



ISTITUTO COMPRENSIVO "GIUSEPPE MAZZINI"- ERICE – TRENTAPIEDI

Via Cesarò, 19 – 91016 Erice (TP) ☎ 0923 826198 –

Cod. Mecc: TPIC831001 - C.F. 80003780816 - www.mazzinierice.edu.it

email: tpic831001@istruzione.it - PEC: tpic831001@pec.istruzione.it

**Circolare n. 44
Prot. n. 10454 /I.4**

Erice, 5/10/2026

A tutto il personale scolastico
Ai genitori
Agli alunni
Al DSGA
Al sito web e registro elettronico

**Oggetto: procedura per la segnalazione e la gestione delle violazioni di dati personali
(data breach)**

Si rende noto alle SS.LL. quanto stabilito dal Regolamento (UE) 2016/679 (GDPR) in materia di sicurezza e protezione dei dati personali e, in particolare, in relazione agli adempimenti da porre in essere in caso di violazione dei dati personali (*data breach*).

Il Regolamento prevede che il titolare del trattamento — l'Istituzione scolastica, rappresentata dal Dirigente Scolastico — adotti misure tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato al rischio. Tra tali misure rientrano anche procedure idonee a consentire la tempestiva individuazione, gestione e segnalazione di eventuali violazioni dei dati personali.

Con la presente circolare si forniscono, pertanto, le indicazioni operative da seguire qualora si verifichi o venga rilevata una possibile violazione dei dati personali.

Che cosa è una violazione di dati personali (data breach)

L'art. 4, punto 12, del GDPR definisce il *data breach* come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

A titolo esemplificativo, possono costituire una violazione dei dati personali:

- la sottrazione o la copia non autorizzata di documenti cartacei o informatici contenenti dati personali;
- la perdita o il furto di una pen drive, di un notebook o di altro dispositivo contenente dati personali;
- l'impossibilità di accedere ai dati a causa di eventi accidentali, virus o attacchi informatici;
- la cifratura di dati o documenti da parte di un *ransomware* o la loro conseguente inaccessibilità;
- la perdita o la distruzione di dati a seguito di incidenti, incendi o calamità;
- la divulgazione non autorizzata di dati personali;
- l'invio di un'e-mail a più destinatari utilizzando i campi "A" o "Cc", rendendo visibili a ciascun destinatario gli indirizzi degli altri.

Adempimenti del personale scolastico in caso di violazione

La tempestività della segnalazione è essenziale per consentire all'Istituzione scolastica di intervenire e limitare le possibili conseguenze della violazione.

Il personale che rilevi o venga a conoscenza di una possibile violazione dei dati personali è tenuto a darne **immediata comunicazione al Dirigente Scolastico** o, in caso di sua temporanea indisponibilità, al Responsabile della protezione dei dati (RPD/DPO) o alle altre figure incaricate della gestione dei sistemi informatici e dell'assistenza normativa, al fine di consentire l'adozione tempestiva delle misure necessarie.

La mancata segnalazione di una violazione di cui si sia venuti a conoscenza può comportare l'adozione di provvedimenti disciplinari. La diffusione o l'utilizzo improprio, da parte di chiunque, di dati acquisiti a seguito di una violazione può, inoltre, comportare conseguenze di natura civile e penale.

Indicazioni per genitori e alunni

Anche gli alunni e i genitori possono venire a conoscenza di una violazione dei dati personali, ad esempio rinvenendo documenti lasciati incustoditi oppure ricevendo, per errore, comunicazioni via e-mail o tramite piattaforme digitali non destinate a loro.

In tali casi, è necessario darne **immediata comunicazione al Dirigente Scolastico** o, in subordine, al RPD/DPO, preferibilmente mediante una prima segnalazione telefonica durante l'orario di servizio della segreteria e, comunque, tramite e-mail ai recapiti di seguito indicati.

La tempestività della segnalazione consente all'Istituzione scolastica di intervenire prontamente al fine di interrompere la violazione o limitarne le conseguenze. La diffusione o l'utilizzo improprio di dati acquisiti a seguito di una violazione può comportare conseguenze di natura civile e penale.

A chi segnalare la violazione

Di seguito i riferimenti da utilizzare per le segnalazioni:

Istituzione scolastica — e-mail: tpic831001@istruzione.it - tel.: **0923826198**

Responsabile della protezione dei dati (RPD/DPO) — Vargiu Scuola Srl, referente Ing. Antonio Vargiu — e-mail: dpo@vargiuscuola.it tel.: 070271526

Adempimenti dell'Amministrazione a seguito della segnalazione

Ricevuta la segnalazione, il Dirigente Scolastico, con il supporto del RPD/DPO e delle eventuali figure tecniche coinvolte, adotta le misure necessarie per contenere la violazione, procede a una prima analisi dell'accaduto e ne valuta la gravità, individuando i possibili rischi per gli interessati e le conseguenti misure da adottare.

Sulla base di tale valutazione, il titolare del trattamento decide se procedere alla notifica della violazione al Garante per la protezione dei dati personali — **entro 72 ore** dal momento in cui ne è venuto a conoscenza, salvo che l'eventuale ritardo sia adeguatamente motivato — e se darne comunicazione agli interessati nei casi in cui la violazione possa comportare un rischio elevato per i loro diritti e le loro libertà.

Il RPD/DPO fornisce il proprio supporto e parere; la decisione finale compete al titolare del trattamento, in applicazione del principio di responsabilizzazione (*accountability*).

Ogni violazione dei dati personali, indipendentemente dal fatto che sia stata o meno notificata al Garante, deve essere documentata nell'apposito registro delle violazioni.

La notifica al Garante, ove dovuta, è effettuata mediante l'apposita procedura telematica disponibile sul portale del Garante per la protezione dei dati personali.

Il Dirigente Scolastico
Dott.ssa Anna Maria Di Marzo



Firmato digitalmente da:
Di Marzo Anna Maria
Firmato il 05/10/2026 14:56
Seriale Certificato: 4121258
Valido dal 30/12/2024 al 30/12/2027
InfoCamere Qualified Electronic Signature CA