ISTITUTO COMPRENSIVO
ISOLA G.S. – COLLEDARA (TE)
Scuola dell'Infanzia, Primaria e Secondaria di primo grado
Tel. 0861/976191
- email: teic81900X@istruzione.it - teic81900X@pec.istruzione.it - Sito Web: www.icisoladelgransasso.edu.it



.

Istituto Comprensivo Isola G.S. - Colledara (TE)

C.da Pozzo, snc – 64045 -Isola del Gran Sasso d'Italia

REGOLAMENTO DATA BREACH

con disposizioni integrate per strumenti di AI generativa

Gemini e Notebook | Google Workspace for Education

Titolare del trattamento	Istituto Comprensivo Isola G.S. - Colledara (TE) –| C.F. 92027310678 | teic81900x
Rappresentante legale	Falconi Giovanna
DPO – Responsabile Protezione Dati	Mario Grimaldi – Cell. 349.3424766 – dpo.grimaldi@proton.me
Versione documento	N. 2 – Settembre 2026 (incorpora Addendum AI)
Normativa di riferimento	GDPR 679/2016 | D.Lgs. 101/2018 | Linee guida EDPB 01/2021 | AI Act (Reg. UE 2024/1689) | Provv. Garante n. 112/2026
Documenti correlati	Policy AI (DOC. 2/6) | DPIA Gemini–Gemini Notebook (aprile 2026) | Istr. operative ATA (DOC. 4B)

INDICE

SEZIONE I – DEFINIZIONI E AMBITO	Artt. 1-2
SEZIONE II – OBBLIGHI DI NOTIFICA	Artt. 3-8
SEZIONE III – VALUTAZIONE DEL RISCHIO E PROCEDURA INTERNA	Artt. 9-12
SEZIONE IV – DOCUMENTAZIONE E CONTROLLO	Artt. 13-15
SEZIONE V – STRUMENTI DI AI GENERATIVA (GEMINI / GEMINI NOTEBOOK)	Artt. 16-21
SEZIONE VI – RESPONSABILITÀ E DISPOSIZIONI FINALI	Artt. 22-25
APPENDICE – Scheda di segnalazione rapida incidente AI	—

SEZIONE I – DEFINIZIONI E AMBITO

Art. 1 – Definizione di Data Breach e tipologie di violazione

Ai sensi dell'art. 4, par. 12 del Regolamento UE 679/2016 (GDPR), per violazione dei dati personali (Data Breach) si intende qualsiasi violazione di sicurezza che comporta – anche 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. La definizione ricomprende qualsiasi evento che metta a rischio la sicurezza dei dati, indipendentemente dalla causa. Le violazioni si classificano in tre tipologie fondamentali:

- Violazione della riservatezza – divulgazione o accesso non autorizzato o accidentale a dati personali (es. invio di email a destinatari errati, accesso abusivo a sistemi informatici, prompt AI contenenti dati personali elaborati da terzi).
- Violazione dell'integrità – modifica non autorizzata o accidentale di dati personali (es. alterazione di registri, manipolazione di documenti digitali).
- Violazione della disponibilità – perdita, distruzione o blocco accidentali o non autorizzati di dati personali (es. ransomware, guasto di server senza backup, smarrimento di dispositivi).

> **i** *Qualunque evento riconducibile a una delle categorie sopra descritte – inclusi gli incidenti coinvolgenti strumenti di AI generativa disciplinati alla Sezione V – deve essere immediatamente segnalato al DPO e al Titolare, senza attendere valutazioni sulla sua gravità.*

Art. 2 – Ambito di applicazione

Il presente Regolamento si applica a tutti i trattamenti di dati personali effettuati dall'Istituto in qualità di Titolare del trattamento, ivi inclusi:

- I trattamenti effettuati mediante strumenti informatici e telematici (registro elettronico, piattaforme didattiche, posta istituzionale, sistemi di videosorveglianza, strumenti di AI generativa).
- I trattamenti effettuati su supporto cartaceo (fascicoli alunni, documentazione amministrativa, atti contabili).
- I trattamenti effettuati da Responsabili esterni nominati dall'Istituto (fornitori IT, piattaforme cloud, Google LLC per Workspace for Education).

Il Regolamento vincola il Dirigente Scolastico, il DSGA, tutto il personale docente e ATA, nonché i Responsabili esterni del trattamento, ciascuno per quanto di propria competenza.

SEZIONE II – OBBLIGHI DI NOTIFICA

Art. 3 – Obbligo e tempistica di notifica (regola delle 72 ore)

In caso di violazione dei dati personali, l'Istituto ha l'obbligo di notificare la violazione al Garante per la Protezione dei Dati Personali quando è probabile che essa comporti un rischio per i diritti e le libertà delle persone fisiche. La notifica deve avvenire senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare è venuto a conoscenza della violazione (art. 33 GDPR).

Decorrenza del termine

Il termine delle 72 ore inizia a decorrere dal momento in cui il Titolare (o un suo dipendente/collaboratore) acquisisce una ragionevole certezza del verificarsi della violazione. Secondo le Linee guida EDPB 01/2021 è ammesso un breve periodo di indagine iniziale (generalmente non superiore a 24 ore) prima di considerare la violazione «conosciuta».

Notifica tardiva

Se la notifica non può avvenire entro 72 ore, essa deve comunque essere effettuata il prima possibile, corredata di motivazione scritta e documentata dei motivi del ritardo. Il ritardo non giustificato espone il Titolare a sanzioni ai sensi dell'art. 83 GDPR.

Esenzione dall'obbligo

La notifica non è dovuta se il Titolare è in grado di dimostrare che la violazione non presenta alcuna probabilità di rischio per i diritti e le libertà degli interessati. In tal caso, l'evento deve comunque essere registrato nel Registro degli incidenti (art. 13).

Art. 4 – Modalità di notifica al Garante

La notifica al Garante avviene esclusivamente tramite la procedura telematica disponibile sul portale dell'Autorità all'indirizzo: https://servizi.gpdp.it/databreach/s/

La notifica può essere effettuata anche in fasi successive (notifica in più fasi), qualora non siano immediatamente disponibili tutte le informazioni necessarie, purché ogni integrazione avvenga senza ulteriore ingiustificato ritardo. La notifica è curata dal DPO, d'intesa con il Dirigente Scolastico, sulla base del verbale del tavolo tecnico (art. 12).

Art. 5 – Contenuto della notifica all'Autorità di controllo

La notifica al Garante deve contenere almeno le seguenti informazioni (art. 33, par. 3 GDPR):

- La natura della violazione, incluse le categorie e il numero approssimativo di interessati coinvolti e di registrazioni di dati interessate.
- Il nome e i dati di contatto del DPO o di altro punto di contatto.
- Le probabili conseguenze della violazione per i diritti e le libertà degli interessati.
- Le misure adottate o proposte per rimediare alla violazione e, ove applicabile, per attenuarne i possibili effetti negativi.

Art. 6 – Comunicazione agli Interessati

Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Istituto comunica la violazione agli interessati coinvolti senza ingiustificato ritardo (art. 34 GDPR). La comunicazione è redatta in linguaggio semplice e chiaro e descrive: la natura della violazione, i dati di contatto del DPO, le probabili conseguenze, le misure adottate.

La comunicazione avviene preferibilmente per iscritto (email istituzionale, lettera). In caso di impossibilità di contatto individuale si ricorre a comunicazione pubblica equivalente sul sito web istituzionale.

Art. 7 – Condizioni per la mancata comunicazione agli Interessati

Ai sensi dell'art. 34, par. 3 GDPR, l'Istituto è esonerato dall'obbligo di comunicazione individuale in presenza di una delle seguenti condizioni:

- Misure tecniche efficaci: i dati violati erano protetti con misure adeguate (es. cifratura robusta, pseudonimizzazione) che li rendono incomprensibili a soggetti non autorizzati.

- Misure correttive tempestive: l'Istituto ha adottato misure idonee a scongiurare la materializzazione di un rischio elevato per gli interessati.
- Sforzo sproporzionato: la comunicazione individuale richiederebbe sforzi sproporzionati; in tal caso si procede a comunicazione pubblica equivalente.

▲	*Il Garante può richiedere la comunicazione anche in presenza delle condizioni di esonero, se ritiene sussistere un rischio elevato non altrimenti mitigato.*

Art. 8 – Possibili determinazioni dell'Autorità di Controllo

Il Garante, in qualità di Autorità di controllo, può in ogni momento: richiedere al Titolare di effettuare o integrare la comunicazione agli interessati; verificare che le condizioni di esonero (art. 7) siano soddisfatte; disporre misure correttive ai sensi dell'art. 58 GDPR; irrogare sanzioni amministrative pecuniarie ai sensi dell'art. 83 GDPR. L'Istituto si impegna a collaborare pienamente con il Garante in ogni fase del procedimento.

SEZIONE III – VALUTAZIONE DEL RISCHIO E PROCEDURA INTERNA

Art. 9 – Valutazione preliminare del rischio

In presenza di una violazione accertata o presunta, l'Istituto procede immediatamente a una valutazione oggettiva della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche interessate. La valutazione considera i possibili danni, tra cui: limitazione dei diritti degli interessati, furto d'identità, perdite finanziarie, pregiudizio reputazionale, discriminazione in ragione di dati particolari.

Fattori aggravanti prioritari:

- Coinvolgimento di categorie particolari di dati (art. 9 GDPR): sanitari, genetici, biometrici, razziali/etnici, religiosi, politici, giudiziari.
- Coinvolgimento di soggetti vulnerabili, in particolare minori.
- Trattamento di una notevole quantità di dati o coinvolgimento di un vasto numero di interessati.
- Creazione o utilizzo di profili personali mediante analisi automatizzata.

Art. 10 – Criteri e fattori di rischio

Nella valutazione del rischio si tiene altresì conto delle circostanze specifiche della violazione:

- Misure di protezione preesistenti: cifratura o altre misure tecniche che limitano efficacemente il rischio.
- Tipologia di dati: comuni, particolari (art. 9) o giudiziari (art. 10 GDPR).
- Reversibilità del danno: possibilità di ripristinare integrità e disponibilità dei dati.
- Contesto della violazione: interna o esterna, intenzionale o accidentale.
- Interessi investigativi: eventuali esigenze delle autorità di pubblica sicurezza.

Livello di rischio	Determinazione operativa
Rischio basso/assente	Nessuna notifica al Garante. Registrazione obbligatoria nel Registro degli incidenti.
Rischio probabile	Notifica obbligatoria al Garante entro 72 ore. Registrazione nel Registro.
Rischio elevato	Notifica al Garante entro 72 ore + comunicazione senza indugio agli interessati. Registrazione. Misure correttive immediate.

Art. 11 – Esiti della valutazione e decisioni operative

Il principio di accountability (art. 5, par. 2 GDPR) impone che l'Istituto sia in grado di dimostrare documentalmente le proprie determinazioni. L'onere della prova è a carico del Titolare. La decisione finale spetta al Dirigente Scolastico in qualità di Titolare, sulla base della proposta formulata dal DPO nel verbale del tavolo tecnico (art. 12).

Art. 12 – Procedura interna di valutazione – Tavolo tecnico

Segnalazione iniziale

Ogni soggetto che viene a conoscenza di una violazione è tenuto a segnalarla immediatamente – anche verbalmente – e a formalizzare la comunicazione scritta entro massimo 24 ore a: Dirigente Scolastico (Titolare), DPO, DSGA. I Responsabili esterni devono notificare la violazione al Titolare senza ingiustificato ritardo.

Convocazione del Tavolo tecnico

Il DPO, ricevuta la segnalazione, convoca entro 24 ore (anche in videoconferenza) un tavolo tecnico composto da: DPO (coordinatore), Responsabile UOR coinvolta, DSGA, Amministratore di sistema, consulente informatico. Il DPO può convocare ulteriori soggetti in ragione della specificità del caso.

Verbale conclusivo

All'esito del tavolo tecnico, il DPO redige un verbale sottoscritto da tutti i partecipanti, protocollato e trasmesso al Dirigente Scolastico. Il verbale documenta: analisi dell'evento, valutazione del rischio, esito e proposte operative.

SEZIONE IV – DOCUMENTAZIONE E CONTROLLO

Art. 13 – Registro degli incidenti di sicurezza

Il Titolare è tenuto a documentare qualsiasi violazione dei dati personali, indipendentemente dall'obbligo di notifica al Garante, mediante un apposito Registro degli incidenti di sicurezza (art. 33, par. 5 GDPR). Il Registro contiene per ciascun evento:

- Data e ora dell'evento e della sua scoperta.
- Descrizione della natura della violazione e tipologia (riservatezza/integrità/disponibilità).
- Categorie e numero approssimativo di interessati e di registrazioni coinvolte.
- Esito della valutazione del rischio (assente, probabile, elevato).
- Azioni intraprese (notifica al Garante, comunicazione agli interessati, misure correttive).
- Documentazione di supporto (verbali, report tecnici, screenshot, ecc.).

Per gli incidenti coinvolgenti strumenti AI, il Registro è integrato con i campi aggiuntivi previsti dall'art. 20. Il Registro è custodito dal Titolare, che può delegarne la tenuta al DPO, ed è reso disponibile al Garante in occasione di ispezioni. La conservazione minima è di 5 anni.

Art. 14 – Misure preventive e formazione del personale

Al fine di ridurre il rischio di violazioni, l'Istituto adotta le seguenti misure preventive strutturali:

- Formazione periodica del personale: formazione annuale in materia di protezione dei dati, con attenzione alla prevenzione dei data breach, alle misure di sicurezza informatica, alle procedure di segnalazione interna e all'uso sicuro degli strumenti AI.
- Misure tecniche di sicurezza: autenticazione sicura, cifratura dei dispositivi mobili, backup regolari, aggiornamento dei sistemi, gestione degli accessi.
- Misure organizzative: definizione dei profili di accesso, procedure per la gestione della documentazione, verifica periodica dei contratti con i Responsabili esterni.
- Esercitazioni simulate (tabletop exercise): almeno una volta l'anno il DPO organizza una simulazione di gestione di un data breach, inclusi scenari AI.

Art. 15 – Gestione dei Responsabili esterni del trattamento

I Responsabili esterni del trattamento designati ai sensi dell'art. 28 GDPR (inclusa Google LLC per Workspace for Education) sono tenuti contrattualmente a: notificare al Titolare qualsiasi violazione senza ingiustificato ritardo; fornire tutte le informazioni necessarie per la valutazione del rischio; adottare misure correttive per contenere e rimediare alla violazione; cooperare con il DPO nelle attività di indagine.

Il DPO verifica periodicamente che i DPA (Data Processing Agreement) contengano clausole specifiche in materia di data breach e siano allineati alle prescrizioni del Garante. La designazione di un Responsabile esterno non esonera il Titolare dalla propria responsabilità.

SEZIONE V – STRUMENTI DI AI GENERATIVA – GEMINI E GEMINI NOTEBOOK

i	*La presente Sezione integra il Regolamento con disposizioni specifiche per gli incidenti di sicurezza coinvolgenti Google Gemini e Google Gemini Notebook, integrati nella piattaforma Google Workspace for Education. È adottata in attuazione dell'azione correttiva n. 9 della DPIA Gemini–Gemini Notebook (aprile 2026) e coordina con la Policy AI (DOC. 2/6).*

Art. 16 – Classificazione degli scenari di incidente AI

Le violazioni di dati personali che possono verificarsi nell'utilizzo degli strumenti AI sono classificate in tre scenari tipici:

AI-1	**Data leakage via prompt**	Inserimento accidentale di dati personali identificativi (nome, diagnosi, dati retributivi, codice fiscale, ecc.) in un prompt di Gemini o Gemini Notebook. I dati vengono elaborati da Google LLC su infrastrutture potenzialmente extra-UE/SEE.
AI-2	**Accesso trasversale Gemini/Drive o Gmail**	Gemini integrato con Gmail o Google Drive accede a cartelle o email contenenti dati personali sensibili non pertinenti al prompt, con rischio di elaborazione non autorizzata o aggregazione involontaria di informazioni.
AI-3	**Condivisione errata Gemini Notebook**	Un notebook Gemini Notebook contenente dati personali viene condiviso con soggetti non autorizzati per errore di configurazione dei permessi, con conseguente accesso non autorizzato ai contenuti.

Tutti e tre gli scenari sopra descritti possono configurare una violazione dei dati personali ai sensi dell'art. 4, c. 12 del GDPR. Il personale che si trovi in una delle situazioni descritte è tenuto ad avviare immediatamente la procedura di segnalazione prevista dall'art. 17.

Art. 17 – Procedure di segnalazione interna – Scenari AI

Scenario AI-1 – Data leakage via prompt

Passo	Timing	Responsabile e modalità
PASSO 1 INTERROMPI	Immediato	Il dipendente interrompe l'attività, non invia ulteriori prompt correlati, non tenta di rimediare autonomamente. Annota per iscritto il contenuto del prompt e dell'output ricevuto.
PASSO 2 SEGNALA AL DSGA/DS	Entro 60 min	Segnala verbalmente al DSGA/DS: quale dato personale, in quale contesto, quale output generato.
PASSO 3 NOTIFICA FORMALE	Entro 4 ore	Il DS informa per iscritto il DPO (dpo.grimaldi@proton.me). L'Amministratore di sistema verifica i log di accesso Gemini in Admin Console.
PASSO 4 VALUTAZIONE DPO	Entro 24 ore*	Il DPO convoca il tavolo tecnico (art. 12) nella composizione minima: DPO, DS, DSGA, Amministratore di sistema. Valuta: natura del dato, probabilità di accesso da parte di Google, rischio per l'interessato.
PASSO 5 DECISIONE	Entro 72 ore se necessario	Il DPO redige il verbale e formula la proposta al Titolare (DS). Il Titolare decide: (a) nessuna notifica; (b) notifica al Garante ex art. 33 GDPR; (c) comunicazione all'interessato ex art. 34 GDPR.

▲	** DATI AD ALTO RISCHIO: Se il dato riguarda dati sanitari, diagnosi BES/DSA, dati giudiziari/disciplinari, o dati di studenti minorenni, il PASSO 4 deve avvenire entro 4 ore, non 24 (priorità ai sensi degli artt. 9-10 GDPR).*

Scenario AI-2 – Accesso trasversale Gemini/Drive o Gmail

Questo scenario si verifica quando l'utente rileva, o sospetta, che Gemini integrato con Drive o Gmail abbia elaborato contenuti non pertinenti al prompt, inclusi dati personali sensibili presenti in cartelle o email accessibili all'account.

Passo	Timing	Responsabile e modalità
PASSO 1 IDENTIFICA	Immediato	L'utente cessa l'uso di Gemini su quel file/cartella. Annota: cartella/file, prompt, output anomalo.
PASSO 2 SEGNALA	Entro 1 ora	Segnala a DS e DPO (dpo.grimaldi@proton.me). L'Amministratore di sistema verifica in Admin Console i permessi della cartella Drive e i log di accesso Gemini.
PASSO 3 CONTENIMENTO	Entro 2 ore	L'Amministratore di sistema rimuove l'accesso di Gemini alla cartella/file (restrizione permessi in Admin Console) e documenta l'intervento.
PASSO 4 VALUTAZIONE	Entro 24 ore	Il DPO valuta: tipologia di dati accessibili a Gemini, probabilità che i dati siano stati elaborati da Google, rischio residuo per gli interessati.
PASSO 5 DECISIONE	Entro 72 ore se necessario	Stessa procedura dello Scenario AI-1, Passo 5. Notifica al Garante se il rischio è probabile.

Scenario AI-3 – Condivisione errata di notebook Gemini Notebook

Passo	Timing	Responsabile e modalità
PASSO 1 REVOCA	Immediato	L'utente revoca immediatamente l'accesso al notebook (rimozione del condivisore non autorizzato dall'interfaccia Gemini Notebook). Annota chi ha avuto accesso e per quanto tempo.
PASSO 2 SEGNALA	Entro 1 ora	Segnala a DSGA e DS. L'Amministratore di sistema verifica se l'accesso ha comportato download o copia dei contenuti.
PASSO 3 VALUTAZIONE	Entro 24 ore	Il DPO valuta: contenuto del notebook, identità del soggetto che ha avuto accesso non autorizzato, azioni compiute durante il periodo di accesso.
PASSO 4 DECISIONE	Entro 72 ore se necessario	Il DPO formula la proposta al Titolare come per gli scenari precedenti.

Art. 18 – Valutazione del rischio – Fattori specifici per incidenti AI

In aggiunta ai criteri degli artt. 9-10, per gli incidenti AI il tavolo tecnico deve tenere conto dei seguenti fattori specifici:

Fattore	Criteri di valutazione
Natura del dato elaborato	Dati sanitari, BES/DSA, giudiziari, retributivi e dati di minori comportano livello di rischio ALTO indipendentemente dalle altre circostanze.
Impostazione AI training	Se l'impostazione che disabilita l'uso dei dati per l'addestramento dei modelli AI di Google non è attiva al momento dell'incidente, il rischio è ALTO.
Elaborazione fuori UE/SEE	I dati elaborati da Gemini possono transitare su infrastrutture Google fuori dal SEE. Fattore strutturale che incide sulla gravità dell'impatto, ma non modifica da solo l'obbligo di notifica.
Durata dell'esposizione	Negli scenari AI-2 e AI-3 la durata dell'esposizione può essere prolungata: il tempo trascorso prima della revoca è fattore di aggravamento.
Pseudonimizzazione/anonimizzazione	Se il dato era pseudonimizzato/anonimizzato conformemente alla Policy AI (DOC. 2/6), il rischio è ridotto. Il tavolo tecnico verifica l'effettività della misura.

Art. 19 – Raccordo con la Policy AI e le istruzioni operative

Le procedure della presente Sezione V si coordinano con le seguenti disposizioni della Policy Interna AI – DOC. 2/6:

- Art. 12 Policy AI (Segnalazione incidenti): definisce le tempistiche generali, integrate dalle tempistiche specifiche del presente art. 17.
- Art. 5 Policy AI (Regole sui prompt): il rispetto delle regole riduce la probabilità degli incidenti AI-1. La violazione è fattore aggravante nella valutazione del rischio.
- Art. 6 Policy AI (Regole ATA) e DOC. 3/6 / DOC. 4B: le istruzioni IO-ATA5 definiscono la procedura di segnalazione per il personale ATA, coordinata con il presente Regolamento.

Art. 20 – Registro degli incidenti AI – Sezione dedicata

Il Registro degli incidenti (art. 13) è integrato con una sezione dedicata agli incidenti AI. I campi standard dell'art. 13 si applicano anche agli incidenti AI e si integrano – non si sostituiscono – con i seguenti campi aggiuntivi:

Campo aggiuntivo Sezione AI	Valore / Note
Scenario AI	AI-1 / AI-2 / AI-3 (v. art. 16)
Strumento coinvolto	Gemini / Gemini Notebook / Integrazione Gmail / Integrazione Drive
Tipologia di dato	Identificativo / Sanitario / BES-DSA / Retributivo / Giudiziario / Minore / Altro
Impostazione AI training al momento dell'incidente	Disabilitata (conforme) / Abilitata (non conforme) / Non verificata
Misura di contenimento tecnico adottata	Descrizione dell'intervento dell'Amministratore di sistema

Esito della valutazione DPO	Notifica al Garante: sì / no / in corso | Comunicazione all'interessato: sì / no
Azione correttiva permanente	Modifica policy, formazione aggiuntiva, restrizione tecnica adottata a seguito dell'incidente

Art. 21 – Contatti operativi per la segnalazione degli incidenti AI

Ruolo	Recapito
Dirigente Scolastico (Titolare)	Falconi Giovanna – TEIC81900X@ISTRUZIONE.IT
DPO	Mario Grimaldi – dpo.grimaldi@proton.me – Cell. 349.3424766
Amministratore di sistema/referente google workspace	Animatore digitale/amministratore google workspace
Portale notifica al Garante	https://servizi.gpdp.it/databreach/s/

SEZIONE VI – RESPONSABILITÀ E DISPOSIZIONI FINALI

Art. 22 – Sanzioni e responsabilità

Sanzioni amministrative (art. 83 GDPR)

La violazione degli obblighi in materia di data breach (artt. 33 e 34 GDPR) è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 € o, per le imprese, fino al 2% del fatturato mondiale annuo. Le sanzioni sono effettive, proporzionate e dissuasive.

Responsabilità civile (art. 82 GDPR)

Chiunque subisca un danno materiale o immateriale causato da una violazione ha diritto al risarcimento. Il Titolare è esonerato solo se dimostra di non essere in alcun modo imputabile dell'evento dannoso.

Falsi positivi

Non è prevista alcuna sanzione per la notifica di un incidente che si riveli successivamente un falso allarme. È pertanto preferibile notificare in caso di dubbio.

Responsabilità disciplinare

Il personale che omette di segnalare una violazione, o che con la propria condotta abbia causato o contribuito a causarla, può essere soggetto a procedimento disciplinare ai sensi del CCNL applicabile.

Art. 23 – Strumento telematico di notifica

La notifica al Garante avviene tramite la procedura telematica ufficiale disponibile all'indirizzo: https://servizi.gpdp.it/databreach/s/ – compilazione del modello ufficiale (v. 2021-04), che raccoglie le informazioni prescritte dall'art. 33, par. 3 GDPR e dalle Linee guida EDPB 01/2021. Il DPO cura compilazione e invio, conservandone copia agli atti. Ogni notifica è protocollata e inserita nel Registro degli incidenti.

Art. 24 – Aggiornamento del Regolamento

L'Istituto si riserva di aggiornare il presente Regolamento in caso di: modifiche normative o nuovi provvedimenti del Garante/EDPB; nuovi scenari di incidente AI identificati nella pratica operativa; modifiche alle funzionalità di Gemini o Gemini Notebook da parte di Google; aggiornamento della DPIA; variazioni organizzative rilevanti. Gli aggiornamenti sono comunicati al personale tramite circolare interna e pubblicati sul sito istituzionale.

Art. 25 – Norma finale ed entrata in vigore

Il presente Regolamento entra in vigore dalla data di adozione da parte del Dirigente Scolastico ed è pubblicato sul sito istituzionale nella sezione dedicata alla Privacy. Per tutto quanto non espressamente previsto si rinvia al GDPR 679/2016, al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, alle Linee guida EDPB 01/2021, ai provvedimenti del Garante, alla Policy AI (DOC. 2/6) e alla DPIA Gemini–Gemini Notebook (aprile 2026).

Il Dirigente Scolastico

Falconi Giovanna

_____

Data _____

APPENDICE – SCHEDA DI SEGNALAZIONE RAPIDA INCIDENTE AI

Da compilare immediatamente e trasmettere a DS e DPO entro 2 ore dall'accaduto.

A – IDENTIFICAZIONE DELL'INCIDENTE

Data e ora dell'incidente (approssimativa)	
Nome del segnalante	
Qualifica	☐ Docente ☐ ATA ☐ Studente ☐ Altro: _____

B – CLASSIFICAZIONE

Scenario identificato	☐ AI-1 Data leakage prompt ☐ AI-2 Accesso Drive/Gmail ☐ AI-3 Gemini Notebook
Strumento coinvolto	☐ Gemini ☐ Gemini Notebook ☐ Gemini in Gmail ☐ Gemini in Drive
Tipologia di dato personale coinvolto	☐ Identificativo ☐ Sanitario/BES-DSA ☐ Retributivo ☐ Minore ☐ Altro: _____

C – DESCRIZIONE E AZIONI DEL SEGNALANTE

Descrizione sintetica dell'accaduto	(spazio libero – continuare sul retro se necessario)
Azioni già intraprese	(es. interruzione uso, revoca accesso, ecc.)
Output di Gemini / Gemini Notebook correlato	☐ Conservato ☐ Eliminato ☐ Non disponibile
Note aggiuntive	

▲ *TRASMETTERE ENTRO 2 ORE a DS («pec») e DPO (dpo.grimaldi@proton.me). NON condividere questa scheda con soggetti non coinvolti nella procedura.*

D – USO RISERVATO DS / DPO

Data e ora di ricezione	
Preso in carico da	
Prot. n. (assegnato dalla segreteria)	
Esito valutazione DPO	☐ Nessuna notifica (rischio improbabile) ☐ Notifica al Garante ☐ Comunicazione all'interessato
Azione correttiva adottata	