DPIA QUADRO

Valutazione d'Impatto sulla Protezione dei Dati (Art. 35 GDPR) sull' utilizzo di Sistemi di Intelligenza Artificiale Generativa in ambito scolastico conforme ai principi del Regolamento (UE) 2024/1689 – AI Act

---

1. Premessa

La presente Valutazione d'Impatto sulla Protezione dei Dati (DPIA), redatta ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (GDPR), disciplina il quadro generale relativo all'utilizzo di sistemi di Intelligenza Artificiale (IA) generativa nell'ambito delle attività istituzionali, didattiche, formative ed organizzative di una Istituzione scolastica.

La DPIA è predisposta anche in considerazione della progressiva applicazione del Regolamento (UE) 2024/1689 (AI Act), con particolare riferimento alla governance dei sistemi di IA; alla tutela dei minori; alla trasparenza; alla supervisione umana; alla gestione dei rischi; all'alfabetizzazione in materia di IA (AI Literacy); alla protezione dei dati personali.

Il presente documento costituisce una DPIA quadro generale.

Per ciascuna piattaforma o fornitore utilizzato dall'Istituto dovranno essere predisposte specifiche schede integrative contenenti: caratteristiche tecniche; configurazioni adottate; verifiche privacy; trasferimenti internazionali; misure di sicurezza; valutazione rischi specifici.

---

2. Ambito di applicazione

La presente DPIA si applica all'utilizzo di: piattaforme di IA generativa; chatbot conversazionali; assistenti digitali basati su IA; sistemi di supporto alla produzione di contenuti; strumenti di sintesi automatica; sistemi di supporto alla didattica; piattaforme IA integrate nei servizi cloud scolastici.

---

3. Finalità del trattamento

I sistemi di IA possono essere utilizzati esclusivamente per: supporto alla didattica; supporto alla progettazione didattica; attività laboratoriali; sviluppo competenze digitali; alfabetizzazione IA; supporto alla produzione di contenuti; supporto linguistico; sintesi e rielaborazione testi; supporto organizzativo e documentale; formazione del personale.

È vietato l'utilizzo dei sistemi IA per finalità incompatibili con i compiti istituzionali dell'Istituto.

---

4. Categorie di interessati

Sono coinvolti nell'utilizzo di strumenti d intelligenza artificiale: gli studenti; le famiglie; i docenti; il personale ATA; i collaboratori esterni; gli amministratori di sistema.

Particolare attenzione è riservata ai dati dei minori.

---

5. Categorie di dati trattati

I dati trattabili con strumenti di IA sono: dati identificativi essenziali; e-mail istituzionali; username; log tecnici; contenuti dei prompt; elaborati scolastici; documenti didattici.

---

6. Dati il cui inserimento è vietato

È fatto espresso divieto di inserire nei sistemi IA: dati sanitari; dati BES/DSA/disabilità; dati giudiziari; informazioni disciplinari; dati familiari riservati; fotografie identificative di minori; dati biometrici; credenziali; documenti amministrativi riservati; dati appartenenti alle categorie particolari ex art. 9 GDPR (dati sensibili).

---

7. Base giuridica del trattamento

Il trattamento si fonda sui seguenti riferimenti normativi: art. 6 par. 1 lett. e) GDPR; art. 6 par. 1 lett. c) GDPR; D.Lgs. 297/1994; D.P.R. 275/1999; Piano Nazionale Scuola Digitale; normative ministeriali sulla digitalizzazione scolastica.

Per eventuali attività ulteriori potrà essere acquisito specifico consenso ove necessario.

---

8. Necessità della DPIA

La DPIA è ritenuta necessaria ogni qualvolta il trattamento presenta: L'utilizzo di nuove tecnologie; utilizzo di sistemi IA; trattamento dati di minori; possibili trasferimenti extra SEE; rischio inserimento improprio dati personali; possibile profilazione indiretta; elaborazione automatizzata di contenuti.

---

9. Principi AI Act adottati dall'Istituto

L'Istituto adotta i seguenti principi organizzativi coerenti con il Regolamento (UE) 2024/1689:

9.1 Supervisione umana

Ogni utilizzo dell'IA in ambito scolastico deve essere sottoposto a supervisione umana da parte del personale docente o amministrativo competente.

9.2 Trasparenza

Gli utenti devono essere informati: dell'utilizzo di sistemi IA; dei limiti delle risposte generate; dei rischi connessi; delle regole di utilizzo.

9.3 Protezione dei minori

L'utilizzo dell'IA nell'ambito scolastico deve avvenire nel rispetto del superiore interesse del minore.

9.4 Accountability

L'Istituto mantiene: documentazione delle piattaforme utilizzate; verifiche privacy; policy interne; audit periodici con gli addetti alla gestione della IA; formazione del personale.

9.5 AI Literacy

L'Istituto promuove adeguata alfabetizzazione in materia di IA nei confronti di: docenti; studenti; personale ATA; amministratori.

---

10. Classificazione dei sistemi di IA utilizzati

Categoria	**Esempi**	**Livello rischio**
IA generativa supporto didattica	Chatbot educativi	Limitato
Assistenti documentali	Sintesi testi	Limitato
Supporto organizzativo	Produzione bozze	Limitato
Sistemi valutazione automatica	Correzione automatica	Potenzialmente alto
Sistemi profilazione studenti	Analisi comportamentale	Alto
Riconoscimento emozioni	Emotion AI	Vietato/sconsigliato

---

11. Sistemi vietati o non autorizzati

È vietato l'utilizzo di: sistemi di riconoscimento emozionale sugli studenti; sistemi biometrici non autorizzati; sistemi di profilazione invasiva; sistemi di sorveglianza automatizzata dei comportamenti; IA per decisioni automatizzate prive di supervisione umana.

---

12. Descrizione tecnica del trattamento

- Modalità di accesso

L'accesso ai sistemi IA può avvenire: tramite browser web; tramite account istituzionali; tramite dispositivi scolastici; tramite dispositivi BYOD autorizzati.

- Configurazioni preferibili

L'Istituto privilegia: configurazioni centralizzate "Edu"; piattaforme con gestione amministrativa centralizzata; account istituzionali; controllo amministrativo utenti.

---

13. Trasferimenti verso Paesi terzi

L'utilizzo di sistemi IA cloud può comportare trasferimenti di dati verso Paesi extra SEE.

L'Istituto verifica ove possibile:

- presenza SCC; (Clausole Contrattuali Standard adottate dalla Commissione Europea ai fini della regolamentazione dei trasferimenti di dati personali verso Paesi extra UE);
- documentazione privacy; (rilasciata dal fornitore a corredo dello strumento di IA);
- eventuale adesione Data Privacy Framework; (sistema di trasferimento dati approvato tra Unione Europea e Stati Uniti);
- presenza di subprocessor; (soggetti terzi ai quali il fornitore principale del servizio IA affida parte delle operazioni di trattamento dei dati personali);
- misure supplementari;(ulteriori garanzie tecniche, organizzative o contrattuali adottate per aumentare il livello di protezione dei dati personali trasferiti fuori dallo SEE);
- retention dati; (quanto tempo i dati restano memorizzati; dove vengono conservati; per quali finalità; quando vengono cancellati o anonimizzati);

Qualora le SCC non risultino direttamente verificabili, tale circostanza viene riportata nelle schede integrative del singolo fornitore.

---

14. Analisi di necessità e proporzionalità

L'utilizzo dei sistemi IA è ritenuto proporzionato purché: siano utilizzati per finalità istituzionali; sia limitato il trattamento dati; siano vietati dati particolari; sia garantita la supervisione docente; siano adottate policy interne; siano effettuate verifiche periodiche.

---

15. Analisi generale dei rischi

Rischio	**Probabilità**	**Impatto**	**Livello**
Inserimento dati personali nei prompt	Alta	Alta	Alto
Inserimento dati particolari minori	Media	Molto Alto	Alto

Rischio	Probabilità	Impatto	Livello
Trasferimenti extra UE	Media	Alto	Medio-Alto
Utilizzo improprio IA	Alta	Medio	Medio-Alto
Hallucinations/contenuti errati	Alta	Medio	Medio
Decisioni automatizzate improprie	Media	Alto	Medio-Alto
Profilazione indiretta	Media	Medio	Medio
Accessi non autorizzati	Media	Alto	Medio-Alto
Mancanza trasparenza algoritmica	Media	Medio	Medio
Violazione minimizzazione	Alta	Alto	Alto

---

16. Misure di mitigazione

l'Istituto adotta le seguenti misure organizzative, tecniche, informative:

16.1 Misure organizzative

Adozione regolamento IA; disciplinare utilizzo studenti/docenti; policy prompt; supervisione docente; autorizzazioni formalizzate; audit periodici; aggiornamento Registro Trattamenti; formazione del personale.

16.2 Misure tecniche

- autenticazione forte;
- account istituzionali assegnati dall'Istituzione scolastica ai singoli utenti;
- logging accessi – (registrazione e conservazione delle informazioni relative agli accessi effettuati ai sistemi informatici, alle piattaforme e ai dati trattati)
- segregazione utenti - (ogni utente vede solo ciò che è autorizzato a vedere in base al ruolo);
- limitazione upload – (restrizioni tecniche e organizzative finalizzate a controllare, ridurre o impedire il caricamento di determinati dati, documenti o contenuti all'interno delle piattaforme IA);
- monitoraggio amministrativo – (attività di controllo, supervisione e verifica effettuata dall'amministrazione o dagli amministratori del sistema sull'utilizzo delle piattaforme, degli account e delle funzionalità disponibili);

- aggiornamento dispositivi – (aggiornamento periodico di sistemi operativi, software, applicazioni, firmware e componenti di sicurezza dei dispositivi utilizzati per accedere o utilizzare i sistemi informatici e le piattaforme IA)
- filtri DNS/web che impediscono al dispositivo di raggiungere determinati domini.

16.3 Misure informative

informative privacy dedicate; policy IA; istruzioni operative; informative famiglie; percorsi AI Literacy – (alfabetizzazione all'intelligenza artificiale).

---

17. Rischio residuo

Il livello di rischio risultante dopo l'applicazione delle misure tecniche, organizzative e contrattuali adottate per mitigare i rischi individuati è il seguente:

Area di rischio	**Ambito di valutazione**	**Livello residuo**
Riservatezza	Rischio di accesso non autorizzato, divulgazione impropria, perdita di controllo o trattamento illecito dei dati personali trattati mediante i sistemi IA	Medio
Integrità	Rischio di alterazione, modifica non autorizzata, corruzione o inaccuratezza dei dati e dei contenuti trattati o generati dai sistemi IA	Basso
Disponibilità	Rischio di indisponibilità dei servizi, perdita di accesso ai dati o interruzione operativa delle piattaforme IA utilizzate dall'Istituto	Basso
Diritti e libertà dei minori	Rischio di impatto sui diritti fondamentali, sulla tutela dei minori, sulla non discriminazione, sulla profilazione o sull'utilizzo improprio dei dati degli studenti	Medio
Accountability e governance	Rischio connesso all'insufficiente tracciabilità, controllo, supervisione, documentazione o conformità normativa nell'utilizzo dei sistemi IA	Medio
Trasferimenti internazionali	Rischio derivante dal trasferimento di dati personali verso Paesi extra UE, dalla presenza di subprocessor esteri o dall'utilizzo di servizi cloud internazionali	Medio

Il rischio residuo così formulato è ritenuto accettabile purché: siano rispettate le policy interne; siano utilizzati strumenti autorizzati; venga mantenuta supervisione umana; siano effettuate verifiche periodiche.

18. Governance IA dell'Istituto

L'Istituto adotta: elenco delle piattaforme autorizzate; registro degli strumenti IA; verifiche privacy periodiche; classificazione rischi IA; procedure segnalazione incidenti; aggiornamento documentale periodico.

19. Obblighi del personale

Il personale scolastico deve: utilizzare esclusivamente strumenti autorizzati; evitare inserimento dati particolari; verificare criticamente gli output IA; garantire supervisione educativa; rispettare policy e regolamenti interni.

20. Obblighi degli studenti

Gli studenti devono: utilizzare l'IA solo per finalità didattiche; non inserire dati personali; non utilizzare strumenti vietati; rispettare le istruzioni dei docenti.

21. Conclusioni

L'utilizzo di sistemi di IA generativa in ambito scolastico è ritenuto compatibile con il GDPR e con i principi del Regolamento (UE) 2024/1689 (AI Act) purché:

- sia garantita supervisione umana;
- siano vietati trattamenti invasivi;
- siano utilizzati strumenti autorizzati;
- siano adottate adeguate misure organizzative e tecniche;
- venga assicurata formazione continua;
- siano effettuate verifiche periodiche.

La presente DPIA costituisce documento quadro generale e dovrà essere integrata da schede specifiche relative ai singoli fornitori o piattaforme IA utilizzate.

22. Allegati

- Regolamento IA;
- Policy utilizzo IA;

- Procedura gestione incidenti IA;
- Policy BYOD;
- Piano formazione AI Literacy;
- Audit checklist IA.

---

23. Data e firme

Data: 18 / 09 / 2026

Il Titolare del trattamento

Firma: