Valutazione d'Impatto sulla Protezione dei Dati (DPIA) – Uso di Strumenti di IA Generativa nelle Scuole

Istituto Scolastico: ISTITUTO COMPRENSIVO SANTA CATERINA CAGLIARI.

Responsabile/Titolare del Trattamento: Dirigente Scolastico –MASSIMO SPIGA

Responsabile della Protezione dei Dati (RPD/DPO): MARIO MUREDDU

Documento per uso interno. Spazi riservati per firma del Titolare e parere del RPD in calce.

1. Finalità del trattamento

L'istituto intende introdurre strumenti di **Intelligenza Artificiale (IA) generativa** a supporto delle attività didattiche e organizzative. Le finalità del trattamento dei dati con tali strumenti riguardano principalmente il **miglioramento dei processi educativi** e amministrativi. In particolare, si prevede che gli strumenti di IA generativa verranno utilizzati per:

- **Supporto alla didattica e creazione di contenuti:** i docenti potranno avvalersi dell'IA per generare materiali didattici personalizzati, quiz, sintesi di testi o spunti creativi da utilizzare nelle lezioni, adattando i contenuti alle esigenze di ciascuna classe o studente. Tali applicazioni valorizzano le potenzialità dell'IA a supporto della didattica e dell'innovazione digitale, consentendo ad esempio la preparazione di risorse interattive e percorsi personalizzati.
- **Supporto allo studio per gli studenti:** in alcuni casi controllati, agli studenti potrà essere consentito di utilizzare strumenti di IA (ad es. chatbot educativi) come tutor virtuali per approfondimenti, esercitazioni o feedback immediati sui propri elaborati. Ciò potrà favorire un apprendimento personalizzato, fermo restando il monitoraggio costante da parte dei docenti.
- **Semplificazione di attività amministrative:** l'IA generativa potrà essere impiegata dal personale amministrativo per automatizzare bozze di documenti, comunicazioni standard o rispondere a richieste frequenti (es. tramite chatbot informativi interni), con l'obiettivo di ottimizzare i processi organizzativi della scuola.

Le **finalità** sono dunque orientate al **corretto svolgimento dell'attività didattica e amministrativa**, sfruttando le tecnologie emergenti per migliorare l'efficacia dei servizi scolastici. L'uso dell'IA avverrà in modo **sperimentale e controllato**, perseguendo un'innovazione responsabile e bilanciando i benefici con la tutela dei diritti degli interessati (studenti, famiglie, personale).

(Nota: Si esclude volutamente da questa DPIA qualsiasi valutazione sugli effetti pedagogici o sull'apprendimento, concentrandosi esclusivamente sugli impatti in termini di protezione dei dati personali.)

2. Contesto normativo e giuridico

L'introduzione di strumenti di IA generativa nelle scuole avviene nel rispetto del quadro normativo vigente in materia di protezione dei dati e delle tecnologie emergenti. I riferimenti principali sono:

- **Regolamento (UE) 2016/679 (GDPR):** disciplina cardine per la protezione dei dati personali. La scuola, in qualità di titolare del trattamento, è tenuta a garantire che ogni uso di IA sia conforme ai principi di liceità, correttezza, trasparenza, minimizzazione dei dati, esattezza e integrità/confidenzialità (artt. 5 e ss. GDPR). Particolare attenzione è rivolta ai minori: i bambini meritano specifica protezione riguardo ai propri dati personali, essendo meno consapevoli di rischi e conseguenze.
- **Regolamento UE "AI Act" (in fase di definizione):** la nuova normativa europea sull'Intelligenza Artificiale classificherà i sistemi di IA per livello di rischio (inaccettabile, alto, limitato, minimo) e introdurrà obblighi specifici per fornitori e utilizzatori. Anche se l'AI Act non è ancora definitivamente applicabile al momento di questa valutazione, le **Linee Guida ministeriali 2025** raccomandano di allinearsi sin da ora ai suoi principi. In ambito educativo, l'AI Act e le linee guida correlate considerano ad **alto rischio** quei sistemi di IA che possano avere impatti significativi sul percorso di vita degli studenti (es. software che decidono ammissioni o attribuiscono voti). L'utilizzo di sistemi generativi per creare contenuti didattici o di supporto allo studio rientra invece tipicamente in categorie di rischio **limitato o minimo**, purché tali sistemi vengano usati in maniera trasparente (dichiarando quando si interagisce con un'IA) e sotto supervisione umana. Va comunque monitorata l'evoluzione legislativa: il legislatore italiano sta preparando disposizioni nazionali in materia di IA (disegno di legge A.C. 2316/S.1146 del 2024-25) in coerenza con l'approccio europeo.
- **Provvedimenti e orientamenti del Garante Privacy:** l'Autorità Garante per la protezione dei dati personali ha già posto l'attenzione sui rischi derivanti da IA generativa. In particolare, nel 2023 il Garante ha adottato provvedimenti verso un fornitore di servizi di IA generativa molto diffuso, riscontrando diverse violazioni del GDPR: mancata informativa e base giuridica inadeguata per l'uso dei dati personali nell'addestramento del modello, assenza di meccanismi di verifica dell'età degli utenti minori, e mancata notifica di una violazione di dati. Tali interventi sottolineano l'importanza di assicurare **trasparenza, liceità del trattamento e tutela dei minori** nell'uso di IA. La scuola, in qualità di pubblica amministrazione, è tenuta a osservare eventuali futuri provvedimenti generali o linee guida emanate dal Garante sul tema (ad es. elenchi delle tipologie di trattamenti soggetti a DPIA obbligatoria ex art.35.4 GDPR, che potrebbero includere utilizzi di IA su larga scala, trattamenti automatizzati su minori, ecc.).
- **Linee Guida AgID/ACN e disposizioni nazionali:** le Linee Guida per l'uso dell'IA nella Pubblica Amministrazione e specificamente nelle istituzioni scolastiche forniscono un quadro di riferimento per un'adozione **consapevole e sicura** dell'I. Il Ministero dell'Istruzione e del Merito (MIM) nel 2025 ha emanato indicazioni operative che richiedono alle scuole un approccio improntato alla **responsabilità (accountability)** e alla **gestione del rischio** nell'introdurre l'IA. Ciò implica, ad esempio, che la scuola in qualità di *"deployer"* (utilizzatore finale di un sistema di IA) debba stipulare accordi contrattuali chiari con i fornitori, assicurandosi che questi rispettino obblighi di

trasparenza, qualità dei dati e monitoraggio continuo. Inoltre, in linea con il principio di "privacy by design/default" (art. 25 GDPR), le piattaforme di IA dovranno essere configurate e utilizzate riducendo al minimo i dati personali trattati e privilegiando l'utilizzo di dati anonimi o sintetici quando possibile.

- **Normativa nazionale su digitale e cybersecurity (AgID, ACN):** la scuola è soggetta alle regole italiane in tema di uso di servizi cloud e sicurezza informatica. La **circolare AgID n. 2/2018** (ora di competenza dell'Agenzia per la Cybersicurezza Nazionale - ACN) prevede che le PA possano utilizzare esclusivamente servizi cloud qualificati e inseriti nell'elenco ufficiale. Questo principio si applica anche alle piattaforme di IA cloud-based scelte dalla scuola. Inoltre, l'ACN e l'AgID promuovono l'adozione di misure minime di sicurezza ICT e di policy per la gestione sicura dei dati (es. **criteri di autenticazione forte, cifratura, controllo accessi, backup**), che dovranno essere rispettati nell'implementare gli strumenti di IA. Si terrà conto, infine, delle linee guida fornite da AgID in tema di procurement ICT e **due diligence** dei fornitori digitali, nonché di eventuali raccomandazioni di AgID/ACN specifiche sull'IA.

In sintesi, il contesto giuridico impone alla scuola di integrare i nuovi strumenti nel pieno rispetto della disciplina privacy (GDPR e Codice Privacy), anticipando al contempo le **future regole sull'IA** e attenendosi alle best practice indicate dalle autorità (Garante, AgID, ACN). La conformità normativa e la tutela dei diritti degli interessati costituiscono premesse imprescindibili per qualsiasi iniziativa di IA in ambito scolastico.

3. Descrizione dei trattamenti e categorie di dati

Modalità di utilizzo degli strumenti di IA: L'impiego di IA generativa avverrà attraverso piattaforme software (ad esempio, applicazioni web o servizi cloud) selezionate dall'istituto per le finalità di cui sopra. Gli scenari d'uso principali sono due:

- **Scenario A – IA senza dati personali di terzi:** il personale docente o amministrativo utilizza l'IA per generare contenuti o elaborare informazioni **senza inserire dati personali riferiti a studenti, genitori o altri interessati**. Ad esempio, un docente può chiedere al sistema di generare esercizi su un certo argomento o un modello di programma didattico, partendo da prompt generali. In questo scenario l'IA elabora principalmente dati testuali non riferibili a persone identificate, o al più dati personali del docente stesso (ad esempio, l'account di accesso al servizio, i log di utilizzo associati e le conversazioni stesse).
- **Scenario B – IA con dati personali di terzi:** gli strumenti di IA vengono alimentati con **dati personali di studenti o famiglie** per ottenere elaborazioni specifiche. Ciò potrebbe includere, ad esempio, fornire al sistema elaborati degli studenti per ottenerne una valutazione automatizzata, oppure inserire dati (anche minimali) su studenti per generare report personalizzati, lettere o piani didattici individualizzati. In questo scenario il trattamento riguarda dati riferiti a interessati terzi (minori e/o loro genitori).

Categorie di dati trattati: a seconda dello scenario e dell'uso specifico, le categorie di dati personali coinvolti possono includere:

- *Dati identificativi e di contatto:* informazioni per identificare in modo univoco gli utenti della piattaforma (docenti, studenti, genitori), quali nome e cognome,

username/account, indirizzo email istituzionale. Questi dati di **servizio** sono necessari per l'accesso alle piattaforme e per registrare le attività degli utenti.

- *Dati relativi al percorso scolastico:* nel caso di scenario B, potrebbero essere trattati dati personali comuni degli studenti, quali compiti svolti, temi o elaborati caricati sul sistema, voti o giudizi (qualora si sperimenti un'IA a supporto della valutazione), indicazioni sul rendimento o sulle difficoltà di apprendimento. Queste informazioni, prodotte nell'ambito delle attività didattiche, rientrano tra i **dati educativi** dello studente.
- *Dati particolari (sensibili):* in linea di principio si eviterà di trattare tramite IA dati appartenenti a categorie particolari ai sensi dell'art. 9 GDPR (es. dati su salute, origine etnica, opinioni politiche, credo religioso, etc.). Tuttavia, esiste il rischio che alcuni **elaborati degli studenti** o contenuti forniti possano incidentalmente rivelare informazioni di natura sensibile (si pensi a un tema in cui lo studente menzioni convinzioni personali, o a dati su BES/DSA – bisogni educativi speciali). Qualora tali dati siano coinvolti, si adotteranno misure aggiuntive per tutelarli (es. anonimizzazione preventiva del testo, o esclusione di questi elaborati dall'uso con l'IA) – vedere sez. 6 Misure.
- *Dati di log e tecnici:* i sistemi di IA generativa potrebbero registrare metadati relativi alle interazioni, quali orario delle richieste, indirizzi IP di connessione, informazioni sul dispositivo utilizzato, e registro delle operazioni effettuate (log di chat o di generazione). Tali dati, sebbene non sempre direttamente identificativi per la scuola, potrebbero essere accessibili al fornitore del servizio AI e rientrano quindi nel perimetro di questa valutazione.
- *Dati aggregati o anonimi:* in alcuni casi, per addestrare o migliorare i modelli AI, i fornitori potrebbero utilizzare dati derivanti dall'uso complessivo del servizio. La scuola richiederà garanzie che ogni eventuale dato di questo tipo venga **aggregato/anonimizzato** e non più riconducibile a persone identificabili, nel rispetto del principio di minimizzazione.

Ambito del trattamento: i trattamenti avverranno prevalentemente in forma digitale, attraverso piattaforme **cloud** accessibili via Internet. Gli strumenti individuati sono servizi di IA generativa forniti da terze parti specializzate (ad esempio piattaforme messe a disposizione da aziende tecnologiche) che agiscono su infrastrutture cloud. Tali servizi possono elaborare input testuali o altri tipi di dati forniti dagli utenti (ad es. immagini, nel caso si sperimenti IA generativa per creare contenuti visivi, benché al momento si preveda soprattutto l'uso testuale).

È importante notare che **l'ambito non comprende decisioni automatizzate** con effetti giuridici sui minori: l'IA verrà utilizzata come supporto e strumento creativo, non per sostituirsi al giudizio umano in materia disciplinare o valutativa. Ad esempio, non saranno delegati all'IA compiti quali assegnazione di voti o ammissione a corsi, utilizzi che invece sarebbero classificati ad alto rischio e soggetti a rigidi divieti (come evidenziato dalle linee guida ministeriali).

Supporto tecnico e fornitori coinvolti: i fornitori delle soluzioni di IA generativa agiranno tipicamente quali **Responsabili del Trattamento** per conto della scuola, trattando i dati secondo le istruzioni fornite contrattualmente. In allegato (Allegato 1 – *Tabella comparativa dei fornitori di IA generativa valutati*) è riportato un confronto neutro tra diverse piattaforme considerate (ad es. Gemini, Microsoft 365 Copilot, Canva Magic Write, Adobe Firefly, OpenAI ChatGPT, etc.), con informazioni sulle rispettive caratteristiche, sedi dei server, politiche

privacy e misure di sicurezza implementate. Tale tabella funge da documentazione di due diligence e guida la scelta delle piattaforme ammesse all'uso in istituto.

In sintesi, **Scenario A** comporta trattamenti di dati personali molto limitati (principalmente dati del personale e dati di servizio), mentre **Scenario B** implica il trattamento di dati riferiti agli interessati (studenti/famiglie) e sarà quindi oggetto di un'analisi più approfondita dei rischi. Entrambi gli scenari verranno gestiti in conformità alle normative vigenti e ai princìpi di necessità e proporzionalità descritti di seguito.

4. Valutazione della necessità e proporzionalità

Necessità del trattamento: L'introduzione di strumenti di Intelligenza Artificiale generativa si inserisce nel quadro delle politiche di innovazione e digitalizzazione della scuola e può rappresentare una **leva di miglioramento qualitativo** della didattica e dell'organizzazione. In un contesto caratterizzato da classi numerose, crescente eterogeneità dei bisogni formativi e necessità di ottimizzare processi amministrativi e comunicativi, l'utilizzo dell'IA – in forma **sperimentale, controllata e con supervisione umana costante** – può contribuire a rafforzare la capacità del sistema scolastico di rispondere in modo efficace e personalizzato alle esigenze educative, favorendo la partecipazione, l'inclusione e lo sviluppo delle competenze digitali.

Pur non costituendo uno strumento indispensabile, l'adozione di tecnologie di IA generativa può essere considerata **coerente con l'interesse pubblico** sotteso alla funzione educativa e con i compiti istituzionali della scuola volti all'innovazione metodologica e alla qualità dell'insegnamento. In tal senso, il ricorso all'IA non sostituisce il ruolo docente ma ne integra e amplifica le possibilità operative, in coerenza con i principi di **proporzionalità, trasparenza e responsabilità** previsti dal GDPR.

Va inoltre considerato che, ai sensi del principio di **autonomia didattica** sancito dalla normativa scolastica, ciascun docente conserva la libertà di scegliere **le tecniche e le metodologie** più idonee al perseguimento delle finalità educative, mentre la scelta dei **mezzi e degli strumenti** rientra nelle competenze dell'istituzione scolastica, chiamata a garantirne la sicurezza, la conformità normativa e la coerenza con gli obiettivi istituzionali.

Ne consegue che l'amministrazione scolastica **non può in via generale vietare** l'uso di strumenti di IA da parte dei docenti, ma deve **identificare e mettere a disposizione mezzi tecnologici sicuri e conformi** (infrastrutture qualificate, piattaforme certificate, servizi in cloud approvati), in modo che l'esercizio dell'autonomia didattica non esponga l'istituto a rischi di trattamento illecito o di violazione della privacy. Al contrario, l'assenza di mezzi sicuri individuati o la dichiarazione indiscriminata di non conformità potrebbero costituire una **limitazione indebita della libertà didattica**.

Pertanto, la scuola è chiamata a operare in un equilibrio ragionevole tra **tutela dei dati personali e libertà di insegnamento**, assicurando un contesto normativamente sicuro in cui l'utilizzo di strumenti di IA, quando funzionale alle finalità educative, possa svolgersi in modo conforme, trasparente e responsabile.

Va sottolineato che la **necessità** è stata ponderata limitando gli scenari d'uso all'essenziale: l'IA non sarà impiegata in ogni ambito, ma solo dove può apportare un beneficio concreto (ad es. generazione di materiali, supporto individuale allo studente) e sempre come ausilio al

docente, mai in sostituzione integrale. Inoltre, scenario B (quello con dati personali degli studenti) verrà attivato solo se strettamente necessario per la finalità perseguita e dopo aver esplorato soluzioni alternative a minor impatto. Ad esempio, prima di inserire dati reali di studenti in un sistema AI, si valuterà se sia sufficiente utilizzare dati fittizi o anonimizzati a fini di test.

Proporzionalità e minimizzazione: il trattamento proposto è proporzionato rispetto agli obiettivi educativi da raggiungere. Verranno applicati sin dall'inizio i principi di **privacy by design e by default** (art. 25 GDPR), assicurando che:

- **Minimizzazione dei dati:** si utilizzerà la **minima quantità di dati personali** necessaria. Scenario A dimostra come molte funzionalità dell'IA possano essere sfruttate senza alcun dato personale degli studenti. Anche nello scenario B, si limiteranno le informazioni fornite all'IA (es.: usare solo dati strettamente rilevanti per l'attività didattica specifica, evitando di inserire interi database di informazioni personali). Il personale sarà istruito a *non caricare dati sensibili o identificativi se non indispensabili*.
- **Limitazione delle finalità:** i dati eventualmente trattati dagli strumenti di IA saranno usati esclusivamente per le finalità didattiche/organizzative descritte e non ulteriormente trattati per scopi incompatibili. I fornitori dovranno contrattualmente garantire di non utilizzare i dati della scuola per fini propri (es. addestramento dei loro modelli su dati degli studenti) al di fuori di quanto autorizzato.
- **Conservazione proporzionata:** i dati personali eventualmente forniti all'IA (es. brani di testo studente) non saranno conservati dalla scuola oltre il tempo necessario all'elaborazione. Se il sistema IA conserva tracce delle elaborazioni nel suo cloud, la scuola verificherà i tempi di retention dichiarati dal fornitore e richiederà che siano coerenti con le esigenze (es. cancellazione dei dati grezzi dopo l'output generato).
- **Accesso controllato:** l'accesso ai servizi di IA sarà consentito solo a utenti autenticati (docenti, studenti autorizzati, personale) nell'ambito delle loro mansioni o attività didattiche. Ogni utente avrà credenziali individuali; non sono previste elaborazioni aperte al pubblico esterno.
- **Trasparenza verso gli interessati:** gli studenti (e i loro genitori) verranno informati in modo chiaro sull'utilizzo di IA nel processo formativo, spiegando le modalità e scopi. In caso di interazione diretta con un chatbot o sistema generativo, l'utente sarà sempre messo a conoscenza del fatto che sta dialogando con un'IA. Inoltre, i docenti segnaleranno quando forniscono contenuti generati dall'IA come supporto, così che vi sia consapevolezza e si possano segnalare eventuali errori.

Nella valutazione di proporzionalità si è tenuto conto anche delle possibili implicazioni etiche ed educative: l'uso dell'IA non deve ledere la centralità del rapporto umano docente-studente né introdurre bias o discriminazioni. Per questo, l'IA verrà usata come *strumento complementare*. Ogni output generato sarà vagliato criticamente da un insegnante prima di essere utilizzato in classe o comunicato agli studenti. Questo garantisce anche l'aderenza al principio che *"il controllo finale rimane umano"*, evitando effetti eccessivamente invasivi o automatizzati.

Si ritiene, alla luce di quanto sopra, che i trattamenti siano **necessari** per perseguire gli scopi legittimi dell'istituto e **proporzionati** in relazione ai potenziali impatti sugli interessati, poiché

configurati in modo da ridurre al minimo tali impatti. La DPIA prosegue verificando in dettaglio i rischi residui e le misure adottate per mantenerli a un livello accettabile.

5. Analisi dei rischi (Scenario A e Scenario B)

In questa sezione si analizzano i principali rischi per i diritti e le libertà delle persone interessate associati all'uso degli strumenti di IA generativa, distinguendo tra **Scenario A** (uso senza dati personali di terzi) e **Scenario B** (uso con dati personali di terzi). Per ciascuno scenario sono valutati sia i rischi di natura **operativa** (legati a processi e comportamenti umani) sia quelli di natura **IT** (tecnologici e di sicurezza informatica).

Si premette che, pur presentando profili di rischio diversi, **entrambi gli scenari ricadono nell'ambito di applicazione del GDPR**. Anche quando l'IA viene usata senza dati di terzi, infatti, possono comunque essere coinvolti dati personali (come quelli del docente che interagisce col sistema, o dati non strutturati che l'IA può generare/combinare). Scenario A va dunque considerato *a rischio ridotto*, ma non esente da ogni rischio; scenario B comporta rischi più elevati e richiede cautele maggiori.

Scenario A: Uso di IA senza dati personali di terzi

Descrizione scenario A: il docente o personale utilizza la piattaforma di IA per scopi di servizio (es. preparare materiale didattico) senza inserire informazioni riferite a studenti specifici o altri soggetti esterni. I dati trattati dall'IA sono in questo caso perlopiù testo o richieste generiche fornite dall'operatore umano. Gli unici dati personali coinvolti direttamente sono quelli dell'operatore stesso (identificato come utente del servizio).

Principali rischi in Scenario A:

- **R1. Violazione della riservatezza dei dati dell'utente (docente/personale):** poiché l'accesso all'IA avviene tramite account, esiste il rischio che i **dati personali del personale** (es. nome, email, ruolo associato all'account, eventualmente contenuti delle richieste fatte) possano essere **acceduti o divulgati indebitamente**. Ciò potrebbe avvenire in caso di attacco informatico al fornitore dell'IA (data breach) o di accesso abusivo da parte di terzi. Anche senza terzi, va considerato che le richieste e interazioni del docente con l'IA potrebbero essere memorizzate nel cloud del fornitore: se non adeguatamente protette, un malfunzionamento o errore potrebbe esporle. *Impatto:* esposizione di informazioni relative all'attività professionale del docente o alla scuola (es. materiale didattico in bozza) con possibile violazione di confidenzialità. *Minacce/fonte di rischio:* attori malevoli esterni (hacker), vulnerabilità del sistema cloud, errore umano del docente (es. utilizzare reti insicure).
- **R2. Uso improprio o fuga di contenuti generati:** i contenuti creati dall'IA (es. un test, una circolare bozza) potrebbero contenere informazioni che, se diffuse prematuramente o non corrette, possono causare problemi (es. un quiz potrebbe rivelare domande d'esame). C'è rischio **operativo** se il personale non gestisce correttamente questi output (ad es. condividendoli inavvertitamente in rete o con persone non autorizzate). *Impatto:* potrebbe compromettere l'integrità del processo didattico (esami) o l'immagine dell'istituto se bozze inadeguate circolano. *Minacce:* negligenza o scarsa formazione del personale nell'uso degli strumenti (errore umano).

- **R3. Dipendenza tecnologica e continuità operativa:** se i docenti fanno affidamento sull'IA per preparare materiali in tempi stretti, un'eventuale **indisponibilità del servizio** (down di piattaforma, problemi di connessione) potrebbe creare disservizi nell'attività scolastica. Questo è un rischio più che altro operativo/organizzativo. *Impatto:* ritardi nella preparazione delle lezioni o nella comunicazione, senza però implicazioni dirette sui dati personali (per questo scenario la continuità del servizio è un problema minore di sicurezza, ma comunque considerato).

Valutazione livello di rischio Scenario A: complessivamente, i rischi per la privacy in scenario A sono **moderati**. La potenziale gravità di R1 (data breach) è significativa – una violazione di account docente e relative attività potrebbe esporre anche dati interni della scuola – ma la **probabilità** di tali eventi, con adeguate misure di sicurezza, è ritenuta **bassa** (vedi sez. 6 per misure mitigative: cifratura, autenticazione ecc.). R2 comporta un impatto più sull'integrità/qualità dei dati che sulla privacy in senso stretto, ed è mitigabile con formazione (abbassandone la probabilità). R3, come detto, ha impatto principalmente organizzativo e viene qui menzionato solo per completezza, avendo riflessi indiretti sulla missione educativa (non incide su diritti/future libertà in termini GDPR, dunque non alza il rischio privacy residuo).

In sintesi, scenario A **non presenta rischi elevati per i diritti dei soggetti** se gestito con le dovute cautele, ma richiede comunque misure base di sicurezza ICT e buone prassi d'uso per evitare anche minimi incidenti.

Scenario B: Uso di IA con dati personali di terzi (studenti/famiglie)

Descrizione scenario B: il personale fornisce all'IA dati personali riguardanti studenti o loro familiari, per ottenere un risultato specifico (es. analisi di testi studenteschi, elaborazione di report individuali, traduzione/riassunto di documenti contenenti dati personali). In questo scenario, quindi, dati di **persone fisiche identificate** entrano nel sistema di IA e vengono processati da un fornitore esterno in cloud.

Principali rischi in Scenario B:

- **R4. Violazione di riservatezza dei dati degli interessati:** questo è il rischio più significativo. Coinvolgendo dati di minori e famiglie, un **data breach** o un accesso non autorizzato ai dati potrebbe avere impatti gravi. Ad esempio, se venissero immessi nel sistema nomi di studenti associati a valutazioni o note disciplinari, la divulgazione non autorizzata di tali informazioni lederebbe la privacy e potrebbe causare danni emotivi o reputazionali agli interessati. *Impatto:* elevato – divulgazione di dati personali (anche potenzialmente "particolari", se presenti) di minori a soggetti non autorizzati, con possibili conseguenze sulle loro vite (stigma, disagio, ecc.). *Minacce e fonti:* vulnerabilità del servizio di IA (intrusione hacker, mancata cifratura), politiche inadeguate del fornitore (es. salvataggio di dati su server extra-UE senza garanzie, con rischio di accesso da giurisdizioni non equivalenti), nonché **errore umano** da parte del personale (es. inserimento per sbaglio di dati personali in prompt che dovrebbero essere anonimi). Il rischio di accesso abusivo ai sistemi cloud e relative conseguenze è riconosciuto come scenario temuto in soluzioni cloud ad elevato rischio.
- **R5. Uso secondario non autorizzato dei dati da parte del fornitore:** molti servizi di IA generativa **conservano ed elaborano i dati forniti dagli utenti per migliorare il modello** o per altri scopi. Se la scuola immette dati di studenti, c'è il rischio che il provider

li utilizzi al di fuori delle finalità consentite, ad esempio includendoli nel training generale dell'AI o condividendoli (in forma non adeguatamente anonimizzata) con terze parti. *Impatto:* violazione del principio di limitazione della finalità e potenziale esposizione futura dei dati (un modello potrebbe persino rigenerare parte di un testo contenente dati personali in risposte ad altri utenti, se quei dati sono stati inglobati nel suo training – scenario remoto ma da considerare). *Minacce:* clausole contrattuali opache, policy del fornitore che prevedano cessione dati a terzi o archiviazione in paesi terzi senza tutele. Se il provider non viene nominato formalmente Responsabile del trattamento ex art. 28 GDPR, potrebbe trattare i dati come Titolare, aumentando il rischio di usi non controllati.

- **R6. Rischi di bias, errore o output inappropriato riferito a persone:** fornendo all'IA dati personali, ad esempio descrizioni di studenti, c'è il rischio che l'IA restituisca *output inesatti, distorti o discriminatori* riguardanti quelle persone. Esempio: se un docente chiedesse all'AI di valutare automaticamente il profilo di uno studente in base ai dati inseriti, il modello potrebbe generare un giudizio erroneo o influenzato da bias (non avendo reali capacità valutative umane). Questo potrebbe portare a decisioni ingiuste (se il personale si fidasse acriticamente dell'output) o alla diffusione di informazioni inesatte sull'interessato. *Impatto:* lesione dei diritti dello studente (es. diritto a una valutazione corretta, diritto alla non discriminazione), potenzialmente anche un impatto psicologico se tali output fossero comunicati. *Minacce:* opacità degli algoritmi, dataset di training non neutri, mancanza di supervisione umana critica. In ambito scolastico le linee guida ministeriali sottolineano l'importanza di evitare decisioni algoritmiche non corrette e di affidarsi sempre al controllo umano qualificato.
- **R7. Violazione dei diritti degli interessati (informativa, accesso, ecc.):** introducendo un trattamento nuovo come l'IA, la scuola deve assicurare il rispetto dei diritti privacy degli interessati. Un rischio è che non siano adeguatamente informati (violando il dovere di trasparenza) o che non possano esercitare il diritto di accesso/cancellazione sui dati dati passati all'IA. Ad esempio, se i genitori chiedono di sapere se e quali dati del figlio sono stati processati da IA, la scuola deve poterlo riferire; se chiedono cancellazione, occorre valutare come soddisfarla anche presso il fornitore. *Impatto:* erosione della fiducia nell'istituzione, potenziale illiceità del trattamento. *Minacce:* mancanza di procedure interne per gestire tali richieste, contratti con fornitori che non prevedono assistenza nell'esercizio dei diritti, oppure semplice dimenticanza di aggiornare l'informativa verso gli interessati circa questi nuovi usi.

Valutazione livello di rischio Scenario B: i rischi sopra descritti, se non mitigati, **possono comportare un livello di rischio intrinsecamente alto**, dato che coinvolgono minori e potenziali trattamenti su larga scala tramite un sistema esterno. In particolare R4 (data breach di dati di minori) ha gravità massima e probabilità da stimare con attenzione: sebbene eventi di violazione massiva non siano frequenti, non sono nemmeno teorici – in quanto sono noti casi analoghi avvenuti in passato. La probabilità di un incidente per R4 viene valutata *moderata* (non trascurabile) considerando la superficie d'attacco (servizi cloud accessibili via internet) e la possibile attrattività di dati scolastici, ma verrà abbassata con misure di sicurezza e scelte oculate di fornitori (vedi sez. 6). R5 attiene a compliance e governance: la gravità qui dipende da cosa potrebbe fare il fornitore con i dati – potenzialmente elevata se li riutilizzasse impropriamente. Tuttavia, si prevede di ridurre drasticamente la *probabilità* di R5 scegliendo solo fornitori con chiare garanzie contrattuali (probabilità residua bassa). R6 e R7 riguardano soprattutto correttezza e diritti: si possono mitigare con formazione e procedure, portando questi rischi a un livello *medio-basso residuo*.

Complessivamente, **Scenario B presenta rischi residui potenzialmente significativi**, ma gestibili attraverso le misure tecniche e organizzative descritte oltre. Di fondamentale importanza è il controllo umano e l'adozione di regole interne che impediscano usi impropri: ad esempio, **Scenario B non deve mai degenerare in un affidamento all'IA di decisioni su studenti**; l'IA resta consulente e non decisore. Seguendo questo principio e applicando le tutele, lo scenario B può essere mantenuto entro un livello di rischio accettabile per la privacy. In ogni caso, il fatto stesso di utilizzare dati personali di minori fa sì che la situazione debba essere costantemente rivalutata: se emergessero nuovi rischi o utilizzi non previsti, la DPIA andrà aggiornata.

(Segue nel prossimo paragrafo l'elenco delle misure di mitigazione implementate o pianificate per affrontare i rischi di cui sopra.)

6. Misure tecniche e organizzative adottate o previste

Alla luce dei rischi individuati, la scuola ha definito un insieme articolato di **misure di sicurezza, tecniche ed organizzative**, per prevenire o mitigare gli impatti negativi sull'integrità, riservatezza e disponibilità dei dati personali trattati mediante IA generativa. Tali misure si ispirano ai principi del GDPR e alle best practice indicate dalle autorità (Garante, AgID, ACN, MIM). Di seguito le principali:

Misure organizzative e di governance:

- **Policy interna e codice di condotta d'uso:** verrà emanata una specifica **istruzione di servizio/regolamento interno** che disciplina l'utilizzo degli strumenti di IA da parte di docenti e personale. Tale policy definirà quali dati possono o non possono essere inseriti nelle piattaforme (vietando, ad esempio, di fornire dati identificativi degli studenti a sistemi non autorizzati, o qualsiasi dato sensibile), nonché le finalità ammesse. Il Dirigente Scolastico supervisionerà il rispetto di queste regole. Saranno previste sanzioni disciplinari in caso di uso difforme, in modo da responsabilizzare gli operatori.
- **Formazione e sensibilizzazione:** tutti gli utilizzatori (docenti, personale e eventualmente studenti coinvolti) riceveranno formazione specifica sull'uso consapevole dell'IA. I docenti saranno formati a **valutare criticamente gli output** (riconoscere errori o bias algoritmici), a proteggere le credenziali e a seguire le linee guida interne per l'inserimento dei dati. Agli studenti verrà insegnato un approccio critico all'IA, sottolineando le potenzialità ma anche i limiti (esempio: spiegare il concetto di *"allucinazione"* dell'IA, cioè risposte errate spacciate per corrette). La consapevolezza è una delle misure chiave per ridurre il rischio di errore umano.
- **Due diligence sui fornitori e whitelist interna:** prima di adottare qualsiasi piattaforma di IA, la scuola effettua una rigorosa **valutazione preventiva del fornitore** in termini di conformità normativa, sicurezza e protezione dati. Sono stati analizzati i termini d'uso, le policy sul trattamento dei dati (verificando se c'è condivisione con terzi, finalità ulteriori, trasferimenti extra-UE) e le certificazioni eventualmente possedute (ad es. conformità ISO/IEC 27001 per la sicurezza, adherence al GDPR, ecc.). Solo i fornitori che **garantiscono adeguate misure tecniche e organizzative** (come richiesto dall'art. 28 GDPR) e accettano di sottoscrivere un accordo di nomina a Responsabile del Trattamento vengono inseriti in una **"white list" interna** di servizi approvati. La scelta privilegerà servizi **accreditati per la PA**: come da circolare AgID 2/2018 e successive disposizioni ACN, l'istituto utilizzerà esclusivamente **servizi cloud qualificati** e presenti

nel Marketplace Cloud per la PA. Questo assicura standard minimi di sicurezza e affidabilità.

- **Accordi contrattuali e nomina a Responsabile (Art. 28 GDPR):** con ciascun fornitore approvato sarà formalizzato un contratto o **Addendum GDPR** che specifichi gli obblighi di riservatezza, sicurezza e assistenza al titolare. In particolare, i fornitori dovranno: utilizzare i dati **solo per erogare il servizio richiesto**, **non conservarli oltre il necessario**, non comunicarli ulteriormente senza istruzioni, adottare misure di sicurezza idonee (cifratura, controllo accessi, etc.), assistere la scuola nel gestire richieste di esercizio dei diritti da parte degli interessati e nel caso di data breach. Verrà verificato che i termini di servizio non contengano clausole lesive (es. *data mining* a fini propri). La **nomina formale a Responsabile del Trattamento** sarà effettuata ai sensi dell'art. 28(3) GDPR, includendo anche eventuali sub-responsabili (es. partner cloud) nel rispetto della catena di fornitura.
- **Limitazione degli scenari d'uso:** operativamente, si è deciso di **limitare scenario B** (IA con dati personali degli studenti) a pochi casi sperimentali e comunque opzionali. Ad esempio, se si volesse provare un correttore automatico di elaborati, ciò verrà fatto solo previo consenso informato del docente responsabile e con notifica ai genitori, offrendo eventualmente un opt-out. In generale, l'IA sarà prima sfruttata nei casi *no data personali*; solo qualora emergano forti vantaggi didattici si passerà a scenario B, e anche in quel caso **con il minor coinvolgimento di dati identificativi possibile** (preferendo magari dare in pasto all'IA testi anonimi o pseudonimizzati).
- **Monitoraggio e revisione:** la scuola istituirà un meccanismo di **monitoraggio continuo** sull'uso delle piattaforme AI. Il Responsabile Protezione Dati (RPD/DPO) verrà coinvolto nelle valutazioni iniziali e vigilerà successivamente sul rispetto delle misure. Saranno effettuati audit periodici sull'aderenza delle pratiche alla DPIA. Inoltre, qualsiasi incidente o anomalia verrà registrato e analizzato (registro dei data breach, anche se minori) e la DPIA sarà aggiornata in caso di modifiche sostanziali o nuovi rischi individuati.

Misure tecniche di sicurezza:

- **Autenticazione forte e gestione degli accessi:** l'accesso alle piattaforme di IA avverrà tramite autenticazione robusta. Dove possibile, sarà attivata l'**autenticazione a più fattori (MFA)** per gli account dei docenti/personale, riducendo il rischio di accessi non autorizzati (mitigazione R1, R4). I privilegi sulle piattaforme saranno configurati in base al ruolo: ad esempio, un eventuale account studente avrebbe permessi limitati e supervisione.
- **Cifratura dei dati e delle comunicazioni:** tutte le comunicazioni con i servizi cloud di IA saranno protette tramite crittografia TLS/HTTPS. Se i fornitori lo supportano, verrà richiesta la **cifratura end-to-end o at-rest** dei dati sensibili caricati (es. documenti). Così, anche in caso di intercettazione o accesso illecito, i dati sarebbero illeggibili senza chiavi (mitigazione R4).
- **Protezione dei dispositivi e reti:** i dispositivi utilizzati per accedere all'IA (PC della scuola, tablet) dovranno rispettare le policy di sicurezza dell'istituto: aggiornamenti regolari, antivirus/antimalware attivi, configurazioni che impediscano salvataggi non sicuri di dati. Le connessioni da rete esterna (es. docente da casa) dovranno avvenire

preferibilmente tramite **VPN istituzionale** o comunque con canali cifrati. Queste misure riducono i rischi di intrusione e di esposizione accidentale di dati.

- **Limitazione e pseudonimizzazione dei dati in input:** a livello pratico, si adotterà un accorgimento tecnico-organizzativo fondamentale: **fornire ai sistemi IA il minor dato personale possibile**. Ad esempio, se si chiede all'IA di correggere un compito, prima di inviarlo si potrà rimuovere nome dello studente e altri identificativi (pseudonimizzazione). Oppure, se si sperimenta un AI per report, si potrebbe assegnare un **ID fittizio** agli studenti invece di usare il nome reale, e poi riconciliare i risultati internamente. Ciò garantisce che il fornitore non riceva direttamente dati identificativi, riducendo l'impatto di eventuali violazioni (mitigazione R4, R5).
- **Storage e trasferimenti conformi (no extra-UE non protetti):** la scelta dei fornitori terrà conto della localizzazione dei server. Si privilegiano servizi con data center nell'Unione Europea. Se dovessero essere coinvolti trasferimenti di dati fuori dallo Spazio Economico Europeo, questi **saranno coperti da adeguate garanzie** (decisione di adeguatezza UE, Standard Contractual Clauses, Binding Corporate Rules, ecc.) in conformità agli artt. 44-49 GDPR. Si eviterà di utilizzare servizi noti per inviare dati in paesi privi di garanzie, a meno di consenso esplicito o altra base legittima. Inoltre, come da indicazioni, si porrà **particolare attenzione alle policy sulla cessione a terzi e salvataggio extra-UE** dei dati da parte dei cloud provider, vietando contrattualmente ogni sub-trasferimento non autorizzato.
- **Backup e resilienza:** benché scenario A e B non prevedano archiviazione primaria di dati personali critici nell'IA (che è usata più come transito/elaborazione), l'istituto garantirà che i dati originali (es. compiti studente caricati) restino disponibili nei propri sistemi. I contenuti generati importanti saranno copiati o salvati sui server scolastici se necessario. In caso di indisponibilità del servizio cloud, esisteranno modalità alternative per portare avanti la didattica, assicurando continuità senza perdita di dati (questo attiene più alla disponibilità operativa).
- **Test e valutazione pre-rilascio:** prima di un uso esteso, qualsiasi applicazione di IA verrà testata in ambiente controllato, preferibilmente con **dati fittizi**, per valutare il comportamento del sistema. Si controllerà quali dati registra, se ci sono output imprevisti, e si valuteranno eventuali rischi non emersi teoricamente. Questo consente di correggere configurazioni o decidere di non usare affatto una soluzione che si dimostri troppo rischiosa.

Misure a tutela dei diritti e della compliance GDPR:

- **Informativa e consenso (se necessario):** l'informativa privacy dell'istituto sarà aggiornata per descrivere chiaramente questi nuovi trattamenti con IA, specificando finalità, base giuridica (presumibilmente l'esecuzione del compito di interesse pubblico della scuola, ex art. 6(1) e GDPR, per scenario B) e diritti degli interessati. Per attività non coperte da obblighi normativi e soprattutto se vi è coinvolgimento di dati sensibili, si valuterà di ottenere un **consenso** esplicito dai genitori/tutori, se questo risulta la base giuridica più opportuna. In generale, cercheremo di fondare il trattamento su basi giuridiche solide (adempimento dei compiti istituzionali), usando il consenso solo per funzionalità opzionali.
- **Gestione delle richieste degli interessati:** il personale dell'istituto e i referenti privacy saranno preparati a gestire eventuali richieste di accesso, rettifica o cancellazione

relative ai dati trattati dall'IA. Sarà mantenuto un **registro delle attività** svolte con IA (almeno a livello di categorie di dati e finalità) per poter rispondere in modo trasparente. In caso un genitore richieda, ad esempio, la cancellazione di dati caricati su un sistema AI, la scuola si attiverà presso il fornitore (grazie alle clausole contrattuali) affinché quei dati vengano eliminati definitivamente dai suoi sistemi.

- **Data Protection by Design/Default:** come misura generale, ogni nuova implementazione AI passerà dal vaglio del DPO e dei referenti ICT, che applicheranno i principi di minimizzazione e necessità già in fase progettuale. Se, ad esempio, un certo strumento di IA non consente un utilizzo rispettoso dei principi (magari perché obbliga a fornire troppi dati personali), si preferirà non usarlo. Tutte le configurazioni disponibili sulle piattaforme (es. settaggi di privacy, disabilitazione della memorizzazione delle chat quando possibile) saranno impostate per la **massima protezione di default**.

Implementando queste misure, la scuola intende portare i rischi residui a un livello accettabile e garantire un utilizzo dell'IA **sicuro, trasparente e rispettoso** della normativa. Vale la pena ribadire che i fornitori selezionati dovranno mantenere un alto standard: in qualsiasi momento, qualora emergano falle o comportamenti non conformi da parte loro (es. cambio dei termini di servizio in senso peggiorativo), la piattaforma sarà sospesa e, se necessario, sostituita con alternative più affidabili. La *white list* interna sarà un documento dinamico, aggiornato con l'evoluzione tecnologica e regolamentare.

Infine, come ulteriore garanzia, si favorirà l'utilizzo di **dati sintetici o anonimizzati** per scopi di test e configurazione, come raccomandato anche nelle linee guida ministeriali: ciò significa che ogni volta che è possibile addestrare o provare un sistema con dati finti invece che reali, questa opzione sarà perseguita, riducendo drasticamente l'esposizione di dati personali reali.

7. Valutazione residua del rischio e necessità di consultazione preventiva del Garante

Valutazione complessiva del rischio residuo: considerando le misure di mitigazione implementate, il rischio residuo associato ai trattamenti in esame è valutato come **moderato**.

- Per **Scenario A**, il rischio era già basso in partenza e con le misure (policy rigorose, sicurezza account, formazione) diventa **trascurabile/basso**. Non si ravvisano criticità sostanziali per i diritti degli interessati in questo scenario residuo.
- Per **Scenario B**, il rischio intrinseco era più alto, ma grazie alle salvaguardie (limitazione dell'uso, scelte accurate dei fornitori con garanzie, minimizzazione e pseudonimizzazione dei dati inseriti, supervisione umana continua) si ritiene che **nessun rischio residuo elevato** permanga. In particolare, la minaccia di violazione grave di dati di minori (che sarebbe stato l'elemento più preoccupante) è mitigata su più fronti: riduzione della superficie (pochi dati caricati, e spesso pseudonimi), obblighi stringenti sui fornitori, cifratura e controlli accessi. La probabilità stimata di un data breach significativo è ridotta al minimo ragionevole, e anche in tal caso l'impatto sarebbe limitato (esempio: furto di dati anonimi o parziali invece che interi profili). I restanti rischi (bias, errori) sono controllati dal fattore umano e dalla trasparenza, mantenendoli a livello accettabile.

È importante sottolineare che questa valutazione si basa sullo stato attuale delle tecnologie e delle conoscenze. Il DPO ha esaminato i risultati e concorda sul fatto che, con le misure

programmate, il livello di rischio per i diritti e le libertà degli interessati **non è da ritenersi "elevato residuo"** ai sensi dell'art. 36 GDPR. Cioè, non permangono scenari in cui sia probabile che si verifichino danni gravi e irreversibili per le persone, dopo le mitigazioni.

Necessità di consultazione preventiva: dato che il rischio residuo non è elevato, **non si rende necessaria la consultazione preventiva** dell'Autorità Garante prima di procedere con il trattamento (ai sensi dell'art. 36 GDPR). La consultazione preventiva sarebbe obbligatoria solo qualora la DPIA avesse evidenziato un rischio residuo alto non mitigabile. In caso contrario, è sufficiente per il titolare documentare la DPIA (come fatto) e attuare le misure previste. Si rimane comunque disponibili a eventuale confronto con il Garante per chiarimenti o indicazioni se lo stesso Autorità dovesse ritenere opportuno fornire linee guida sul tema specifico.

Va comunque evidenziato che le **Linee Guida del MIM 2025** prevedono, per i sistemi di IA ad alto rischio in ambito educativo, l'obbligo di condurre un'analisi d'impatto integrata che includa anche i diritti fondamentali, e qualora i rischi permangano elevati, di consultare il Garante prima dell'implementazione. Nel nostro caso, come detto, non siamo nella situazione di un sistema ad alto rischio (non affidiamo all'IA decisioni critiche sugli studenti), tuttavia facciamo nostro tale principio: *qualora in futuro la scuola volesse adottare sistemi di IA più invasivi o emergessero nuovi rischi significativi, la DPIA verrebbe aggiornata e, se del caso, si procederebbe a consultazione preventiva del Garante.*

Parere del RPD: il Responsabile della Protezione dei Dati è stato coinvolto durante tutto il processo di valutazione. Il RPD **concorda con le conclusioni** della DPIA, ritenendo che, allo stato attuale e con le misure messe in campo, l'uso degli strumenti di IA generativa possa avvenire nel rispetto della normativa privacy e senza rischio elevato residuo per gli interessati. Il RPD raccomanda di mantenere alta l'attenzione in fase di implementazione pratica, di eseguire test periodici di sicurezza e di aggiornare la DPIA in caso di cambi di scenario.

Conclusioni: questa DPIA ha esaminato in modo approfondito l'introduzione dell'IA generativa a scuola, identificando benefici, rischi e misure di mitigazione. Il **rischio residuo** è giudicato accettabile (medio-basso) e compensato dai vantaggi che l'innovazione può portare al processo educativo, a condizione che tutte le garanzie previste vengano effettivamente applicate. Non emergendo un rischio elevato, non si configura obbligo di consultazione preventiva del Garante. La scuola si impegna comunque a procedere con **cautela e responsabilità**, documentando le scelte, formando gli utenti e vigilando costantemente.

Il presente documento viene firmato dal Titolare del trattamento a conferma dell'analisi svolta.

Luogo, CAGLIARI, (30 GENNAIO 2026)

Il Titolare del Trattamento (Dirigente Scolastico) Prof. Massimo Spiga

Firmato digitalmente

Allegati:
- *Allegato 1:* Tabella comparativa dei fornitori di IA generativa valutati (Gemini, Copilot, Canva, Adobe Firefly, ChatGPT, ecc.) – **documento separato**.