIC89700C
Cod. Fiscale 98094140781
Cod. Fatturazione Elettronica UFUQUG

e-mail: csic89700c@istruzione.it
PEC: csic89700c@pec.istruzione.it

**Al personale docente e Ata
Ai genitori
All'Albo\Al Sito**

DIRETTIVA SULLE NORME PER LA SICUREZZA DEI DATI E LA TUTELA DELLA PRIVACY I.C.B.ZUMBINI

(Ai sensi del Regolamento UE 2016/679 - GDPR, del D.Lgs. 196/2003 e ss.mm.ii., del D.Lgs. 82/2005 - CAD, della L. 241/1990 e del Codice di Comportamento dei dipendenti pubblici)

1. QUADRO GENERALE E PRINCIPI FONDAMENTALI DEL TRATTAMENTO

In vista dell'avvio dell'anno scolastico 2026/2027, si rende necessario richiamare l'attenzione di tutto il personale in servizio nell'I.C.B.Zumbini sul rispetto rigoroso delle norme in materia di protezione dei dati personali e sicurezza informatica. Nel contesto della Transizione Digitale e dell'adozione consolidata dei sistemi di Didattica Digitale Integrata e dell'Agenda Digitale d'Istituto, la tutela dei dati personali — in particolare riferiti a soggetti minorenni — costituisce un primario dovere d'ufficio e un preciso obbligo di legge.

• **Base Giuridica e Interesse Pubblico Rilevante:** Le istituzioni scolastiche svolgono compiti di rilevante interesse pubblico. Ai sensi dell'art. 2-sexies del Codice Privacy (D.Lgs.196/2003 e ss.mm.ii.), la base giuridica del trattamento per finalità formative, didattiche e gestione della carriera scolastica è rappresentata dall'esercizio di pubblici poteri e dalle funzioni istituzionali. Pertanto, **non occorre il consenso espresso** di studenti e famiglie per i trattamenti ordinari legati alla gestione scolastica, agli esiti degli apprendimenti e alla valutazione.

• **Principi di Minimizzazione e Cautela:** In conformità all'art. 5 del GDPR, i dati trattati devono essere adeguati, pertinenti e limitati a quanto necessario (*minimizzazione dei dati*).

Non possono essere richiesti dati non strettamente rilevanti per le finalità istituzionali. Massima cautela deve essere adottata per le categorie particolari di dati personali (ex art. 9 GDPR: dati relativi alla salute, disabilità, DSA, convinzioni religiose) o giudiziari.

• **Dati Sensibili e Inclusione:** La conoscenza dei dati riguardanti studenti con disabilità (L. 104/1992, D.Lgs. 66/2017) o con disturbi specifici dell'apprendimento (L. 170/2010) è strettamente riservata ai soli soggetti direttamente coinvolti nei processi educativi, inclusivi e sanitari (docenti del consiglio di classe, genitori e operatori sanitari della rete multidisciplinare per la redazione di PEI e PDP).

2. SOGGETTI COINVOLTI NEL TRATTAMENTO DEI DATI E ARTICOLAZIONE DEI RUOLI

Titolare del Trattamento:

• Il **Dirigente Scolastico**, pro tempore, rappresenta il Titolare del trattamento. Spetta al DS determinare finalità, mezzi e garanzie di sicurezza dei trattamenti, coordinare la tenuta del Registro dei Trattamenti, aggiornare le informative, valutare l'impatto privacy (DPIA) sui processi e autorizzare formalmente il personale al trattamento dei dati.

Designati, Autorizzati e Responsabili del Trattamento:

• **Docenti:** Ricevono formale autorizzazione cumulativa/individuale dal Dirigente Scolastico al trattamento dei dati degli alunni e delle famiglie, per i soli scopi connessi alla funzione docente e alla gestione delle attività didattiche.

• **DSGA e Personale ATA:** Il DSGA è designato quale referente/responsabile per l'organizzazione delle operazioni di trattamento relative ai servizi amministrativo-contabili e gestisce il personale ATA formalmente autorizzato ed incaricato.

• **Fornitori Esterni (Responsabili del Trattamento ex art. 28 GDPR):** Qualsiasi soggetto esterno o fornitore di servizi software/digitali che tratti dati per conto della scuola deve essere formalmente nominato *Responsabile Esterno*

del Trattamento mediante contratto vincolante.

o **Piattaforme Nazionali (SIDI, UNICA, INVALSI):** Quando la scuola utilizza applicativi e portali ministeriali (SIDI, Piattaforma UNICA per le iscrizioni e la carriera, prove INVALSI), il Ministero dell'Istruzione e del Merito (MIM) o l'Ente nazionale agisce quale Responsabile Esterno del Trattamento per conto dell'Istituto.

o **Pacchetti e Software di Registro Locale:** I fornitori privati dei pacchetti informatici gestionali o dei registri elettronici locali assumono il ruolo di Responsabili Esterni del Trattamento.

Responsabile della Protezione dei Dati (RPD / DPO):

• Figura di consulenza e vigilanza indipendente, nominata dall'Istituto ai sensi degli artt. 37-39 del GDPR. Supporta la dirigenza nella conformità normativa, svolge attività di formazione al personale e funge da punto di contatto per il Garante e gli interessati.

3. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO ED ACCESSO AGLI ATTI

• **Registro dei Trattamenti (Art. 30 GDPR):** L'Istituto è tenuto a redigere, aggiornare costantemente e conservare in formato elettronico il Registro delle attività di trattamento (articolato nei processi di *Gestione Iscrizioni*, *Gestione Carriera Scolastica Alunni*, *Gestione Contrattualizzazione e Carriera del Personale docente e ATA*). Il Registro riporta le finalità, le basi giuridiche, i soggetti destinatari, i termini di conservazione e le misure di sicurezza adottate, rimanendo a disposizione del Garante Privacy.

• **Accesso ai Dati e Accesso agli Atti (L. 241/1990):** Per rettifiche o informazioni sui propri dati personali, gli interessati (genitori, studenti maggiorenni, personale) possono rivolgersi direttamente al Titolare. Per le richieste di accesso ai documenti amministrativi ai sensi della L. 241/1990, la scuola valuterà la sussistenza di un interesse diretto, concreto e attuale del richiedente, contemperando il diritto di accesso con la tutela della riservatezza dei terzi.

4. REGOLAMENTAZIONE PER FOTOGRAFIE, RIPRESE E SISTEMI DI VIDEOSORVEGLIANZA

• **Uso di Immagini e Video per Fini Didattici:** La ripresa di foto o filmati nell'ambito di progetti scolastici, open day, recite o eventi istituzionali è lecita se finalizzata alla soladocumentazione didattica interna, nel rispetto del principio di proporzionalità (privilegiando riprese di gruppo e atteggiamenti costruttivi, evitando primi piani o contesti svalutativi).

• **Consenso per la Diffusione Online:** Qualora la pubblicazione o diffusione delle immagini debba avvenire su canali pubblici esterni (sito web dell'Istituto, social media della scuola, brochure), è **tassativamente obbligatoria l'acquisizione del consenso scritto ed esplicito** dei genitori/tutori (o dello studente se maggiorenne). È fatto divieto assoluto al personale di pubblicare immagini di alunni sui propri profili social personali.

• **Impianti di Videosorveglianza:** L'installazione di telecamere negli spazi scolastici è ammessa esclusivamente per la tutela dell'edificio e del patrimonio contro atti vandalici o furti, limitatamente al perimetro esterno e alle aree vulnerabili. Le telecamere devono essere segnalate da appositi cartelli e devono rimanere disattivate durante l'orario di svolgimento delle attività scolastiche ed extrascolastiche.

5. GESTIONE DEL RISCHIO DI DATA BREACH (VIOLAZIONE DEI DATI) ED ACCOUNTABILITY

In attuazione del principio di *Accountability* (responsabilizzazione ex art. 24 e 25 GDPR) e dei criteri di *Data Protection by Design and by Default*, l'Istituto applica misure tecniche e organizzative preventive per valutare e mitigare i rischi di violazione informatica, smarrimento o diffusione accidentale dei dati.

• **Definizione di Data Breach:** Costituisce violazione dei dati personali qualsiasi evento accidentale o illecito che comporti la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali conservati o trasmessi (es. smarrimento di pendrive, attacco malware/hacker, invio accidentale di e-mail a destinatari errati con dati sensibili).

• **Obblighi del Titolare in caso di Violazione:**

1. **Notifica al Garante Privacy:** Qualora la violazione presenti un rischio per i diritti e libertà degli interessati, il Titolare deve notificare l'evento all'Autorità Garante **entro 72 ore** dall'avvenuta conoscenza.

2. **Comunicazione agli Interessati:** Se il rischio per gli interessati appare elevato, il Titolare deve informare tempestivamente anche le persone coinvolte.

3. **Registro interno dei Data Breach:** Tutte le violazioni, comprese quelle non soggette a notifica esterna, devono essere formalmente documentate in un registro interno indicandone cause, conseguenze e azioni correttive intraprese.

6. PROCEDURE D'URGENZA PER IL PERSONALE IN CASO DI SMARRIMENTO DISPOSITIVI O ANOMALIE

Ciascun dipendente scolastico è tenuto all'adozione di un comportamento vigile e custode dei dati gestiti.

• **In caso di furto o smarrimento di dispositivi contenenti dati scolastici:** Se un dipendente smarrisce o subisce il furto di supporti informatici (chiavette USB, hard disk esterni, tablet, PC portatili) contenenti dati personali o sensibili di alunni o del personale, è **tenuto a dare immediata comunicazione scritta al Dirigente Scolastico**, specificando la natura dei dati ed i soggetti coinvolti. Contestualmente, il dipendente deve sporgere immediata denuncia alle Autorità di Pubblica Sicurezza (Carabinieri/Polizia di Stato) e fornirne copia alla Segreteria dell'Istituto.

• **In caso di Hackeraggio o Malware:** Nel caso si riscontrino intrusioni informatiche, accessi non autorizzati alla propria casella mail istituzionale, attacchi phishing o anomalie sui device scolastici in uso, occorre darne segnalazione

tempestiva al DSGA, al DS e all'animatore digitale/team per l'innovazione per l'attivazione immediata delle procedure di blocco e messa in sicurezza.

7. ADEMPIMENTI E MODULISTICA PER L'A.S. 2026/2027

Tutto il personale in servizio per l'a.s. 2026/2027 è tenuto a prender visione della presente direttiva e della documentazione allegata.

- **Modulistica:** Entro e non oltre il termine di avvio delle lezioni, tutto il personale è tenuto a sottoscrivere tramite Registro Elettronico (RE) la presa visione dell'atto di autorizzazione/designazione e delle relative istruzioni operative per il trattamento dei dati. Si rammenta che la mancata apposizione della firma digitale/spunta di lettura non esime dall'osservanza delle disposizioni, né ostacola il perfezionamento dell'avvenuta notificalegale, né costituisce difetto di notifica dell'atto pubblicato. Si rammenta che la notifica è avvenuta nel collegio dei docenti del 03-09-2026
- **Consultazione e Formazione:** Si invitano i docenti e il personale ATA a consultare il materiale formativo e i vademecum resi disponibili dall'Autorità Garante e dal Ministero per la sicurezza in rete:

1. Garante Privacy - Sezione Scuola e Privacy: <https://www.garanteprivacy.it/temi/scuola>;
2. Progetto "Io non cado nella rete": <https://iononcadonellarete.it/web/site#!il-progetto>

Il mancato rispetto delle disposizioni e delle misure di sicurezza previste dalla presente direttiva costituisce inosservanza dei doveri d'ufficio e fonte di responsabilità disciplinare e amministrativa.

La presente direttiva e la relativa regolamentazione **s'intendono valide ed efficaci a partire dalla data di pubblicazione e conservano la propria validità per gli anni scolastici successivi**, fino all'eventuale adozione di nuove disposizioni o modifiche formali da parte del Dirigente Scolastico o in presenza di nuovi interventi normativi.

Il Dirigente
Marietta Iusi
F.to digitalmente