I.I.S. G. GANGALE – CIRÒ MARINA (KR)
P.zza Kennedy, 10 – 88811 Cirò Marina (KR) | kris00400c@istruzione.it

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Utilizzo di servizi di Intelligenza Artificiale generici autorizzati dall'Istituto

Documento n.	DPIA-IA-01/2025
Versione	2.0 – aggiornata
Data di emissione	Settembre 2025
Data aggiornamento	Maggio 2026
Titolare del trattamento	I.I.S. G. Gangale – Dirigente Scolastica
Redatta da	DPO d'Istituto
Approvata da	Dirigente Scolastica
Classificazione	Documento interno riservato

KRIS00400C - AC25CBA - REGISTRO PROTOCOLLO - 0006401 - 17/06/2026 - I - U

1. Oggetto della valutazione

La presente DPIA valuta i rischi per i diritti e le libertà delle persone fisiche derivanti dall'eventuale utilizzo, da parte del personale docente e amministrativo dell'I.I.S. G. Gangale, di servizi di Intelligenza Artificiale (IA) generici – ossia strumenti IA non riconducibili alle piattaforme istituzionali Google Workspace for Education – preventivamente autorizzati dal Dirigente Scolastico su parere del DPO e inseriti nell'Elenco degli Strumenti IA Autorizzati dell'Istituto.

L'utilizzo di tali strumenti è finalizzato a:

- supporto alla preparazione di materiali didattici e attività di classe;
- supporto alla produzione di comunicazioni e documenti amministrativi;
- ricerca, sintesi e organizzazione di informazioni a fini professionali;
- sperimentazione didattica e aggiornamento professionale.

PERIMETRO	La presente DPIA si applica esclusivamente agli strumenti inseriti nell'Elenco degli Strumenti IA Autorizzati dell'Istituto (doc. ELENCO-IA-01). L'utilizzo di strumenti non autorizzati è vietato (Regolamento IA, Art. 4; PIA, Sez. 6). Per ciascun nuovo strumento non ancora inserito nell'Elenco, il DPO effettua una valutazione preliminare prima dell'autorizzazione.

2. Introduzione e necessità della DPIA

2.1 Riferimenti normativi

Riferimento normativo	Pertinenza
GDPR – Reg. UE 2016/679, art. 35	Obbligo di DPIA per trattamenti ad alto rischio

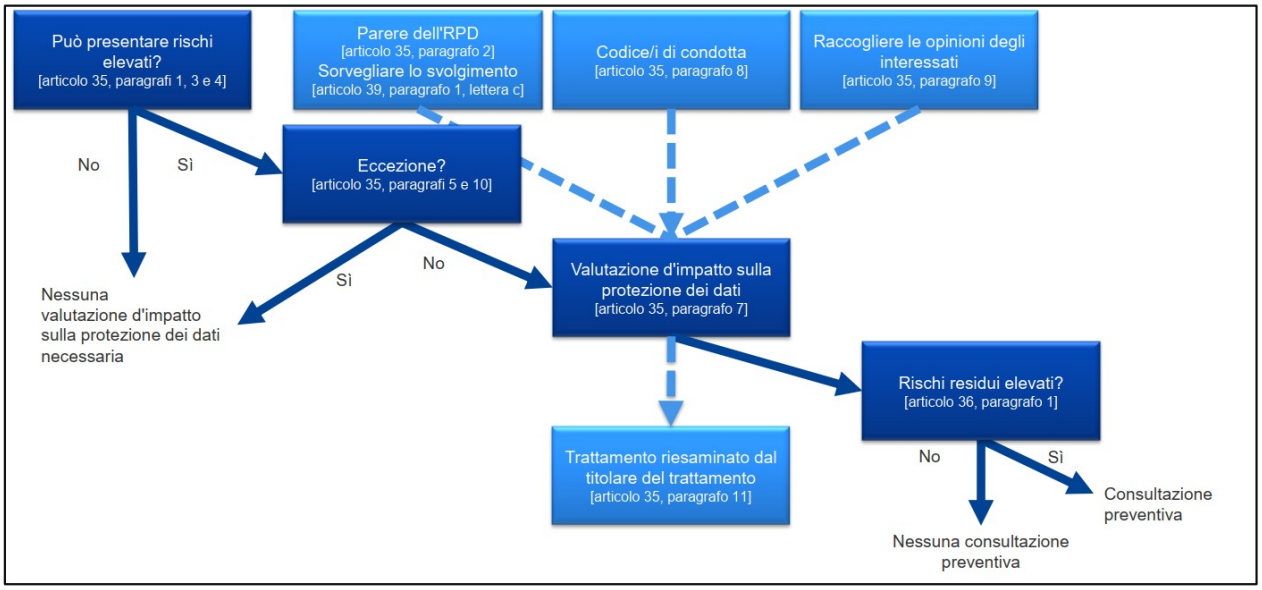
AI Act – Reg. UE 2024/1689	Classificazione dei sistemi IA per livello di rischio
D.Lgs. 196/2003 e s.m.i.	Codice Privacy italiano
Linee guida MIM – D.M. 166/2025	Uso dell'IA nelle istituzioni scolastiche
CAD – D.Lgs. 82/2005	Digitalizzazione PA
PIA d'Istituto – A.S. 2025/2026	Documento strategico interno di riferimento
Regolamento IA d'Istituto	Normativa interna di governance IA

2.2 Criteri di obbligatorietà della DPIA

Ai sensi dell'art. 35 GDPR e delle Linee guida del Gruppo Art. 29 (WP248), la DPIA è obbligatoria quando il trattamento soddisfa almeno due dei seguenti criteri. Il presente trattamento soddisfa i seguenti:

Criterio WP248	Applicabile?
Uso di nuove tecnologie (sistemi IA generativi)	SÌ
Trattamento di dati di soggetti vulnerabili (minori, dipendenti)	SÌ – personale e potenzialmente studenti
Valutazione o scoring di persone fisiche	PARZIALE – esclusa per policy interna (PIA Sez. 3)
Trattamento su larga scala	NO – uso limitato al personale autorizzato
Decisioni automatizzate con effetti giuridici	NO – principio human-in-the-loop (PIA Sez. 2)

	La DPIA è obbligatoria in quanto il trattamento soddisfa almeno due criteri WP248: utilizzo di nuove tecnologie (IA generativa) e trattamento di dati di soggetti vulnerabili (personale dipendente e, indirettamente, studenti). La valutazione è disposta ai sensi dell'art. 35 GDPR e del PIA d'Istituto, Sez. 6.



La presente DPIA ha lo scopo di:

- analizzare in modo sistematico i trattamenti di dati personali connessi all'utilizzo dei servizi di Intelligenza Artificiale
- valutare la **necessità e proporzionalità** dei trattamenti rispetto alle finalità educative e istituzionali
- individuare i **rischi per i diritti e le libertà degli interessati**, con particolare riferimento agli **alunni minorenni**
- definire e valutare l'efficacia delle **misure tecniche e organizzative** adottate o da adottare
- determinare il **livello di rischio residuo** e la sua accettabilità

1.1 Processo di valutazione

Il processo che porta alla valutazione del rischio prevede alcune fasi, così riassunte:

Fase 1: identificazione dei trattamenti
Consiste nell'individuare tutti gli elementi del trattamento dati:

- Tipologia di dati
- Finalità
- Categorie di interessati
- Modalità di trattamento
- Misure tecniche/organizzative
- Destinatari
- Eventuale trasferimento extra UE
- **Fase 2: Panoramica dei rischi**
- Vengono individuati i potenziali rischi, cioè la probabilità con cui un evento dannoso possa verificarsi, e le relative conseguenze, determinando una scala di probabilità del rischio che va da "improbabile" a "quasi certo" e una scala di incidenza delle conseguenze che va da "trascurabili" a "gravissime".
- **Fase 3: Valutazione del rischio ed eventuali misure correttive**
- Si valutano rischi e conseguenze, determinando l'esito della DPIA.

3. Descrizione del trattamento e del contesto

3.1 Titolare del trattamento

Elemento	Dettaglio
Titolare	I.I.S. G. Gangale – Istituzione scolastica
Rappresentante legale	Dirigente Scolastica
Indirizzo	P.zza Kennedy, 10 – 88811 Cirò Marina (KR)
Codice Meccanografico	KRIS00400C
PEC	kris00400c@pec-istruzione.it

3.1 Servizi di Intelligenza Artificiale oggetto della DPIA

Il Responsabile del trattamento è il soggetto che tratta i dati per conto del Titolare, sulla base di un contratto o altro atto giuridico conforme all'art. 28 GDPR.

La tabella seguente riporta i requisiti minimi che il fornitore deve soddisfare per essere autorizzato

Requisito	Dettaglio richiesto
Identificazione fornitore	Ragione sociale, sede legale, paese di stabilimento
Contratto art. 28 GDPR	Data Processing Agreement (DPA) o equivalente firmato
Inserimento lista ACN/AgID	Verifica nell'elenco SaaS qualificati ACN (ex AgID)
Data Privacy Framework UE-USA	Certificazione DPF se il fornitore trasferisce dati verso USA
Registro dei Responsabili	Iscrizione nel Registro dei Responsabili del Trattamento dell'Istituto
Non utilizzo dati per addestramento	Dichiarazione contrattuale esplicita (Reg. IA Art. 15 lett. g; PIA Sez. 6)

Prima di autorizzare qualsiasi strumento IA generico, il DPO verifica la sussistenza di tutti i requisiti sopra elencati e identifica nominalmente il Responsabile del trattamento. Lo strumento viene inserito nell'Elenco degli Strumenti Autorizzati solo dopo questa verifica (PIA, Sez. 5 e Sez. 6).

3.3 Altri soggetti coinvolti

Soggetto	Ruolo nel trattamento
Personale docente e ATA	Utilizzatori degli strumenti – inseriscono prompt e verificano gli output
DPO d'Istituto	Verifica preventiva, supervisione DPIA, consulenza al Titolare
Referente IA	Supporto tecnico-pedagogico, raccordo con il Gruppo IA
Gruppo di Lavoro IA	Valutazione preliminare degli strumenti, proposta di autorizzazione al DS
Dirigente Scolastica	Autorizzazione finale degli strumenti, aggiornamento DVR
Amministratori di sistema	Gestione degli account istituzionali per i servizi IA autorizzati
Studenti	Non utilizzatori diretti – indirettamente coinvolti quando il personale prepara materiali

3.4 Categorie di dati trattati

Categoria di dato	Trattato?
Dati identificativi del personale (nei prompt)	NO – vietato da policy (PIA Sez. 6)
Dati identificativi degli studenti (nei prompt)	NO – vietato da policy (PIA Sez. 6)
Dati di log e metadati di utilizzo	SÌ – account istituzionale utilizzato per l'accesso
Dati relativi al contenuto dei prompt	SÌ – il testo inserito costituisce dato personale se riferibile a persona
Dati sensibili (salute, origine etnica, ecc.)	ASSOLUTAMENTE NO – vietato da policy (PIA Sez. 6; GDPR art. 9)
Dati biometrici o di riconoscimento	ASSOLUTAMENTE NO – vietato da PIA Sez. 3 e AI Act

3.5 Finalità e base giuridica del trattamento

Finalità	Base giuridica (GDPR art. 6)

Supporto alla didattica e alla preparazione di materiali	Art. 6, par. 1, lett. e – esecuzione di compito di interesse pubblico
Supporto all'attività amministrativa e burocratica	Art. 6, par. 1, lett. e – esecuzione di compito di interesse pubblico
Aggiornamento professionale del personale	Art. 6, par. 1, lett. c – adempimento di obbligo legale (formazione)
Ricerca e sintesi di informazioni a fini istituzionali	Art. 6, par. 1, lett. e – esecuzione di compito di interesse pubblico

4. Verifica di conformità all'AI Act – Allegato III (PIA Sez. 3)

Il PIA d'Istituto (Sez. 3 – Regole e limitazioni) elenca esplicitamente le categorie di strumenti vietati nell'ambiente scolastico, corrispondenti alle categorie ad alto rischio dell'Allegato III dell'AI Act (Reg. UE 2024/1689). La loro esclusione è condizione necessaria per l'autorizzazione di qualsiasi strumento IA generico.

La tabella seguente riporta la verifica sistematica di ogni categoria rilevante dell'AI Act – Allegato III rispetto all'uso ammesso dall'Istituto per i servizi IA generici.

Categoria AI Act	Applicabile?	Motivazione
Sistemi di valutazione automatica degli studenti (All. III, p. 3)	**NO – VIETATO da PIA**	Il PIA (Sez. 3) vieta esplicitamente sistemi automatici di valutazione. Lo strumento non deve includere funzionalità di scoring o grading automatico.
Sistemi di profilazione di studenti e famiglie (All. III, p. 5)	**NO – VIETATO da PIA**	Il PIA (Sez. 3) vieta la profilazione di studenti e famiglie. Lo strumento non deve costruire profili comportamentali o predittivi.
Riconoscimento biometrico, facciale o delle emozioni (All. III, p. 1)	**NO – VIETATO da PIA**	Il PIA (Sez. 3) vieta riconoscimento emozioni, facciale ed elaborazione biometrica. Lo strumento non deve acquisire o elaborare dati biometrici.
Proctoring automatico degli esami (All. III, p. 3)	**NO – VIETATO da PIA**	Il PIA (Sez. 3) vieta il proctoring automatico. Lo strumento non deve sorvegliare automaticamente lo svolgimento di prove valutative.
Sistemi di IA generale (GPAI) – uso generico assistito	**SÌ – ammesso con misure**	Lo strumento rientra nella categoria GPAI (es. modelli di linguaggio generativi) utilizzati per scopi di supporto didattico/amministrativo. Non rientra nell'Allegato III. Soggetto alle misure di mitigazione della presente DPIA.

4.1 Procedura di verifica per nuovi strumenti

Per ciascun nuovo strumento IA generico candidato all'autorizzazione, il DPO – con il supporto del Referente IA e del Gruppo di Lavoro IA – verifica che:

- lo strumento non includa, come funzionalità principale o accessoria, capacità riconducibili alle categorie vietate del PIA Sez. 3 e dell'Allegato III AI Act;
- le condizioni d'uso (Terms of Service) e la documentazione tecnica del fornitore escludano esplicitamente l'uso per valutazione automatica, profilazione o riconoscimento biometrico;
- le impostazioni di utilizzo adottate dall'Istituto disabilitino eventuali funzionalità opzionali riconducibili alle categorie vietate.

I servizi IA generici autorizzati dall'Istituto rientrano nella categoria GPAI (modelli di IA di uso generale) e non nell'Allegato III AI Act, a condizione che siano utilizzati esclusivamente nelle modalità indicate nella presente DPIA e nelle Linee guida operative. Funzionalità non conformi al PIA non possono essere attivate.

L’obiettivo è dunque quello di formare gli alunni ad un consapevole e funzionale uso delle tecnologie digitali, per poter guidare i più piccoli e preparare i più grandi verso un percorso di studi universitari e/o un mondo del lavoro che richiede competenze e capacita digitali. Del trattamento sono esplicitamente informati gli interessati con specifica informativa, che definisce tutti gli aspetti del trattamento e la legittimità dello stesso da parte del titolare, il quale agisce per il perseguimento di finalità istituzionali connesse all’esecuzione di un

compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Nell'ambito di tali finalità, il titolare definisce quali dati trattare e con quali strumenti, e questa DPIA è volta a valutare proprio il rischio di tale scelta.

4.2 Basi giuridiche che rendono lecito il trattamento

L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Nello specifico, la scuola organizza la propria attività per lo svolgimento, primariamente, degli obiettivi prefissati nel PTOF (Piano Triennale dell'Offerta Formativa), che rappresenta il documento identificativo della scuola e contiene un'indicazione chiara e dettagliata di obiettivi, linea d'azione e mezzi a disposizione per raggiungerli. Agisce poi in conformità del CAD (Codice dell'Amministrazione Digitale), il quale prevede e promuove l'uso delle nuove tecnologie nella PA per le attività amministrative e organizzative, e delle Linee guida MIM per l'IA.

4.3 Caratteristiche dei dati trattati

I dati personali trattati tramite l'utilizzo della piattaforma cloud e dei servizi IA sono nominativo (presente nell'account di accesso), altri come log di accesso, indirizzo IP o identificativi del dispositivo, eventi di sicurezza, impostazioni e metadati. I dati trattati, seppur limitati più possibile rispetto alle finalità, consentono di identificare l'utente in considerazione del nominativo inserito nell'account individuale, assegnato ad ogni interessato per poter identificare in maniere univoca l'utente all'interno della piattaforma. Non vengono gestiti dati sensibili né documenti che possano ricondurre a tale categoria di dati.
I dati vengono verificati e aggiornati periodicamente, eliminando gli utenti non più operativi, archiviando/cancellando i file non più pertinenti. Eventuali segnalazioni di rettifica da parte degli interessati vengono prese in carico dall'amministratore della piattaforma, dopo averne verificato l'attendibilità e applicabilità.
La conservazione dei dati è effettuata per il periodo necessario al perseguimento delle finalità. Successivamente, per i documenti rilevanti ai fini didattici/amministrativi, si procede all'archiviazione dai dati per il tempo previsto dalla normativa di riferimento. Per i documenti che costituiscono prove di valutazione, ad esempio, l'archiviazione ha la durata di almeno un anno e comunque deve rispettare i tempi previsti dalla circolare n.44 del 2005 della Direzione Generale degli Archivi. Altri tipi di prove e documenti, possono essere archiviati fino alla fine dell'anno scolastico o del percorso in cui si inserisce il documento.

5. Disciplina degli AI Agent (PIA Sez. 4)

Il PIA d'Istituto (Sez. 4 – AI Agent e automazione) stabilisce che gli agenti autonomi sono 'utilizzabili solo previa autorizzazione del Dirigente' e devono essere 'sempre supervisionati da un adulto competente', e che 'non possono accedere ad aree contenenti dati sensibili'.

5.1 Definizione di AI Agent ai fini della presente DPIA

Ai fini della presente DPIA, si definisce AI Agent (agente autonomo) qualsiasi sistema IA che:

- agisce in modo autonomo su piattaforme, sistemi o applicazioni (es. esegue ricerche, invia richieste, accede a file, compila moduli) senza intervento umano passo dopo passo;
- opera in modalità multi-step, pianificando e concatenando azioni in sequenza per raggiungere un obiettivo;
- può interagire con altri sistemi informatici o dati dell'Istituto in modo non supervisionato.

5.2 Utilizzo di AI Agent nell'ambito della presente DPIA

Scenario	Regime applicabile
Strumento IA generico usato in modalità chat/prompt-risposta (senza autonomia operativa)	AMMESSO – rientra nell'utilizzo standard coperto dalla presente DPIA

Strumento IA con funzionalità agente attivata (es. accesso a file, navigazione web autonoma, invio email)	SOGGETTO A AUTORIZZAZIONE SPECIFICA del DS prima di ogni attivazione
Agente autonomo che accede a dati sensibili dell'Istituto (registro elettronico, PEI, PDP, fascicoli personali)	VIETATO – non autorizzabile ai sensi del PIA Sez. 4

5.3 Procedura di autorizzazione per l'uso agentivo

1. Il personale che intende utilizzare uno strumento IA in modalità agente (con autonomia operativa) deve **presentare richiesta scritta al Referente IA**, descrivendo la funzionalità da attivare, i sistemi a cui l'agente accederà e le misure di supervisione previste.
2. Il Referente IA, con il supporto del DPO, valuta la richiesta rispetto al PIA Sez. 4 e alle prescrizioni della presente DPIA.
3. Il Dirigente Scolastico autorizza per iscritto l'attivazione della funzionalità agentiva, specificando le condizioni di utilizzo e il supervisore adulto responsabile.
4. L'autorizzazione è specifica per funzionalità e strumento: non è trasferibile ad altri strumenti o modalità d'uso.
5. Ogni sessione agentiva autorizzata deve essere supervisionata in tempo reale da un adulto competente designato.

In nessun caso un AI Agent può operare in autonomia completa su dati dell'Istituto, dei docenti o degli studenti. Il principio 'human-in-the-loop' del PIA (Sez. 2) si applica a maggior ragione all'uso agentivo degli strumenti IA.

5.4 Trasferimento dati al di fuori dell'Unione Europea (verso gli USA)

La Commissione Europea, in virtù dei negoziati tra UE e USA che hanno portato all'adozione dell'accordo UE-USA Data Privacy Framework, è giunta alla conclusione che gli Stati Uniti garantiscono un livello di protezione adeguato comparabile a quello dell'Unione europea, con protezioni e garanzie sufficienti sul trattamento dei dati personali. Sulla base della nuova decisione di adeguatezza, i dati personali possono circolare in modo sicuro dall'UE verso le imprese statunitensi che partecipano al quadro, senza la necessità di ulteriori garanzie per la protezione dei dati.

6. Principi fondamentali del trattamento

6.1 Principi GDPR applicati

Principio GDPR	Applicazione nel trattamento
Liceità, correttezza e trasparenza	Base giuridica identificata; informativa pubblicata sul sito e comunicata al personale
Limitazione della finalità	Uso esclusivo per le finalità istituzionali indicate nella Sez. 3.5
Minimizzazione dei dati	Divieto di inserire dati personali identificativi nei prompt; uso anonimizzato
Esattezza	Verifica umana obbligatoria di ogni output prodotto dallo strumento (human-in-the-loop)
Limitazione della conservazione	I dati non vengono conservati dall'Istituto oltre le finalità; verifica contrattuale dei tempi di retention del fornitore
Integrità e riservatezza	Accesso tramite account istituzionale; misure di sicurezza tecniche e organizzative
Responsabilizzazione	Documentazione del trattamento, DPIA, formazione del

	personale, monitoraggio

6.2 Trasferimento dei dati verso paesi terzi

Alcuni fornitori di strumenti IA generici possono avere sede o infrastrutture negli Stati Uniti o in altri paesi terzi. Il trasferimento di dati verso tali paesi è ammesso solo se:

- il fornitore è certificato nell'ambito del Data Privacy Framework UE-USA (decisione di adeguatezza Commissione UE, 10 luglio 2023); oppure
- il trasferimento è coperto da Clausole Contrattuali Standard (SCC) adottate dalla Commissione UE; e
- il DPO ha verificato e documentato la garanzia applicabile prima dell'autorizzazione dello strumento.

7. Misure a tutela degli interessati

7.1 Informativa agli interessati

- Informativa sul trattamento dei dati personali pubblicata sul sito web istituzionale (sezione Privacy/IA);
- Comunicazione ai docenti e al personale ATA tramite registro elettronico e circolare interna;
- Informativa specifica per studenti e famiglie pubblicata sul sito e consegnata all'inizio dell'anno scolastico.

7.2 Diritti degli interessati

Ai sensi degli artt. 15-23 GDPR, gli interessati possono esercitare i propri diritti (accesso, rettifica, cancellazione, limitazione, opposizione, portabilità) contattando il Titolare del trattamento o il DPO ai recapiti indicati nell'informativa. I diritti possono essere esercitati anche nei confronti del Responsabile del trattamento (fornitore dello strumento), nei limiti del contratto art. 28 GDPR.

7.3 Misure tecniche e organizzative

Misura	Descrizione
Account istituzionale obbligatorio	L'accesso agli strumenti IA avviene esclusivamente tramite account istituzionale dell'Istituto; sono vietati account personali
Minimizzazione degli input	Divieto assoluto di inserire nei prompt: nomi di studenti, voti, diagnosi, PEI/PDP, dati sensibili o identificativi di persone fisiche
Anonimizzazione/ pseudonimizzazione	Quando necessario riferirsi a situazioni reali, utilizzare descrizioni anonimizzate (es. 'uno studente con difficoltà in matematica', non il nominativo)
Verifica umana degli output	Ogni output prodotto dallo strumento deve essere verificato, validato e – se necessario – corretto da un adulto responsabile prima di qualsiasi uso (human-in-the-loop)
Contratto art. 28 GDPR	Stipula di DPA con il fornitore prima dell'autorizzazione; verifica dell'eventuale clausola di non utilizzo dei dati per addestramento dei modelli
Dichiarazione obbligatoria uso IA	Il personale docente che utilizza strumenti IA nella produzione di materiali dichiara l'utilizzo nelle modalità previste dalle Linee guida
Formazione del personale	Partecipazione obbligatoria ai percorsi formativi previsti dal Piano di Formazione del PIA (Sez. 7)
Segnalazione incidenti	Ogni incidente di sicurezza o uso non conforme deve essere segnalato al DS e al DPO entro 24 ore dalla conoscenza

8. Raccordo con il DVR – Rischi IA sul luogo di lavoro (PIA Sez. 6)

Il PIA d'Istituto (Sez. 6 – Sicurezza e tutela dei dati) prescrive esplicitamente che 'il DVR viene aggiornato con i rischi IA: stress lavoro correlato, rischi psicosociali, dipendenze tecnologiche'. Questa responsabilità è attribuita al Dirigente Scolastico (PIA Sez. 5). La presente DPIA fornisce gli elementi informativi necessari a tale aggiornamento.

8.1 Rischi IA da integrare nel DVR

Tipologia di rischio IA (PIA Sez. 6)	Descrizione del rischio	Misura preventiva suggerita
Stress lavoro correlato	Utilizzo intensivo di strumenti IA che aumenta il carico cognitivo, genera dipendenza o crea aspettative di produttività non sostenibili	Formazione sull'uso consapevole; limiti di utilizzo raccomandati; monitoraggio del benessere del personale
Rischi psicosociali	Ansia da performance, sensazione di sostituzione professionale, perdita di autonomia decisionale, disorientamento nell'identità professionale	Coinvolgimento del personale nella governance IA; comunicazione trasparente sui limiti e le finalità degli strumenti; supporto psicologico
Dipendenze tecnologiche	Progressiva incapacità di svolgere attività didattiche o amministrative senza il supporto degli strumenti IA; riduzione delle competenze cognitive proprie	Alternanza programmata tra attività con e senza IA; valutazione periodica dell'impatto; attività di formazione critica

8.2 Procedura di aggiornamento del DVR

6. La presente DPIA, viene trasmessa alla Dirigente Scolastica e all'RSPP come documento informativo ai fini dell'aggiornamento del Documento di Valutazione dei Rischi (DVR).
7. L'RSPP, con il supporto del Referente IA e del DPO, integra nella sezione pertinente del DVR i rischi IA identificati nella tabella 8.1.
8. Il DVR aggiornato viene portato all'attenzione del Medico Competente (se nominato) e del Rappresentante dei Lavoratori per la Sicurezza (RLS).
9. Il monitoraggio dei rischi IA nel DVR è soggetto alla revisione annuale prevista dal PIA Sez. 8.

9. Valutazione del rischio

9.1 Metodologia

Il Livello di Rischio (LR) è calcolato come prodotto tra la Probabilità dell'evento (P) e il relativo Impatto (C – conseguenza), secondo la formula LR = P × C, con valori da 1 a 3 per ciascuna variabile:

Valore	Probabilità (P)	Conseguenze (C)
1	Improbabile	Lievi
2	Possibile	Moderate
3	Probabile	Gravi
4	CERTO	GRAVISSIME

LR	Livello di rischio	Azione richiesta e valori di riferimento

1-3	BASSO	Monitoraggio ordinario	1≥ LR ≤3
4-7	MEDIO	Misure di mitigazione rinforzate	4≥ LR ≤7
8-12	ALTO	Misure urgenti – rivalutare il trattamento	8≥ LR ≤12
13-16	ALTISSIMO	Misure immediate	13≥ LR ≤16

9.2 Scenari di rischio e misure di mitigazione

Scenario di rischio	P	C	LR=P×C	Misure di mitigazione
Inserimento accidentale di dati personali nei prompt	2	2	**4 – MEDIO**	Formazione obbligatoria; policy di minimizzazione; alert nei moduli d'uso; verifica trimestrale dal DPO
Utilizzo non autorizzato di strumenti non inseriti nell'Elenco	2	3	**6 – MEDIO**	Procedura di autorizzazione preventiva; comunicazione al personale; segnalazione obbligatoria; controlli periodici del Referente IA
Accesso illegittimo ai dati trattati tramite il fornitore	1	3	**3 – BASSO**	Contratto art. 28 GDPR; verifica DPF/SCC; clausola di non addestramento sui dati; cifratura dati in transito
Utilizzo di AI Agent non autorizzati	2	3	**6 – MEDIO**	Procedura di autorizzazione specifica (Sez. 5); divieto di attivazione autonoma; supervisione adulto competente; segnalazione obbligatoria
Output dell'IA non verificato utilizzato come documento ufficiale	2	3	**6 – MEDIO**	Principio human-in-the-loop; dichiarazione d'uso obbligatoria; formazione sulla verifica degli output; responsabilità professionale del firmatario
Rischi psicosociali e dipendenza tecnologica del personale	2	2	**4 – MEDIO**	Integrazione nel DVR (Sez. 8); formazione critica; monitoraggio benessere; supporto del Medico Competente

9.2 Misure esistenti o pianificate

Controllo degli accessi

Gli accessi logici degli utenti avvengono attraverso l'account individuale eventualmente assegnato ad ognuno ed autorizzato, con eventuali limitazioni in base alla tipologia di utente (docente, alunno). Gli account di utenti non più interessati del titolare (es. docenti non più in servizio o alunni che si trasferiscono) vengono disattivati.

Minimizzare la quantità di dati personali

I dati personali vengono minimizzati più possibile, compatibilmente con il perseguimento delle finalità e il raggiungimento degli obiettivi. Vengono acquisite dalla piattaforma una serie di informazioni, come ID del dispositivo, browser, sistema operativo, lingua selezionata, in parte classificabili come dati personali. Non vengono gestiti dati sensibili né documenti che possano ricondurre a tale categoria di dati.

Anonimizzazione dei dati

L'account può contenere in chiaro il nome dell'utente, per poter identificare in maniera univoca il soggetto all'interno della piattaforma. La gestione di account anonimi non sarebbe attuabile, perché non consentirebbe di effettuare sulla piattaforma il controllo degli accessi logici compromettendo la sicurezza della stessa. Vengono anonimizzati/pesudonimizzati i dati eventualmente contenuti in documenti condivisi, la cui natura non consente di indicare le informazioni in chiaro (circostanza rara e non prevista per il trattamento dati tramite la piattaforma e i servizi IA).

Misure di sicurezza informatica

I sistemi di sicurezza dei dispositivi in uso o in previsione d'uso presso e della scuola devono essere periodicamente verificati e aggiornati e devono essere dotati di antivirus, anti malware e firewall. I pc

amministrativi sono dotati di credenziali per l'accesso, mentre quelli dei laboratori ne sono sprovvisti per motivi ovvi (utilizzo trasversale da parte di tutti gli alunni), i quali tuttavia non contengono alcun tipo di documenti e informazioni, ma vengono solo utilizzati per attività didattiche ed esercitazioni. Le misure di sicurezza proprie della piattaforma sono attuate direttamente dal fornitore/responsabile del servizio.

Istruzioni agli operatori

Gli operatori sono stati istruiti sul corretto uso dei sistemi, attraverso attività informative, specifici regolamenti e linee guide rivolte a personale e alunni. Sono state fornite informazioni e indicazioni sia da un punto di tecnico, per il corretto uso dello strumento e delle funzioni messe a disposizione, sia da un punto di vista del trattamento dati, per un adeguato uso dei dati e dei documenti da poter condividere tramite la piattaforma e una corretta valutazione dei dati da escludere da questo tipo di trattamento. Le istruzioni e linee guida.

9.2.a Valutazione del rischio

L'analisi del rischio connessa all'impiego degli strumenti di Intelligenza Artificiale considerati si concentra sul rischio residuo, ossia su quei profili di pericolo che possono manifestarsi anche qualora l'uso delle applicazioni avvenga in assenza di un trattamento intenzionale di dati personali.
Il presupposto di base è che i servizi siano configurati e utilizzati in modalità senza dati, ma che permanga un margine fisiologico di rischio riconducibile prevalentemente al fattore umano, soprattutto in ambito scolastico.

Analisi dei rischi

>Inserimento non autorizzato o alterazione involontaria di dati personali

Origine del rischio

Il principale profilo di rischio individuato non deriva dal funzionamento intrinseco degli strumenti di IA, ma dalla condotta dell'utente finale.
In particolare, il rischio consiste nella possibilità che docenti o studenti, in modo non intenzionale o per errata valutazione, inseriscano nei prompt o nei materiali caricati dati personali, in contrasto con le istruzioni e i divieti impartiti dall'istituzione scolastica.
Tale evenienza è riconducibile esclusivamente ad errore umano, non a una carenza strutturale delle misure di sicurezza tecnologiche.

Misure di prevenzione e mitigazione

Per contenere tale rischio, l'istituzione scolastica ha predisposto un sistema integrato di misure organizzative e procedurali, fondato sui seguenti elementi:

- Il personale docente e amministrativo è destinatario di attività informative specifiche, con particolare riferimento alla minimizzazione, alla selezione consapevole delle informazioni e all'uso corretto degli strumenti di IA in ambito didattico.
- L'istituto ha previsto un Regolamento IA e delle Linee guida che vietano espressamente l'utilizzo di tool di IA per la redazione, l'analisi o il caricamento di documenti contenenti dati personali.
- Nei casi eccezionali in cui si renda necessario fare riferimento a situazioni riconducibili a persone fisiche, è previsto l'uso sistematico di tecniche di pseudonimizzazione o anonimizzazione, in modo da impedire l'identificazione diretta o indiretta degli interessati.
-

Valutazione del livello di rischio

- **Probabilità**
  L'eventuale inserimento di dati personali, in particolare se riferiti a minori o a categorie particolari di dati, è valutato come *Poco probabile (Livello P2)***,** in quanto sono state date chiare indicazioni sul divieto di inserimento di dati personali tramite la documentazione adottata, le informative, le linee guida
- **Conseguenze**
  Il *Poco probabile* inserimento di dati personali, in particolare se riferiti a minori o a categorie particolari di dati, è valutato come evento con *Conseguenze Gravi*

(Livello C3), in quanto potenzialmente idoneo a incidere sui diritti e sulle libertà fondamentali degli interessati.

- **Livello di rischio**
  Il livello di rischio LR risulta pari a 2 × 3 = 6, su una scala massima di 16, e può pertanto considerarsi contenuto e sotto controllo.

>Perdita dei contenuti generati o analizzati dall'Intelligenza Artificiale

Origine del rischio

Un ulteriore profilo di rischio riguarda la perdita dei contenuti prodotti o elaborati tramite gli strumenti di IA**,** quali sintesi, bozze di testi o materiali di supporto alla didattica.
Tali contenuti non costituiscono documentazione amministrativa ufficiale né atti soggetti a obblighi di conservazione a lungo termine e, pertanto, non beneficiano delle medesime garanzie previste per i documenti istituzionali**.**

Misure di prevenzione e mitigazione

Le Linee guida di Istituto sulla IA stabiliscono che:

- i docenti sono tenuti a verificare criticamente i contenuti prodotti dall'IA;
- nessun contenuto generato dall'IA è considerato valido o utilizzabile senza una preventiva revisione umana;
- nessuna dato personale deve essere inserito nei prompt e nei documenti allegati ai tool di IA.
-

Valutazione del livello di rischio

- **Probabilità**
  Considerate le modalità operative per l'uso di tool di IA, la probabilità è stimata come *Improbabile (Livello P1)***.**
- **Conseguenze**
  L'eventuale perdita di un prompt, di una bozza o di un elaborato preliminare è valutata come evento con *Conseguenze trascurabili* (Livello C1), in quanto non compromette la continuità dell'azione amministrativa né la missione istituzionale della scuola.
- **Livello di rischio**
  Il livello di rischio LR risulta pari a 1 × 1 = 1, su una scala massima di 16, e può pertanto considerarsi Poco rilevante.

>Accesso illegittimo ai dati

Origine del rischio

Il rischio di un accesso illegittimo ai dati può avvenire per cause dolose o colpose/accidentali, come cessione a terzi non autorizzati delle proprie credenziali di accesso, errata attribuzione dei permessi sulla piattaforma, azione dolosa di hackeraggio sulla piattaforma da parte di terzi.

Misure di prevenzione e mitigazione

Le misure tecniche e organizzative utili a mitigare il rischio di un accesso illegittimo sono quelle descritte nel corso di questa DPIA, e cioè (elenco in continuo aggiornamento):

- Impostazioni tecniche sulla piattaforma
- Formazione tecnica agli utenti
- Definizione delle policy
- Verifica periodi degli utenti attivi e di quelli da disattivare
- Minimizzazione dei dati
- Anonimizzazione e pseudonimizzazione se e quando necessario
- Periodici appelli per una corretta gestione delle credenziali di accesso

Valutazione del livello di rischio

- **Probabilità**

Sulla base delle misure adottate, delle indicazioni agli utenti sulla corretta gestione della piattaforma, la probabilità è stimata come *Poco Probabile (Livello P2)*.

- **Conseguenze**

In base alla natura dei dati trattati (considerando che non è previsto il trattamento di dati sensibili), le conseguenze sono valutate come *Limitate* (C=2).

- **Livello di rischio**

  Il livello di rischio LR risulta pari a $2 \times 2 = 4$, su una scala massima di 16, e può pertanto considerarsi Basso.

9.4 Valutazione complessiva del rischio residuo

L'analisi evidenzia che il rischio residuo associato all'utilizzo dei servizi IA generici autorizzati è complessivamente BASSO-MEDIO, a condizione che le misure di mitigazione individuate siano effettivamente attuate. Nessuno scenario raggiunge il livello ALTO. Il trattamento può procedere con le misure indicate. La valutazione sarà rivalutata annualmente e in caso di introduzione di nuovi strumenti o di modifica sostanziale delle modalità d'uso.

10. Monitoraggio, revisione e raccordo con il PIA

10.1 Piano di monitoraggio

Attività di monitoraggio	Frequenza	Responsabile
Verifica utilizzo strumenti autorizzati vs. non autorizzati	Trimestrale	Referente IA
Aggiornamento Elenco Strumenti IA Autorizzati	A ogni nuova richiesta	DPO + Referente IA
Report semestrale al Dirigente Scolastico	Semestrale (dic. e giu.)	Referente IA + DPO
Revisione della presente DPIA	Annuale o in caso di modifiche sostanziali	DPO
Aggiornamento DVR con rischi IA	Annuale	DS + RSPP
Revisione Piano di formazione PIA	Annuale (Collegio Docenti)	Referente IA + DS
Raccolta segnalazioni da Consigli di Classe	Semestrale	Referente IA

10.2 Condizioni che richiedono una revisione straordinaria della DPIA

- Introduzione di un nuovo strumento IA non ancora valutato;
- Modifica sostanziale delle funzionalità di uno strumento già autorizzato (inclusa attivazione di funzionalità agentive);
- Modifica delle condizioni contrattuali del fornitore (DPA, privacy policy, data retention);
- Data breach o incidente di sicurezza connesso all'utilizzo di strumenti IA;
- Modifica del quadro normativo di riferimento (GDPR, AI Act, Linee guida MIM);
- Aggiornamento del PIA d'Istituto che impatti le prescrizioni relative al trattamento.

11. Approvazione e firme

Ruolo	Nome e cognome	Firma	Data
DPO d'Istituto (redazione)		_____	___/___/_____
Referente IA (consultato)		_____	___/___/_____
Dirigente Scolastica (approvazione)		_____	___/___/_____