FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

DOCUMENTO DI VALUTAZIONE

DPIA

Google Workspace for Education

Valutazione d'impatto sulla protezione dei dati personali
ai sensi dell'art. 35 del Regolamento (UE) 2016/679

ISTITUZIONE SCOLASTICA: [DENOMINAZIONE]

Codice meccanografico: [FGIC878001] | Dominio Workspace: [istitutocomprensivovieste.edu.it]

Titolare del trattamento: Istituzione scolastica, in persona del Dirigente scolastico
Redazione: Dirigente scolastico / gruppo di lavoro privacy e digitale
DPO/RPD consultato: Avv. Nicola Parisi [verificare attualità della nomina]

Versione del 21 ottobre 2026

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

Sintesi esecutiva

La valutazione riguarda il trattamento di dati personali di alunni, docenti e altro personale scolastico mediante account istituzionali Google Workspace for Education, con uso di strumenti cloud per collaborazione, distribuzione di materiali, elaborazione di documenti, comunicazione didattica e, se autorizzata, videoconferenza. Il perimetro operativo assunto come riferimento comprende Gmail, Drive/Documenti, Calendar, Sites e Meet; altri servizi sono inclusi esclusivamente se effettivamente attivati e autorizzati dalla scuola.

Il trattamento è valutato in via prudenziale mediante DPIA per la combinazione di più fattori: interessati vulnerabili (minori), possibile trattamento su scala istituzionale, creazione e condivisione continuativa di contenuti, metadati e registri tecnici, possibile presenza incidentale di dati particolari, rischi di accesso o condivisione non autorizzati e catena di fornitori/sub-responsabili. La presenza di minori, da sola, non implica automaticamente l'obbligo di DPIA; qui la valutazione considera il contesto complessivo e le caratteristiche concrete della piattaforma.

La documentazione Google distingue i dati del cliente dai dati di servizio e distingue i Servizi principali dagli eventuali Servizi aggiuntivi. Per i Servizi principali, i dati creati o caricati sono trattati in base alle istruzioni della scuola, secondo le condizioni contrattuali applicabili; i dati di servizio possono essere trattati per erogare, mantenere e proteggere i servizi e per ulteriori finalità descritte nell'informativa Google Cloud. In assenza di verifica dell'eventuale accettazione dell'Addendum per i dati di servizio, il ruolo di Google per alcune operazioni su tali dati deve restare un punto aperto della valutazione.

Conclusione provvisoria L'impiego della piattaforma può essere compatibile con il GDPR per finalità didattiche circoscritte, a condizione che il Titolare verifichi il contratto effettivamente applicabile, limiti i servizi e le condivisioni, implementi i controlli di sicurezza e documenti le basi giuridiche, i tempi di conservazione e i trasferimenti. Alla data di redazione non è possibile attestare in modo definitivo che tutti i rischi residui siano bassi: le valutazioni residue riportate sono obiettivi condizionati all'effettiva implementazione e verifica delle misure.

1. Oggetto, finalità e campo di applicazione

1.1 Oggetto del trattamento

La DPIA analizza gli effetti dell'utilizzo di un ambiente cloud gestito dall'istituzione scolastica, nel quale gli account vengono creati e amministrati dalla scuola e sono destinati all'attività istituzionale e didattica. Le operazioni possono includere raccolta e organizzazione dei dati identificativi, autenticazione, produzione e archiviazione di contenuti, condivisione tra utenti autorizzati, comunicazioni, gestione di calendari, incontri online, assistenza tecnica, registrazione di log e metadati, esportazione, archiviazione e cancellazione.

1.2 Finalità determinate

- assegnare agli utenti account istituzionali e consentire l'autenticazione ai servizi didattici approvati;
- distribuire e condividere materiali, esercitazioni, risorse e documenti, anche nell'ambito di attività collaborative;
- consentire la redazione, revisione e consegna di elaborati e, ove previsto, il feedback didattico dei docenti;
- gestire calendari e riunioni didattiche, inclusi incontri online quando necessari e proporzionati;
- consentire amministrazione tecnica, sicurezza, gestione degli accessi, assistenza e continuità operativa;
- conservare e trasferire nell'archivio istituzionale i documenti da mantenere per obblighi di legge o esigenze amministrative documentate.

Sono escluse dal perimetro, salvo previa valutazione integrativa: uso personale o consumer degli account; accesso indiscriminato a servizi aggiuntivi non pertinenti; installazione libera di applicazioni di terze parti; uso della piattaforma per procedure amministrative che richiedano un sistema istituzionale specifico; decisioni automatizzate significative; profilazione degli studenti; registrazione sistematica di lezioni; e uso di funzionalità di intelligenza artificiale generativa non espressamente approvate.

1.3 Servizi inclusi e variazioni di perimetro

Categoria	Perimetro di riferimento	Regola di valutazione
Servizi principali indicati nel modello	Gmail, Drive/Documenti, Calendar, Sites, Meet	Includere solo quelli abilitati e effettivamente utilizzati. Verificare anche condivisioni esterne, registrazioni, sottotitoli, trascrizioni, chat e integrazioni.
Altri Servizi Education	Il riepilogo Google corrente comprende, tra gli altri, AppSheet e Read Along	Non presumere che siano abilitati. Se usati, descrivere funzione, dati, destinatari, età degli utenti e finalità.

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

Categoria	Perimetro di riferimento	Regola di valutazione
Altri Servizi principali oggi elencati da Google	Ad es. Classroom, Contatti, Moduli, Gruppi, Fogli, Presentazioni, Chat, Vault, Chrome Sync, Gemini for Education, Gemini Notebook e Google Workspace LTI	Se attivati, integrare inventario, analisi di necessità, tipologie di dati, misure e rischi. Le funzionalità AI richiedono valutazione specifica prima dell'uso.
Servizi aggiuntivi consumer	Ad es. Ricerca Google, Maps e YouTube; possono essere disciplinati da Norme sulla privacy e termini differenti	Impostazione raccomandata: disabilitati per impostazione predefinita, salvo attivazione motivata, informazione adeguata e rispetto delle condizioni Google, incluso il consenso genitoriale richiesto contrattualmente per utenti sotto i 18 anni.

2. Contesto, interessati e categorie di dati

2.1 Interessati

- alunni, anche minorenni, iscritti all'istituzione scolastica;
- docenti, dirigenti e personale ATA o altro personale autorizzato;
- genitori/tutori o altri soggetti i cui dati siano contenuti nelle comunicazioni o nei documenti didattici;
- altri utenti o mittenti esterni, solo se l'accesso o lo scambio con soggetti esterni è autorizzato e necessario.

2.2 Categorie di dati

Categoria	Esempi / note di perimetro
Identificativi e account	Nome, cognome, account e-mail istituzionale, identificativo dell'account, appartenenza a classe/gruppo, ruoli e autorizzazioni. Non è necessario che la scuola raccolga o conservi password in chiaro.
Contenuti didattici	Documenti, elaborati, presentazioni, fogli, file, email, calendari, siti didattici, commenti e feedback. Possono contenere dati riferibili a studenti o terzi.
Dati connessi a Meet	Metadati della riunione, partecipanti, chat e contenuti audio/video durante la sessione; registrazioni, trascrizioni o sottotitoli solo se la funzione è abilitata e il trattamento è previamente autorizzato e informato.
Dati di utilizzo e sicurezza	Log di accesso, data/ora, indirizzi IP, informazioni su browser, dispositivo, sistema operativo, versione/app, eventi tecnici, interazioni con servizi, condivisioni e richieste di supporto. La loro disponibilità dipende da servizio, impostazioni e licenza.
Dati di servizio	Informazioni generate durante l'uso e la gestione dei servizi, distinte dai contenuti del cliente; possono comprendere account, attività d'uso, impostazioni e dispositivi, comunicazioni con supporto e dati amministrativi indicati nell'informativa Google Cloud.
Categorie particolari ex art. 9 GDPR	Non costituiscono una categoria necessaria ordinaria. Potrebbero emergere incidentalmente in elaborati o comunicazioni (salute/disabilità, convinzioni, origine etnica o altri dati particolari). L'inserimento va limitato e, se indispensabile, autorizzato e protetto con accessi segregati.
Dati relativi a condanne/reati	Non previsti per le finalità ordinarie qui valutate; non caricare tali dati nella piattaforma salvo specifica necessità istituzionale, base normativa, istruzioni e valutazione separata.

Prescrizione di minimizzazione I dati particolari, sanitari, relativi a disabilità, PEI/PDP o altri documenti ad alta riservatezza non devono essere collocati in cartelle didattiche condivise in modo ordinario. Ove il trattamento su tale ambiente sia strettamente necessario, occorrono valutazione specifica, base giuridica ex artt. 6 e 9 GDPR e normativa nazionale applicabile, accesso nominativo ristretto, cifratura adeguata, log e tempi di conservazione definiti.

3. Flusso dei dati, ciclo di vita e risorse

Fase	Descrizione	Punti di controllo
1. Attivazione	La scuola crea e assegna account e ruoli agli utenti.	Minimizzare gli attributi; assegnare gruppi/organizzazioni corrette; non inviare né conservare password in chiaro; definire gestione credenziali e recupero.
2. Accesso e uso	L'utente accede ai servizi autorizzati da dispositivi scolastici o personali.	MFA dove disponibile e appropriata; account individuali; protezione dei dispositivi; gestione delle sessioni; istruzioni BYOD.

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

Fase	Descrizione	Punti di controllo
3. Creazione/condivisione	Gli utenti producono e condividono elaborati, email, calendari, materiali e contenuti Meet.	Permessi specifici; restrizione condivisione esterna/pubblica; controllo prima di condividere; supervisione docente; divieto di uso non didattico.
4. Telemetria/supporto	I servizi generano dati di servizio e log; personale autorizzato può attivare richieste di supporto.	Verificare log disponibili e retention; minimizzare i dati nei ticket; accessi amministrativi circoscritti; distinguere dati del cliente e dati di servizio.
5. Valutazione/archiviazione	I materiali necessari a valutazioni o obblighi amministrativi sono trasferiti nel sistema/repository ufficiale previsto.	Individuare versione finale, responsabilità e massimario/prontuario di conservazione; separare file temporanei da documentazione da conservare; limitare accessi.
6. Uscita e cancellazione	Al termine del rapporto di utilità, account e dati sono esportati, disattivati o cancellati secondo una procedura.	Definire scadenze diverse per studenti e personale; esportazione anticipata; cancellazione controllata; verificare tempi e limitazioni contrattuali Google.

La piattaforma è fruita tramite dispositivi e connessioni che possono non essere nella disponibilità fisica della scuola. Il trattamento include pertanto rischi lato utente (dispositivo condiviso, browser, phishing, rete domestica, copie scaricate), oltre ai rischi connessi al fornitore cloud. La modalità di navigazione in incognito non impedisce al servizio cloud di trattare i dati necessari all'erogazione né sostituisce controlli di accesso, cifratura, configurazione e minimizzazione.

4. Necessità, proporzionalità e basi giuridiche

4.1 Necessità e proporzionalità

La piattaforma è valutata come strumento complementare all'attività didattica ordinaria, non come finalità autonoma né come sostituto generalizzato dei sistemi istituzionali di protocollo, registro elettronico o conservazione documentale. Il trattamento deve essere limitato agli strumenti necessari ai processi effettivamente previsti dal PTOF e dalla programmazione didattica. Per ogni servizio attivato il Titolare deve poter motivare: (i) finalità concreta; (ii) necessità rispetto ad alternative meno invasive; (iii) categorie di dati indispensabili; (iv) utenti destinatari; (v) periodo di conservazione; (vi) eventuale accesso esterno o trasferimento.

Il regolamento d'istituto e le policy operative sono strumenti necessari di governance, ma non costituiscono, da soli, la fonte legislativa richiesta dall'art. 6, par. 3, GDPR. La base normativa del compito di interesse pubblico discende dai compiti istituzionali della scuola e dalla normativa nazionale applicabile; il Titolare deve richiamare le disposizioni pertinenti alla propria funzione e alle specifiche operazioni nella documentazione generale dei trattamenti.

4.2 Base giuridica

Operazione	Base giuridica di riferimento
Gestione account e uso dei servizi per la didattica	Art. 6, par. 1, lett. e), GDPR, in relazione al compito di interesse pubblico e alla normativa che attribuisce alla scuola le funzioni educative.
Adempimenti obbligatori connessi al rapporto scolastico/lavorativo	Art. 6, par. 1, lett. c) e/o lett. e), secondo la singola operazione.
Dati particolari eventualmente indispensabili	Art. 9, par. 2, GDPR, in combinazione con la base ex art. 6 e con una specifica condizione e norma nazionale applicabile.
Pubblicazione esterna di foto/video o diffusione non necessaria alla didattica	Valutazione autonoma della finalità e della base giuridica.

Il consenso dei genitori non è assunto quale base giuridica ordinaria del trattamento istituzionale necessario alla didattica tramite i Servizi principali. Resta distinta l'eventuale richiesta contrattuale di consenso parentale prevista da Google per l'accesso dei minori a Servizi aggiuntivi autorizzati dalla scuola, nonché la necessità di valutare una base giuridica separata per finalità facoltative o per la diffusione pubblica di immagini.

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

5. Ruoli privacy e condizioni contrattuali Google

5.1 Titolare, responsabile, autorizzati

- La scuola è Titolare per le finalità e i mezzi essenziali del trattamento istituzionale dei dati di alunni e personale, salvo specifici trattamenti per i quali la qualificazione vada verificata.
- Per i Servizi principali e i dati del cliente, Google opera in linea generale quale responsabile ai sensi delle condizioni applicabili e del Cloud Data Processing Addendum (CDPA/DPA), che disciplina oggetto, durata, finalità, misure di sicurezza, assistenza, incidenti, sub-responsabili, diritti e cancellazione.
- Google può trattare alcuni dati di servizio in qualità di titolare per finalità limitate descritte nella documentazione Google Cloud; l'eventuale Service Data Addendum facoltativo modifica la ripartizione dei ruoli per la parte di dati di servizio trattata come responsabile, senza necessariamente eliminare tutti i trattamenti autonomi di Google.
- I docenti, il dirigente e il personale amministrativo che trattano dati sotto l'autorità della scuola sono autorizzati al trattamento e devono ricevere istruzioni adeguate; non diventano automaticamente responsabili del trattamento in senso GDPR.
- Il fornitore IT o l'amministratore esterno che accede ai dati per conto della scuola deve essere qualificato in base all'attività effettiva e, ove ne ricorrano i presupposti, disciplinato ai sensi dell'art. 28 GDPR. Le app, estensioni o integrazioni di terze parti possono avere titolarità e condizioni autonome e non vanno considerate automaticamente coperte dal DPA Google.

5.2 Verifiche contrattuali richieste

Documento / controllo	Valutazione e azione
Google Workspace for Education Terms of Service	Verificare l'esatta versione accettata, la parte contraente, l'edizione/licenza e l'eventuale contratto offline. La sola disponibilità online delle condizioni non prova l'accettazione da parte della scuola.
Cloud Data Processing Addendum fornito in PDF	Conservare la copia effettivamente incorporata nel contratto e verificare data/accettazione. L'addendum prevede misure tecniche e organizzative, assistenza, notifiche di incidenti, sub-responsabili, diritti di audit/documentazione, trasferimenti e cancellazione.
Service Data Addendum (facoltativo)	Verificare nella Console/contrattualistica se è stato accettato. Se non accettato, chiarire nell'informativa che Google può agire da titolare per talune finalità relative ai dati di servizio descritte dalla propria informativa; se accettato, aggiornare la mappatura dei ruoli e le informative in base al testo accettato.
Sub-responsabili	Esaminare l'elenco ufficiale, l'aggiornamento dei soggetti e dei luoghi di trattamento, il processo di notifica e la gestione di eventuali opposizioni secondo il DPA applicabile. Conservare evidenza della verifica periodica.
Prodotti aggiuntivi / app Marketplace / estensioni	Verificare termini, informativa, permessi OAuth/API, accesso ai contenuti, ubicazione, ruoli privacy e basi del trasferimento. Vietare l'installazione autonoma agli utenti ove tecnicamente possibile.

6. Informativa Google e distinzione tra servizi

L'Informativa sulla privacy di Google Workspace for Education consultata per questa redazione reca data di ultima modifica 13 agosto 2026. La pagina ufficiale distingue: (a) Servizi principali, coperti dalle condizioni Education e dal Cloud DPA; (b) Altri servizi Education, ai quali l'informativa estende le indicazioni riferite ai Servizi principali; (c) Servizi aggiuntivi consumer, per i quali possono trovare applicazione le Norme sulla privacy Google e termini specifici differenti.

Per i Servizi principali, Google dichiara di trattare i dati del cliente secondo le istruzioni della scuola per fornire, proteggere e monitorare i servizi; dichiara inoltre che non vengono mostrati annunci nei Servizi principali e che i dati personali raccolti in questi servizi non sono utilizzati per finalità pubblicitarie. I dati di servizio sono distinti dai contenuti e possono includere dati account, attività, dispositivi/browser, indirizzo IP, eventi tecnici, data e ora e comunicazioni con il supporto; l'informativa descrive impieghi per erogare e mantenere i servizi, sicurezza/affidabilità, assistenza, raccomandazioni di ottimizzazione e adempimenti di legge.

I Servizi aggiuntivi, invece, possono raccogliere ulteriori dati relativi alle ricerche, ai siti visitati, ai video, all'audio, alle risposte AI, alle interazioni e alla posizione; possono essere regolati dalle Norme sulla privacy Google e, per alcuni, da termini specifici. La documentazione Google indica che l'amministratore gestisce l'accesso ai servizi e che, per i Servizi aggiuntivi autorizzati per utenti di età inferiore a 18 anni, la scuola deve ottenere il consenso del genitore/tutore secondo le condizioni Google. Tale requisito contrattuale va distinto dalla base giuridica GDPR che legittima il trattamento svolto dalla scuola per la propria finalità istituzionale.

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

Configurazione raccomandata Disabilitare per default i Servizi aggiuntivi e le app di terze parti non necessarie. Se un servizio viene autorizzato, prima dell'attivazione registrare finalità, necessità, dati, destinatari, termini, informativa, eventuale consenso parentale richiesto da Google, trasferimenti, retention e misure. Ogni ampliamento del perimetro va sottoposto a verifica privacy preventiva.

7. Trasferimenti internazionali e localizzazione

7.1 Quadro contrattuale e DPF

Il Cloud DPA caricato prevede che i trasferimenti soggetti alla normativa europea siano effettuati attraverso una soluzione di trasferimento alternativa adeguata o, se questa non è applicabile/disponibile, mediante le clausole contrattuali tipo (SCC) secondo i moduli e le condizioni pertinenti. La documentazione fornita contempla data center distribuiti in più aree geografiche; pertanto, non è corretto affermare che le SCC assicurino, da sole, la permanenza dei dati esclusivamente nel territorio UE.

Alla data di aggiornamento della presente DPIA, la decisione di adeguatezza UE-USA sul Data Privacy Framework (Decisione di esecuzione (UE) 2023/1795) risulta in vigore. Il registro pubblico del programma indica Google LLC come partecipante attivo al quadro UE-USA DPF, con prossima ricertificazione indicata al 13 settembre 2027. La decisione del Tribunale UE del 3 settembre 2025 nella causa T-553/23 Latombe/Commissione ha respinto il ricorso di annullamento; la sentenza risulta impugnata nella causa C-703/25 P. Lo stato della decisione e della certificazione va riverificato periodicamente.

La decisione di adeguatezza ex art. 45 GDPR può costituire la base per trasferimenti verso l'organizzazione statunitense certificata, solo entro il perimetro della certificazione e per il destinatario effettivo. Non si può estendere automaticamente tale copertura a qualsiasi sub-responsabile, servizio aggiuntivo, società del gruppo o trasferimento ulteriore. Per questi casi occorre verificare l'effettivo destinatario e il meccanismo di trasferimento applicato in base al DPA e ai relativi allegati.

7.2 Limiti della localizzazione UE

La localizzazione in data center UE, ove contrattualmente disponibile e correttamente configurata per l'edizione e per i dati inclusi, può ridurre alcuni rischi ma non deve essere trattata come garanzia assoluta di assenza di accesso da parte di soggetti stabiliti in paesi terzi, né come prova di esclusione di tutti i dati di servizio, metadati, operazioni di supporto o trattamenti dei sub-responsabili. Occorre verificare il perimetro preciso della funzione di data region e il prodotto/licenza cui si applica.

La possibilità che autorità di un paese terzo richiedano dati a fornitori soggetti alla propria giurisdizione costituisce uno scenario da considerare, ma non va descritta come accesso automatico o generalizzato. Rilevano la disciplina applicabile, la validità e portata della richiesta, gli obblighi contrattuali del fornitore e le procedure di contestazione/notifica ammesse dalla legge.

7.3 Valutazione e condizioni

Elemento	Esito della valutazione	Azione necessaria
Google LLC e DPF	Meccanismo di adeguatezza potenzialmente applicabile, subordinato a certificazione attiva e copertura del trasferimento specifico.	Conservare evidenza aggiornata della certificazione e della controparte; verificare il ruolo della società contraente e gli eventuali destinatari ulteriori.
Altri trasferimenti/sub-responsabili	Il DPA prevede un meccanismo contrattuale per trasferimenti soggetti alla normativa europea, incluso ricorso a SCC secondo i casi.	Consultare la lista attuale dei sub-responsabili, le località e le informazioni sui trasferimenti; documentare il meccanismo di ogni flusso rilevante.
Contenuti particolari o altamente riservati	Non giustificati dal solo fatto che sia disponibile un contratto o una data region.	Minimizzare; non caricare se non necessario; valutare cifratura end-to-end/client-side realmente applicata e gestione delle chiavi. Separare l'archivio ufficiale.
Rischio residuo	Non eliminabile in astratto; dipende da destinatari, servizi attivi, contenuti e configurazioni.	Riesame almeno annuale e a ogni variazione significativa normativa, contrattuale o tecnica.

8. Conservazione, esportazione e cancellazione

Non è corretto adottare un periodo unico di conservazione per tutti i dati presenti nella piattaforma. I termini devono differenziarsi in funzione della finalità, del tipo di documento e degli obblighi archivistici/amministrativi applicabili. I materiali

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

temporanei non sottoposti a valutazione devono essere eliminati quando termina la finalità; gli elaborati e i documenti rilevanti per la valutazione o per procedimenti istituzionali devono essere trasferiti nel sistema documentale previsto e conservati secondo le regole archivistiche e il massimario/prontuario applicabile alla specifica tipologia. La regola “almeno un anno” contenuta nella bozza originaria non va generalizzata senza verifica della normativa archivistica applicabile al documento concreto.

Categoria	Regola proposta
Account alunni	Mantenimento per il tempo necessario al ciclo di studi e alle attività documentate; al termine, informazione preventiva, finestra di esportazione definita dalla scuola, disattivazione e cancellazione secondo procedura.
Account personale	Disattivazione tempestiva al termine del rapporto o al venir meno della necessità; trasferimento dei documenti istituzionali al sostituto/repository e finestra di esportazione personale solo se consentita e compatibile con gli obblighi di servizio.
File temporanei e collaborativi non valutativi	Cancellare alla conclusione dell’attività o comunque al termine dell’anno scolastico, salvo necessità documentata di prosecuzione pluriennale.
Elaborati oggetto di valutazione/documenti amministrativi	Trasferire la versione definitiva nell’archivio istituzionale secondo le regole di conservazione applicabili; limitare la permanenza nel Drive didattico al tempo strettamente necessario.
Dati particolari e registrazioni	Retention specifica, accessi ristretti e cancellazione anticipata appena viene meno la necessità; registrazioni Meet non abilitate per default.

Vincolo contrattuale da considerare Nel DPA fornito, Google si impegna a cancellare i dati oggetto di istruzione di eliminazione non appena ragionevolmente possibile ed entro un massimo di 180 giorni, salvo obblighi legali di conservazione. Alla cessazione del servizio è previsto inoltre un periodo di recupero fino a 30 giorni prima dell’avvio della cancellazione dei dati residui, con il termine massimo contrattuale indicato. Questi tempi tecnici non sostituiscono gli obblighi della scuola di cancellare tempestivamente nell’ambiente di propria gestione, né autorizzano una retention eccedente la finalità.

Prima di disattivare o eliminare un account, il Titolare deve verificare l’esportazione dei contenuti necessari, la presa in carico da parte del repository ufficiale, la cancellazione delle condivisioni, la gestione delle copie locali e la registrazione dell’operazione. Il diritto alla cancellazione va esaminato caso per caso: non sussiste un divieto generalizzato di cancellare tutti gli elaborati per un anno; eventuali limiti devono derivare da un obbligo di conservazione o da una necessità istituzionale documentata.

9. Trasparenza e diritti degli interessati

Prima dell’uso, gli interessati devono ricevere un’informativa ai sensi degli artt. 12-14 GDPR, chiara e adatta anche a minori, che identifichi Titolare e DPO, finalità e basi giuridiche, categorie di dati, destinatari, ruoli del fornitore, eventuali trattamenti dei dati di servizio da parte di Google come titolare, trasferimenti internazionali, retention, modalità di esercizio dei diritti e possibilità di reclamo al Garante. L’informativa deve distinguere i servizi effettivamente attivati, non limitarsi a un generico richiamo all’intera suite Google.

La pubblicazione sul sito istituzionale e la comunicazione tramite registro elettronico sono canali adeguati se assicurano accessibilità, tempestività e prova della messa a disposizione. La presa visione non equivale necessariamente a consenso e non trasforma il trattamento istituzionale in trattamento basato sul consenso. Gli interessati esercitano i diritti rivolgendosi alla scuola quale Titolare; il Titolare utilizza le funzioni del servizio e richiede l’assistenza di Google quando necessaria ai sensi del DPA.

La scuola non deve promettere una cancellazione assoluta in ogni caso: accesso, rettifica, limitazione, opposizione e cancellazione sono gestiti in base alle condizioni e ai limiti previsti dal GDPR e alla natura della documentazione pubblica. La rettifica di informazioni valutative deve avvenire con modalità idonee a preservare tracciabilità e correttezza dell’atto/documento, senza alterare impropriamente la documentazione amministrativa.

10. Misure tecniche e organizzative

Le misure di seguito indicate costituiscono il livello minimo atteso per rendere accettabile il rischio residuo. Le misure riferite nella bozza originaria come già attive (restrizione servizi, controllo accessi, formazione, backup, cifratura client-side, policy di data breach e blocco della geolocalizzazione) devono essere verificate e supportate da evidenze. Non si attribuisce loro efficacia finché non siano confermate dal responsabile tecnico/amministratore e dal Titolare.

Area	Misura richiesta	Evidenza da conservare

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

Area	Misura richiesta	Evidenza da conservare
Governance dei servizi	Inventario dei servizi attivi; attivazione per gruppi/organizzazioni; disabilitazione di servizi non necessari e dei servizi aggiuntivi per impostazione predefinita.	Esportazione/screenshot della Console; elenco dei servizi e data verifica.
Identità e accessi	Account nominativi, privilegi minimi, MFA per amministratori e utenti ove disponibile/appropriata, account amministrativi separati, revisione periodica accessi, disattivazione tempestiva.	Configurazione MFA; elenco amministratori; verbale revisione utenti/gruppi.
Condivisione	Limitare condivisione esterna/pubblica; impedire “chiunque abbia il link” salvo autorizzazione puntuale; controllare gruppi e permessi; revisione dei drive condivisi.	Policy sharing; report condivisioni; test periodici e log delle verifiche.
Dati ad alta riservatezza	Minimizzare dati particolari; vietarli in spazi didattici aperti; repository separato con accessi ristretti; cifratura aggiuntiva ove necessaria; gestione delle chiavi fuori dalla piattaforma se richiesta come misura effettiva.	Istruzioni scritte; struttura cartelle e ACL; evidenza tecnica della cifratura e della gestione delle chiavi.
Meet e contenuti multimediali	Registrazione, trascrizione, sottotitoli e funzioni AI disabilitati per default ove non necessari; controllo accesso, informativa e retention se autorizzati.	Impostazioni Meet; istruzioni per docenti; log delle autorizzazioni.
Log, monitoraggio e incidenti	Attivare i log disponibili nell’edizione; definire chi li consulta e per quanto; procedura di risposta agli incidenti; canale immediato di segnalazione; registro incidenti e data breach.	Procedura; test/tabletop annuale; prova accesso al pannello e retention log.
Dispositivi e rete	Aggiornamenti, antimalware, blocco schermo, cifratura device ove possibile, gestione BYOD, divieto di dispositivi/account condivisi senza adeguate misure.	Policy dispositivi; controlli aggiornamento; istruzioni utenti.
Backup e continuità	Esportazioni periodiche o backup indipendente dei dati istituzionali necessari; test di ripristino; verifica che il backup non estenda impropriamente la retention.	Piano backup; log e risultato test di ripristino.
Terze parti	Controllo di marketplace, estensioni e applicazioni OAuth/API; whitelist e approvazione preventiva; revoca delle app inutilizzate.	Elenco app autorizzate; report autorizzazioni; verbale review.
Formazione e supervisione	Formazione iniziale e periodica per docenti, personale e utenti; regole sulla condivisione, phishing, immagini/audio/video, categorie particolari e cyberbullismo.	Registro formazione; istruzioni e regolamento aggiornati.
Cancellazione e retention	Retention per categoria; revisione account inattivi; processo di export, disattivazione, cancellazione e controllo delle copie.	Piano conservazione; ticket/log di cancellazione; check annuale.
Contratti e sub-responsabili	Verificare DPA, Service Data Addendum, lista sub-responsabili, regione dati e canali di notifica degli incidenti.	Contratti accettati; copie datate; verbale di valutazione fornitori.

11. Valutazione dei rischi

11.1 Metodo

La stima è espressa con scala qualitativa/quantitativa a 4 livelli. Gravità (G): 1 trascurabile; 2 limitata; 3 significativa; 4 grave. Probabilità (P): 1 rara; 2 poco probabile; 3 probabile; 4 molto probabile. Il punteggio è G × P. Classificazione: 1-3 basso; 4-7 medio; 8-11 alto; 12-16 molto alto. Le stime sono valutazioni iniziali ragionate e non risultano da statistiche di incidenti dell’istituto. Il rischio residuo indicato è un obiettivo subordinato alla verifica delle misure e deve essere aggiornato se le evidenze non confermano i controlli.

Scenario e impatto principale	Rischio iniziale G×P	Misure determinanti	Rischio residuo obiettivo G×P / condizione
R1. Condivisione errata, link pubblico o permessi eccessivi: divulgazione di elaborati, email o dati di minori a compagni, soggetti esterni o pubblico.	4×3 = 12 Molto alto	Restrizione condivisioni esterne/pubbliche; permessi specifici; revisione gruppi/drive; formazione; audit periodici.	4×1 = 4 Medio
R2. Compromissione account (phishing, password riutilizzata, sessione non protetta) e accesso ai contenuti.	4×3 = 12 Molto alto	MFA, privilegi minimi, amministratori separati, gestione sessioni e recupero account, logging e formazione.	4×1 = 4 Medio
R3. Inserimento eccessivo di dati particolari o altamente riservati in spazi non segregati.	4×3 = 12 Molto alto	Minimizzazione; divieto ordinario; repository separato; autorizzazioni ristrette; cifratura aggiuntiva e base giuridica specifica.	4×1 = 4 Medio
R4. Accesso di app di terze parti o Servizi aggiuntivi con differenti condizioni e raccolta più ampia di dati.	4×3 = 12 Molto alto	Disabilitare di default; approvazione preventiva; controllo OAuth/API; consenso parentale previsto dai termini Google per servizi aggiuntivi e utenti <18 anni.	4×1 = 4 Medio

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

Scenario e impatto principale	Rischio iniziale G×P	Misure determinanti	Rischio residuo obiettivo G×P / condizione
R5. Trasferimenti internazionali, accesso da parte di sub-responsabili o richieste legali di autorità estere.	4×2 = 8 Alto	Verifica del DPF dove applicabile; SCC/soluzione alternativa secondo il DPA; elenco e località dei sub-responsabili; minimizzazione e misure supplementari proporzionate.	3×2 = 6 Medio
R6. Indisponibilità/perdita di file o impossibilità di recuperare contenuti necessari alla valutazione e all'attività scolastica.	3×2 = 6 Medio	Esportazioni/backup indipendente per documenti critici; test di ripristino; procedura di continuità e trasferimento all'archivio ufficiale.	3×1 = 3 Basso
R7. Modifica o cancellazione non autorizzata di elaborati e documenti con impatto sulla correttezza della valutazione o sulla tracciabilità.	3×2 = 6 Medio	Permessi distinti modifica/lettura; cronologia versioni dove disponibile; esportazione della versione definitiva; archivio controllato e log.	3×1 = 3 Basso
R8. Registrazione/trascrizione di incontri, immagini o audio raccolti oltre la necessità e conservati troppo a lungo.	3×3 = 9 Alto	Funzioni off di default; autorizzazione puntuale; informazione preventiva; accesso ristretto; retention e cancellazione definite.	3×1 = 3 Basso
R9. Cancellazione tardiva, esportazione incompleta o permanenza degli account dopo la cessazione della finalità.	3×3 = 9 Alto	Piano di retention; finestre di esportazione; trasferimento agli archivi previsti; disattivazione e cancellazione; considerazione dei tempi tecnici contrattuali Google.	3×1 = 3 Basso
R10. Trattamento dei dati di servizio e possibile divergenza dei ruoli/finalità non rappresentata all'utenza.	4×3 = 12 Molto alto	Verifica/decisione sul Service Data Addendum; aggiornamento informativa; mappatura dei ruoli e delle finalità autonome limitate di Google.	3×2 = 6 Medio
R11. Uso di Gemini for Education/Gemini Notebook o altra funzione AI fuori perimetro, con inserimento di dati personali e output non accurati.	4×3 = 12 Molto alto se attivo	Esclusione dal perimetro fino a decisione formale; se previsto, DPIA integrativa, verifica termini, impostazioni, età, dati inseriti, conservazione, supervisione umana e regole sull'uso di AI.	Non stimabile per questa DPIA. Non abilitare prima di valutazione separata e aggiornamento del documento.

12. Piano di trattamento e azioni prioritarie

N.	Azione	Responsabile	Priorità / evidenza di completamento
1	Inventario servizi/feature: esportare l'elenco dei servizi attivi e delle funzioni Meet; identificare utenti/OU e app collegate.	Amministratore Workspace / Team digitale	Immediata, prima dell'approvazione; report datato della Console.
2	Disabilitare servizi aggiuntivi e applicazioni di terze parti non autorizzati; fissare procedura per richieste di attivazione.	Dirigente + Amministratore	Immediata; policy di accesso e lista autorizzazioni.
3	Verificare contratto Education accettato, DPA incorporato, parte contraente, licenza, addendum e versione dei termini.	DS / DSGA / ufficio competente	Alta; copia contrattuale e schermata/evidenza di accettazione.
4	Decidere e documentare il trattamento dei dati di servizio e l'eventuale accettazione del Service Data Addendum; aggiornare informativa.	Titolare con consulenza DPO	Alta; decisione scritta, testo applicabile, informativa aggiornata.
5	Verificare DPF di Google LLC, meccanismi applicabili ad altri trasferimenti e sub-responsabili, sedi e notifiche.	Titolare / Amministratore / DPO consultato	Alta e poi annuale; stampa PDF o verbale di controllo datato.
6	Testare MFA, privilegi amministrativi, condivisione esterna, link pubblici, recovery account, log e alert.	Amministratore Workspace	Alta; checklist tecnica con esiti test.
7	Approvare piano di retention e uscita: esportazione, deposito nel repository ufficiale, disattivazione, cancellazione e copie.	DS / DSGA / responsabili archivio	Alta; procedura con tempi per categoria e test di un account.
8	Aggiornare regolamento piattaforma e istruzioni: contenuti vietati, dati particolari, immagini/registrazioni, AI, app terze parti, cyberbullismo.	DS con Team digitale e DPO consultato	Alta; atto interno aggiornato e comunicato agli utenti.
9	Rendere l'informativa specifica, accessibile e comprensibile; includere categorie dei servizi, dati di servizio, trasferimenti, retention e diritti.	Titolare / DPO consultato	Prima dell'uso o dell'aggiornamento dei servizi; copia e prova di pubblicazione/comunicazione.
10	Erogare formazione periodica e provare procedura data breach/continuità.	DS / referenti designati	Almeno annuale; registri formativi e verbale di test.
11	Formalizzare valutazione periodica e riesame della DPIA; aggiornare a ogni nuova funzionalità, servizio, licenza o modifica contrattuale.	Titolare	Annuale e su evento; verbale di riesame e versioning.

FGIC878001 - A7AD0F7 - REGISTRO PROTOCOLLO - 0009119 - 21/10/2026 - I.4 - U

13. Consultazione degli interessati e ruolo del DPO

Ai sensi dell'art. 35, par. 9, GDPR, il Titolare valuta, ove opportuno, la raccolta delle opinioni degli interessati o dei loro rappresentanti, fatti salvi i casi in cui ciò pregiudicherebbe interessi pubblici o commerciali o sia sproporzionato/impraticabile. La scelta di non consultare gli interessati deve essere motivata nel fascicolo DPIA: l'argomento non può limitarsi al solo interesse istituzionale all'adozione dello strumento. In ragione della presenza di alunni minorenni, si raccomanda almeno di rendere disponibili informativa e regolamento in linguaggio comprensibile, raccogliere osservazioni tramite canali già utilizzati dalla scuola e documentare le risposte/criticità significative.

Il DPO/RPD è consultato ai sensi degli artt. 35, par. 2, e 39 GDPR e fornisce consulenza indipendente; la responsabilità della DPIA, delle scelte di finalità/mezzi, dell'implementazione delle misure e della decisione sul rischio residuo resta in capo al Titolare. Il parere del DPO deve essere documentato, comprese le eventuali osservazioni non accolte e la motivazione del Titolare.

14. Conclusioni e decisione del Titolare

Sulla base della documentazione esaminata e della valutazione effettuata, l'utilizzo di Google Workspace for Education per scopi didattici limitati può essere considerato proporzionato in presenza di un inventario dei servizi, un contratto applicabile con garanzie ex art. 28 GDPR, una gestione trasparente dei dati di servizio, meccanismi di trasferimento verificati, controlli di accesso e condivisione efficaci, misure specifiche per i dati particolari, retention definita e procedure di esportazione/cancellazione.

Questa conclusione è condizionata: allo stato non è possibile confermare come fatto che le misure descritte nella bozza originaria siano tutte operative, che l'elenco dei servizi attivi corrisponda al perimetro assunto, che il DPA/Service Data Addendum siano stati accettati nella versione pertinente o che le impostazioni di trasferimento e condivisione siano configurate come dichiarato. Il Titolare deve completare il piano di azione, conservare le evidenze e approvare una versione aggiornata della valutazione. Fino a tale verifica, la qualificazione dei rischi residui come bassi o medi resta un obiettivo e non un accertamento.

Il Dirigente Scolastico
Prof. Pietro Loconte