Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO STATALE "*VIA DEI SALICI*"
Via A. Robino 25/A – 20025 Legnano
Tel: 0331 541316
Cod.mec.MIIC85500G – C.F- 84003710153
e-mail: miic85500g@istruzione.it
e-mail: miic85500g@pec.istruzione.it

DPIA - Valutazione d'impatto sulla protezione dei dati

Uso di funzionalita' di Intelligenza Artificiale (AI) in ambiente scolastico

Istituto Comprensivo "Via dei Salici" – Legnano

Sommario

Controllo del documento

Voce	Valore	Voce	Valore
Titolare del trattamento	[Denominazione Istituto]	Rappresentante	Dirigente Scolastico pro tempore
DPO	Ferdinando Bassi (Easyteam.org SRL)	Email DPO	dpo@easyteam.org
Team Referente interno (AI/Privacy)	Colombo Iole Grasso Elena Latella Carmelo Lombardi Gaia	Email	colombo.iole@icsviadeisalici.it grasso.elena@icsviadeisalici.it latella.carmelo@icsviadeisalici.it lombardi.gaiai@icsviadeisalici.it
Ambito DPIA	Uso di funzionalita' AI in strumenti digitali adottati/consentiti	Periodo di validità	Il presente documento è valido fino a successiva revisione; è comunque aggiornato in caso di modifiche rilevanti a trattamenti, strumenti/fornitori o misure di sicurezza e, in ogni caso, con revisione almeno annuale.

Riferimenti normativi essenziali

- Regolamento (UE) 2016/679 (GDPR), in particolare artt. 5, 24, 25, 28, 32, 35, 36.
- D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), come modificato dal D.Lgs. 101/2018.
- Garante per la protezione dei dati personali - Provvedimento 11 ottobre 2018 (Delibera n. 467): elenco trattamenti soggetti a DPIA (art. 35, co. 4 GDPR).
- WP29/EDPB - Guidelines on DPIA and high risk (WP248rev.01, 4 ottobre 2017).
- Regolamento (UE) 2024/1689 (AI Act), in particolare art. 27 (FRIA, se applicabile), art. 50 (trasparenza) e Allegato III (sistemi ad alto rischio in istruzione).
- Base giuridica: art. 6(1)(e) e/o 6(1)(c) GDPR, in relazione alle finalità didattiche e organizzative; eventuali attività facoltative con servizi esterni sono gestite con informativa dedicata e, se del caso, consenso separato e alternativa equivalente.

1. Scopo, perimetro e criteri di applicazione

La presente DPIA valuta i rischi per i diritti e le libertà degli interessati derivanti dall'uso di funzionalità di intelligenza artificiale (AI) integrate o attivabili all'interno di software e servizi digitali utilizzati in ambito scolastico. Il documento è focalizzato sulle funzionalità AI (es. assistenti di scrittura, sintesi, generazione di contenuti, ricerca e chat) e sulle relative operazioni di trattamento (input, output, log, telemetrie, eventuali conservazioni).

Questa DPIA riguarda solo l'uso delle funzioni di Intelligenza Artificiale presenti nei programmi/app e nelle piattaforme della scuola. Le altre funzioni 'normali' degli stessi strumenti (ad esempio scrivere un documento, salvare un file o inviare un'email che non usano l'intelligenza artificiale) non rientrano in questa DPIA, a meno che per far funzionare l'AI vengano usati gli stessi account e gli stessi sistemi di registrazione e conservazione dei dati (ad esempio accessi, cronologia delle attività, archivi e cartelle).

Il presente documento è predisposto come DPIA 'tematica' sull'AI. Qualora una piattaforma o servizio introduca rischi aggiuntivi non legati alle funzioni AI (es. trattamenti amministrativi, registro elettronico), tali aspetti devono essere valutati in DPIA dedicate o mediante aggiornamento del Registro dei Trattamenti.

2. Ruoli e responsabilità

2.1 Titolare del trattamento

Denominazione: Istituto Comprensivo Via dei Salici
Rappresentante legale: Dirigente Scolastico pro tempore
Contatti: MIIC85500G@pec.istruzione.it - 0331-541316
Sede: Via Robino 25 - 20025 Legnano (MI)

2.2 Responsabile della protezione dei dati (DPO)

Nome: Ferdinando Bassi
Società: Easyteam.org SRL
Email: dpo@easyteam.org

2.3 Responsabili del trattamento e sub-responsabili (fornitori)

Come da Regolamento AI adottato dall'Istituto, è vietato utilizzare le credenziali istituzionali dell'Istituto (account di dominio) per registrarsi o accedere a servizi/applicazioni esterne non

autorizzati, incluse le funzioni “Accedi con Google/Microsoft” (SSO) o equivalenti. Per tali servizi esterni non autorizzati è ammesso esclusivamente l’uso dell’email istituzionale come semplice username, senza SSO, con password nuova e dedicata (non riutilizzata e diversa da quella dell’account di dominio). L’accesso tramite credenziali istituzionali è consentito esclusivamente per i seguenti servizi, oggetto della presente DPIA:

1. Google Workspace for Education
2. Microsoft app and services
3. Office 365
4. Canva for Education

L’elenco dei servizi oggetto della presente DPIA e i relativi riferimenti documentali (ruolo privacy del fornitore, controparte/sede, sintesi su ubicazione dei dati e possibili trasferimenti extra SEE, link all’accordo ex art. 28 GDPR – DPA, link a sub-responsabili/trasparenza e misure di sicurezza) sono riportati nell’**Allegato A** , parte integrante del presente documento. L’Allegato A è mantenuto aggiornato dall’Istituto; eventuali modifiche ai fornitori, alle funzionalità AI abilitate o ai termini contrattuali/documentali comportano la verifica di coerenza e, se necessario, l’aggiornamento della presente DPIA.

3. Descrizione del trattamento (funzionalità AI)

3.1 Casi d'uso consentiti

- Supporto alla redazione di materiali didattici (bozze, schemi, rubriche).
- Sintesi e riformulazione di testi non contenenti dati personali o comunque minimizzati.
- Traduzioni e adattamenti linguistici di testi didattici, evitando dati identificativi.
- Generazione di esercizi e quiz su contenuti generali, con supervisione del docente.
- Supporto alla produttività del personale (es. minute, modelli), senza dati particolari.

3.2 Casi d'uso vietati (misure organizzative)

- Inserimento nei prompt di dati personali non necessari o di categorie particolari di dati (es. salute, BES/DSA/PEI, provvedimenti disciplinari).
- Caricamento di documenti contenenti dati personali di studenti/personale su servizi AI consumer o non autorizzati.
- Uso di output AI come unico fondamento per valutazioni, provvedimenti o decisioni che producano effetti significativi senza verifica umana.

- Uso di strumenti non ammessi dall'Istituto (divieto espressamente comunicato; v. Allegato 2).

3.3 Flusso del trattamento

Input: testo o contenuti inseriti dall'utente (docente/personale e, ove consentito, studenti) tramite account istituzionale.
Elaborazione: il servizio AI elabora l'input e genera un output (testo/immagine/riassunto).
Output: contenuto restituito all'utente e, se necessario, salvato in archivi scolastici (Drive/OneDrive) secondo le regole interne.
Log e telemetrie: il fornitore può trattare metadati e log tecnici per sicurezza, prevenzione abusi e miglioramento del servizio, secondo la documentazione contrattuale.

4. Categorie di interessati e dati trattati

4.1 Interessati

- Studenti (inclusi minorenni)
- Genitori/tutori (limitato alle interazioni tramite canali scolastici)
- Docenti
- Personale ATA
- Collaboratori esterni autorizzati (se presenti)

4.2 Categorie di dati

Categoria	**Esempi**	**Previsto nel perimetro AI**	**Note/Divieti**
Dati identificativi (minimizzati)	nome, classe, ruolo	Solo se indispensabile	Preferire fortemente anonimizzazione e pseudonimizzazione.
Dati didattici generali	argomenti, tracce, materiali	Si	Evitare riferimenti a singoli studenti.
Metadati e log	timestamp, IP, device, audit log	Si	Valutare retention e accessi; base contrattuale.
Categorie particolari (art. 9 GDPR)	salute, disabilita', BES/DSA/PEI	No	Vietato inserirli nei prompt; gestione come incidente se accade.

5. Finalità, basi giuridiche e conservazione

5.1 Finalità

- Supporto alla didattica e alla preparazione di materiali formativi.
- Supporto alla produttività e all'organizzazione del lavoro del personale scolastico.
- Sperimentazione didattica controllata e supervisione sull'uso dell'AI, con finalita' educative (alfabetizzazione digitale).

5.2 Basi giuridiche (da completare dall'Istituto)

Per gli istituti scolastici pubblici, la base giuridica è tipicamente il compito di interesse pubblico (art. 6, par. 1, lett. e GDPR) e/o obblighi legali (art. 6, par. 1, lett. c GDPR), con indicazione delle norme di settore. Compilare la tabella seguente per ciascun caso d'uso.

Caso d'uso	**Finalità**	**Base giuridica (art. 6 GDPR)**	**Riferimento normativo**	**Note**
Supporto redazione materiali didattici (docenti/personale)	Preparazione di lezioni, esercitazioni, tracce, griglie e materiali di supporto alla didattica	Art. 6(1)(e) – compito di interesse pubblico/esercizio di pubblici poteri	D.P.R. 275/1999 (autonomia scolastica); D.Lgs. 297/1994 (T.U. scuola); PTOF e delibere degli organi collegiali	Uso con dati minimizzati; vietato inserire dati identificativi degli studenti e categorie particolari nei prompt; usare solo servizi autorizzati con account istituzionale
Sintesi / riformulazioni (accessibilità e inclusione)	Semplificazione testi, adattamento linguistico, supporto a bisogni educativi e accessibilità dei contenuti	Art. 6(1)(e) – compito di interesse pubblico/esercizio di pubblici poteri	L. 104/1992 e D.Lgs. 66/2017 (inclusione); L. 170/2010 (DSA) e relative linee guida; PTOF	Nessun dato personale dello studente nei testi da sintetizzare; preferire contenuti già anonimizzati; verifica umana obbligatoria prima dell'uso in classe

Attività didattiche con studenti (uso guidato)	Attività formative su competenze digitali/IA, esercitazioni guidate e produzione di contenuti didattici	Art. 6(1)(e) – compito di interesse pubblico/esercizio di pubblici poteri	D.P.R. 275/1999; PTOF; regolamento d'istituto e delibere organi collegiali	Accesso solo con strumenti autorizzati; supervisione docente; divieto inserire dati personali nei prompt; nessuna decisione/valutazione automatizzata senza controllo umano

5.3 Conservazione e cancellazione

L'Istituto applica il principio di limitazione della conservazione, definendo per quanto tempo conservare i dati, differenziati in funzione della finalità e della tipologia di dato. In relazione all'uso di funzionalità di IA, si distinguono i seguenti insiemi:

1. **Contenuti prodotti dall'utente e salvati negli archivi scolastici** (es. documenti, presentazioni, elaborati): sono conservati secondo i tempi previsti dalle regole interne di gestione documentale/archivistica dell'Istituto e dai processi didattico-amministrativi di riferimento; al termine sono cancellati o archiviati secondo le procedure vigenti.

2. **Log di accesso e audit** (es. accessi, eventi di sicurezza, tracciamenti tecnici): sono conservati per un periodo limitato e proporzionato alle esigenze di sicurezza, gestione incidenti e accountability, con accesso riservato al personale autorizzato; al termine sono cancellati o anonimizzati secondo le impostazioni di servizio.

3. **Prompt, input e output IA eventualmente conservati dal fornitore**: l'Istituto configura i servizi, ove possibile, per minimizzare la conservazione e disabilitare l'uso dei contenuti per finalità non necessarie (es. addestramento/miglioramento, se previsto come opzione). La conservazione e cancellazione di tali dati seguono le impostazioni del servizio e/o le previsioni contrattuali (DPA/termini) e sono verificate in fase di adozione e nelle revisioni periodiche.

Le modalità di cancellazione (cancellazione logica, tempi di eliminazione definitiva, backup) e le eventuali eccezioni sono documentate nelle impostazioni dei servizi adottati e/o nella documentazione contrattuale dei fornitori (DPA, policy di retention e sicurezza). Eventuali modifiche rilevanti delle policy di conservazione dei fornitori comportano rivalutazione e, se necessario, aggiornamento della presente DPIA.

6. Necessita' e proporzionalità

- L'uso dell'AI e' limitato a funzionalita' di supporto (sintesi, suggerimenti, generazione di contenuti) e non sostituisce la valutazione professionale del docente o del personale.
- Non sono previste decisioni automatizzate vincolanti ai sensi dell'art. 22 GDPR; è garantita la supervisione umana in ogni fase.
- Principio di minimizzazione: evitare l'inserimento di dati personali; usare preferibilmente dati anonimi o pseudonimizzati.
- Privacy by design/by default: utilizzo di account istituzionali, controlli accesso, limitazioni di condivisione, configurazioni di logging e retention.

7. Analisi dei rischi (metodologia)

La valutazione considera: (a) gravità dell'impatto (1-4) e (b) probabilità di accadimento (1-4). Il rischio inerente è dato dalla combinazione dei due fattori; il rischio residuo è calcolato dopo l'applicazione delle misure.

Scala adottata

Valore	Probabilita'	Impatto
1	Raro	Limitato
2	Possibile	Moderato
3	Probabile	Significativo
4	Molto probabile	Grave

8. Registro dei rischi e misure di mitigazione

ID	Rischio / Scenario	Interessi / diritti impattati	Impatto (1-4)	Prob. (1-4)	Rischio inerente	Misure di mitigazione (sintesi)	Rischio residuo
R1	Inserimento nei prompt di dati personali o dati particolari; possibile data leakage verso fornitore.	Riservatezza, minimizzazione	4	2	Alto	Policy d'uso; formazione; divieto dati particolari; account istituzionali; controllo condivisioni; procedura incident/data breach.	Medio
R2	Output errati/allucinazioni usati come base per atti didattici senza verifica.	Accuratezza, correttezza, non discriminazione	3	3	Alto	Supervisione umana obbligatoria; linee guida su fact-check; divieto di uso per decisioni vincolanti; rubriche di verifica.	Medio
R3	Bias/discriminazioni negli output (stereotipi, contenuti inappropriati per minori).	Non discriminazione, tutela minori	3	2	Medio	Filtri contenuto dove disponibili; prompt sicuri; revisione docente; canale	Basso/Medio

						segnalazioni; procedure disciplinari per abusi.	
R4	Uso di strumenti AI non ammessi (consumer) non bloccabili tecnicamente; upload non autorizzato.	Riservatezza, accountability	4	2	Alto	Divieto formale; informazione e formazione; controlli a campione; responsabilizzazione; gestione incidenti; alternative approvate.	Medio
R5	Conservazione/log eccessivi (prompt/output/log) presso fornitore; retention non definita.	Limitazione conservazione, trasparenza	3	2	Medio	Verifica impostazioni; DPA; configurazione retention; minimizzare log; registro trattamenti; audit periodici.	Basso/Medio
R6	Accessi non autorizzati agli account (phishing, password deboli) e quindi ai contenuti AI.	Integrita', riservatezza	4	2	Alto	MFA dove possibile; SSO; policy password; awareness; logging; gestione credenziali e revoche; incident response.	Medio

Valutazione complessiva: rischio residuo medio-basso.

9. Misure tecniche, organizzative e contrattuali

9.1 Tecniche

- Account istituzionali; gestione identita' centralizzata.
- MFA/SSO ove disponibile; gestione credenziali e revoche.
- Limitazioni di condivisione (link pubblici, condivisione esterna) e permessi su storage.
- Logging e audit; controllo accessi amministrativi; segregazione ruoli.
- Configurazioni di servizio per limitare l'uso dei dati per addestramento (ove previsto dal fornitore) e per definire retention.

9.2 Organizzative

- Policy d'uso AI (docenti/studenti/personale) con esempi di dati vietati e casi d'uso consentiti.
- Formazione periodica e comunicazioni alle famiglie; richiamo alla supervisione umana.
- Procedure per incidenti e data breach (artt. 33-34 GDPR): segnalazione, valutazione, notifica, comunicazione agli interessati.
- Procedure per gestione richieste interessati (accesso, rettifica, cancellazione, opposizione) e tracciamento.
- Monitoraggio periodico: audit configurazioni, revisione inventario strumenti, aggiornamento DPIA in caso di modifiche sostanziali.

9.3 Contrattuali

- Nomina del Responsabile del trattamento e accordo ex art. 28 GDPR; elenco sub-responsabili.
- Clausole su ubicazione dati, trasferimenti extra SEE e garanzie (es. SCC) se applicabili.
- SLA su sicurezza, supporto, audit e gestione incidenti; obblighi di cooperazione.
- Trasparenza su log, retention e sull'eventuale utilizzo dei dati per miglioramento/addestramento.

10. AI Act - screening e adempimenti pertinenti

10.1 Screening 'alto rischio' (Allegato III - istruzione)

Le funzionalita' AI considerate in questa DPIA sono impiegate come supporto e non sono destinate a: (a) determinare accesso/ammissione o assegnazioni, (b) valutare esiti di apprendimento per orientare automaticamente il processo, (c) determinare il livello appropriato di istruzione, (d)

monitorare e rilevare comportamenti proibiti durante test (proctoring). Qualora l'Istituto introduca in futuro tali impieghi, dovra' riesaminare la qualificazione come 'high-risk' e valutare gli obblighi aggiuntivi, inclusa FRIA.

10.2 Trasparenza (art. 50 AI Act)

Quando l'AI e' utilizzata per generare o manipolare contenuti destinati a studenti o terzi, l'Istituto adotta regole di trasparenza: indicazione dell'uso di AI ove opportuno; divieto di presentare come reale contenuto sintetico idoneo a trarre in inganno; gestione dei casi di contenuti generati/manipolati (es. immagini) con chiara disclosure.

11. Consultazione DPO e decisione finale

Il DPO e' consultato nella predisposizione e nell'aggiornamento della presente DPIA. In caso di rischio residuo elevato non mitigabile, l'Istituto valuta la consultazione preventiva dell'Autorità di controllo (art. 36 GDPR).

Voce	Esito	Data	Note
Parere DPO	Favorevole	09/02/2026	
Decisione del Titolare	Favorevole	10/02/2026	

Inventario strumenti con funzionalità AI

L’inventario degli strumenti in uso nell’Istituto con funzionalità AI è riportato nell’Allegato A al Regolamento Ai.