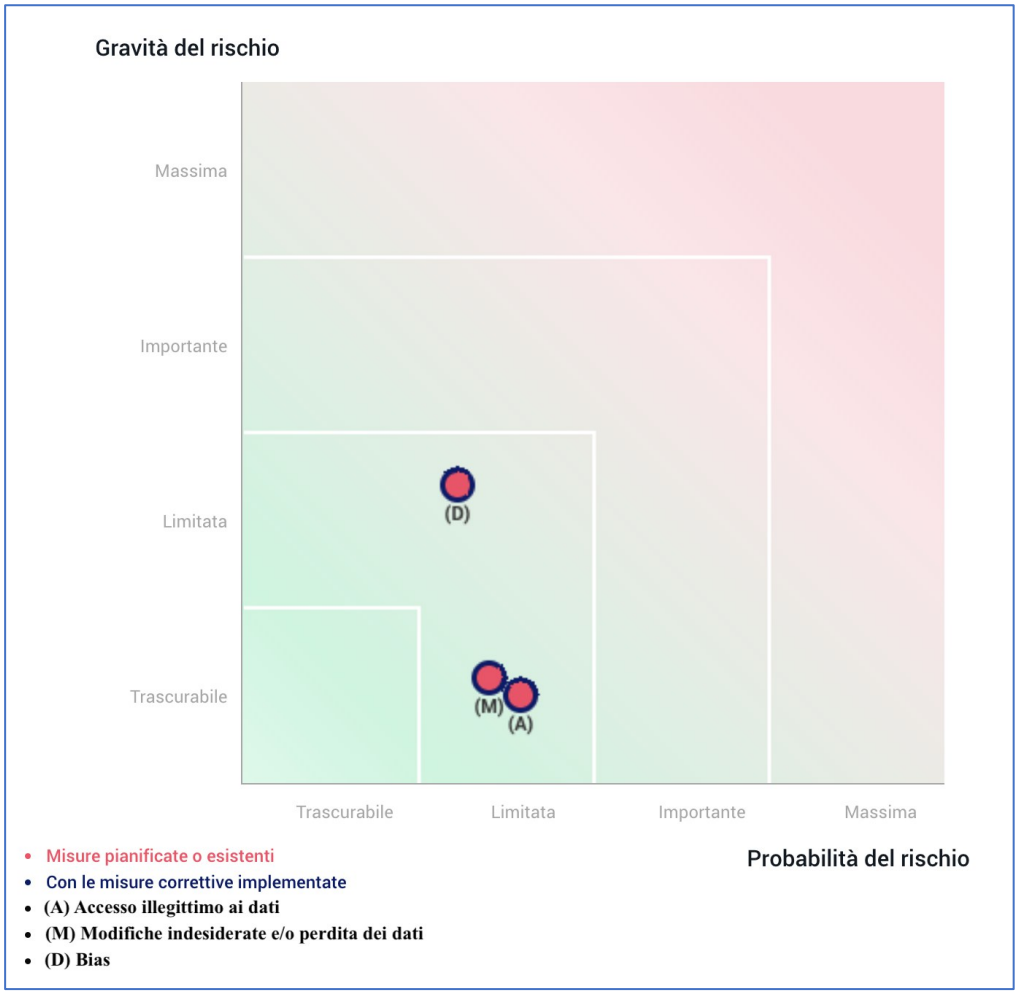
Ministero dell'Istruzione e del Merito
Ufficio Scolastico Regionale per la Lombardia
ISTITUTO COMPRENSIVO MONTE AMIATA
SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI I GRADO
Via Lambro, 92 - 20089 Rozzano (MI)
tel. 028257921 C.F. 97722520158 C.M. MIIC8GG00C
miic8gg00c@istruzione.it – *miic8gg00c@pec.istruzione.it*
www.icsmonteamiata.edu.it

DPIA relativa all'utilizzo di sistemi di IA integrati nell'ecosistema "Google Workspace" in ambiente scolastico

Mappa dei rischi



Opinione del D.P.O. e degli interessati

Nome del DPO/RPD

NetSense S.r.l.

Posizione del DPO/RPD

Il trattamento può essere implementato.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

La mancata richiesta del consenso e del parere preventivo degli interessati in relazione al trattamento dei dati personali connesso all'utilizzo di strumenti di Intelligenza Artificiale si fonda sulla base giuridica individuata nell'art. 6, par. 1, lett. e) del Regolamento (UE) 2016/679, in quanto il trattamento è necessario per l'esecuzione di un compito di interesse pubblico e per l'esercizio di pubblici poteri di cui è investita l'Istituzione scolastica, nonché nell'art. 2-ter del Codice in materia di protezione dei dati personali (D.lgs. 30 giugno 2003, n. 196 e ss.mm.ii.). Una più completa descrizione della base giuridica per l'utilizzo dei sistemi di IA è fornita nel seguito del documento.

In coerenza con le Linee guida del Ministero dell'Istruzione e del Merito e con il Piano di Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), l'adozione e l'impiego degli strumenti di IA rientrano nelle attività istituzionali della scuola e sono deliberati nell'ambito degli organi collegiali competenti, costituendo parte integrante dell'offerta formativa e dell'organizzazione del servizio scolastico**. In tale contesto, il ricorso al consenso degli interessati non risulta giuridicamente appropriato, in quanto potrebbe determinare uno squilibrio tra le parti e compromettere l'uniformità, la continuità e l'effettività del servizio pubblico, né risulta necessario acquisire un parere individuale preventivo, poiché le scelte relative all'adozione degli strumenti digitali e di Intelligenza Artificiale sono assunte a livello istituzionale e regolamentare**.

Resta fermo che l'Istituzione scolastica garantisce in ogni caso il rispetto dei principi di trasparenza, informazione, tutela dei diritti degli interessati e controllo umano sull'utilizzo dei sistemi di Intelligenza Artificiale, assicurando adeguate modalità di comunicazione e di esercizio dei diritti previsti dal GDPR.

Contesto - Panoramica del trattamento

Quale è il trattamento in considerazione?

Nel contesto della progressiva trasformazione digitale del sistema educativo e dell'evoluzione delle metodologie didattiche e organizzative, l'istituzione scolastica ha avviato un percorso strutturato di integrazione dell'Intelligenza Artificiale (IA) nei processi di insegnamento-apprendimento e nelle attività amministrative e gestionali. Tale percorso è definito e regolamentato dal Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), parte integrante del PTOF, e si sviluppa in coerenza con le Linee guida del Ministero dell'Istruzione e del Merito, con il quadro normativo europeo e nazionale in materia di IA e con la disciplina sulla protezione dei dati personali.

Il trattamento oggetto della presente Valutazione d'Impatto riguarda l'utilizzo, da parte dell'istituto scolastico, di **strumenti di Intelligenza Artificiale integrati nell'ecosistema digitale già in uso**, in particolare all'interno di piattaforme di produttività e collaborazione (quali Google Workspace for Education o strumenti analoghi), per finalità didattiche, educative, organizzative e amministrative. L'IA è adottata esclusivamente come **strumento di supporto** alle attività umane e non come sistema decisionale autonomo, nel rispetto del principio di centralità della persona e della supervisione umana.

In ambito didattico, il trattamento consiste nell'impiego di funzionalità di IA a supporto della progettazione delle attività didattiche, della personalizzazione degli apprendimenti, della produzione e rielaborazione di contenuti, del feedback formativo e dell'analisi degli esiti, sempre sotto il controllo e la validazione del docente. Tali strumenti possono essere utilizzati sia dai docenti sia dagli studenti, nell'ambito di attività curricolari ed extracurricolari deliberate dagli organi collegiali, attraverso account istituzionali assegnati dalla scuola e utilizzabili in ambiente scolastico o domestico mediante dispositivi digitali personali o messi a disposizione dall'istituto.

In ambito organizzativo e amministrativo, il trattamento riguarda l'utilizzo di strumenti di IA per il supporto a processi quali la predisposizione di bozze di documenti e comunicazioni, la classificazione e ricerca documentale, l'analisi aggregata di dati relativi a esiti scolastici, frequenze, progettualità e fabbisogni formativi, nonché il supporto alla pianificazione e al monitoraggio delle attività dell'istituto. Anche in tali casi, le operazioni sono svolte con **supervisione costante del personale competente** (Dirigente scolastico, DSGA, assistenti amministrativi) e senza automatizzazione di decisioni che producano effetti giuridici o significativi sugli interessati.

Il trattamento coinvolge dati personali di studenti, docenti, personale ATA e, in misura limitata e pertinente, delle famiglie, trattati nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, limitazione delle finalità e conservazione, nonché di privacy by design e by default. L'istituto utilizza esclusivamente strumenti e configurazioni che escludono funzionalità invasive o non pertinenti, quali la profilazione dettagliata, il riconoscimento delle emozioni o il trattamento non necessario di dati particolari.

L'accesso agli strumenti di IA avviene tramite credenziali istituzionali, con tracciabilità delle operazioni e nel rispetto delle policy interne sull'uso delle tecnologie digitali. Gli utenti sono preventivamente informati sulle finalità, le modalità e i limiti del trattamento, nonché sui rischi connessi all'uso dell'IA, attraverso informative, regolamenti di istituto e attività formative previste dal PUIA.

La presente DPIA è pertanto finalizzata ad analizzare in modo sistematico i rischi per i diritti e le libertà degli interessati derivanti dall'utilizzo di strumenti di Intelligenza Artificiale nel contesto scolastico, nonché a individuare e valutare le misure tecniche e organizzative adottate dall'istituto per prevenire e mitigare tali rischi, assicurando che l'innovazione tecnologica si sviluppi in modo coerente con la tutela dei dati personali, la sicurezza delle informazioni e i principi etici e pedagogici richiamati nel PUIA.

Quali sono le responsabilità connesse al trattamento?

In considerazione della complessità dei trattamenti di dati personali connessi all'utilizzo di strumenti di Intelligenza Artificiale in ambito scolastico, nonché dei potenziali impatti sui diritti e sulle libertà degli interessati, l'istituto definisce un sistema di responsabilità chiaro e coerente con il **Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA)**. La presente DPIA declina operativamente tale sistema di governance, individuando ruoli, compiti e responsabilità dei soggetti coinvolti nel trattamento, in conformità al Regolamento (UE) 2016/679 e alla normativa nazionale.

1. **Il Titolare del Trattamento**: In questo caso, l'Amministrazione Scolastica rappresentata dal Dirigente Scolastico in carica. Il Dirigente assume un ruolo centrale di supervisione e guida nei confronti delle altre parti coinvolte. La sua responsabilità principale è garantire una gestione adeguata dei dati e dei sistemi informatici ed esercitare una funzione di indirizzo strategico, supervisione e responsabilità ultima, come previsto dal PUIA.

2. **Responsabili del Trattamento ai sensi dell'art. 28 del GDPR**: In accordo con quanto previsto dall'articolo 28 del GDPR, il Titolare del Trattamento sceglie fornitori di sistemi di IA che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del GDPR e a garantire la tutela dei diritti dell'interessato. Essi hanno la responsabilità di trattare i dati in modo sicuro e conforme alle disposizioni normative, sulla base di un accordo redatto di Responsabile del Trattamento ai sensi dall'articolo 28 del GDPR. Si ricorda inoltre che le Pubbliche amministrazioni possono avvalersi esclusivamente di fornitori qualificati per i servizi digitali della Pubblica Amministrazione (PA), che prima seguivano le regole AGID (Agenzia per l'Italia Digitale) e ora sono gestite e qualificate dall'ACN (Agenzia per la Cybersicurezza Nazionale) per garantire sicurezza e affidabilità con processi che prevedono requisiti stringenti definiti da decreti e circolari. Nel caso in questione il Responsabile esterno è la Google LLC con sede in Mountain View in California (USA).

3. **I docenti**: in qualità di soggetti autorizzati al trattamento, svolgono un ruolo centrale nell'attuazione concreta del PUIA in ambito didattico. Essi sono responsabili di: utilizzare gli strumenti di IA nel rispetto delle finalità, dei limiti e delle modalità definiti dal PUIA, dal Regolamento di istituto per l'uso della IA e dalla presente DPIA; garantire la riservatezza dei dati personali degli studenti nella gestione di materiali didattici, comunicazioni e interazioni online; verificare e validare i contenuti e i risultati prodotti dagli strumenti di IA, evitando un uso acritico o automatico; informare e formare gli studenti sul corretto utilizzo degli strumenti digitali e sull'importanza della tutela della privacy e dei dati personali.

In coerenza con il PUIA, i docenti mantengono sempre la responsabilità professionale delle scelte didattiche e valutative, che non possono essere delegate ai sistemi di IA.

4. **Il Responsabile della Protezione dei Dati (RPD)**: ha il compito di fornire supporto a titolare, docenti e interessati, per tutte quelle questioni concernenti la protezione dei dati personali all'interno dell'ambito di applicazione del trattamento.

5. **Amministratori di sistema:** persone fisiche designate dal DS ai sensi dell'art. 2-quaterdecies del Codice in materia di protezione dei dati personali (Dlgs 196/2003 e s..mm.ii.) quali soggetti che operano sotto la sua autorità a cui sono attribuiti specifici compiti e funzioni connessi al trattamento relativamente alla gestione tecnica e della sicurezza dei sistemi informativi. Essi garantiscono la corretta configurazione degli ambienti digitali e delle piattaforme che integrano funzionalità di IA; assicurano il controllo degli accessi, la tracciabilità delle operazioni e l'adozione di misure di sicurezza adeguate; collaborano con il Titolare e con il RPD nella prevenzione e gestione di eventuali incidenti di sicurezza o violazioni dei dati personali.

La collaborazione strutturata tra tutti i soggetti sopra indicati, così come delineata nel PUIA e attuata attraverso la presente DPIA, rappresenta un elemento essenziale per garantire un uso consapevole, sicuro e conforme alla normativa degli strumenti di Intelligenza Artificiale nel contesto scolastico, assicurando che l'innovazione digitale sia sempre accompagnata dalla tutela effettiva dei diritti e delle libertà fondamentali degli interessati.

Ci sono standard applicabili al trattamento?

Attualmente non sono stati individuati standard, certificazioni o codici di condotta pertinenti alla questione in esame. Di conseguenza, al fine di stabilire le misure tecniche ed organizzative da implementare per rispettare i principi del Regolamento, è essenziale far riferimento, oltre alle direttive stabilite dalla normativa vigente (tra le quali si citano l'AI ACT "Regolamento (UE) 2024/1689" e la legge 132 del 23/09/2025 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale") anche alle seguenti linee guida: le Linee guida del Garante europeo del 3 giugno 2024 e le Linee guida del MIM per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche.

Contesto - Dati, processi e risorse di supporto

Quali sono i dati trattati?

Gli strumenti di IA trattano esclusivamente dati personali comuni, già ricompresi nella DPIA Google Workspace, quali: dati identificativi degli account istituzionali; contenuti didattici e materiali di lavoro prodotti dagli utenti; dati relativi all'attività scolastica e amministrativa. Non è previsto il trattamento di categorie particolari di dati personali ai sensi dell'art. 9 del GDPR.

In ogni caso, anche semplicemente in presenza di dati comuni, si applica rigorosamente il principio di **minimizzazione dei dati** così come anche puntualizzato dalle linee guida del MIM.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il trattamento dei dati personali connesso all'utilizzo di strumenti di Intelligenza Artificiale è organizzato secondo un modello basato su casi d'uso specifici, in coerenza con le Linee guida del Ministero dell'Istruzione e del Merito e con il Piano di Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), e si sviluppa lungo un ciclo di vita articolato in diverse fasi, ciascuna delle quali comporta potenziali rischi per i diritti e le libertà degli interessati.

Il ciclo di vita del trattamento non riguarda in modo indistinto la tecnologia di IA nel suo complesso, ma ciascun caso d'uso individuato dall'Istituzione scolastica, che viene preliminarmente definito in termini di finalità, soggetti coinvolti e attività supportate, valutato sotto il profilo della necessità, della proporzionalità e della coerenza con il PTOF e con la presente DPIA, e attivato esclusivamente qualora risulti compatibile con il quadro organizzativo e normativo di riferimento.

Nelle fasi iniziali del trattamento, gli studenti accedono ai servizi di IA mediante l'utilizzo di dispositivi personali o di dispositivi forniti in comodato d'uso dalla scuola, mentre l'Istituzione scolastica provvede alla creazione e alla gestione degli account per docenti, studenti e personale ATA attraverso la piattaforma di gestione dei profili autorizzati all'uso dell'IA, assicurando che l'accesso avvenga nel rispetto dei principi di liceità, minimizzazione e sicurezza. Per ciascun caso d'uso autorizzato, l'impiego degli strumenti di IA avviene in forma supervisionata, con controllo umano costante sugli output prodotti e con modalità di utilizzo differenziate in funzione dell'età degli studenti e del contesto educativo, limitando le funzionalità alle sole strettamente necessarie al perseguimento delle finalità dichiarate.

Nel corso dell'utilizzo, l'Istituto effettua un monitoraggio periodico finalizzato a verificare il rispetto delle finalità, a prevenire utilizzi impropri e a individuare eventuali criticità, prevedendo la possibilità di sospendere o cessare il trattamento qualora emergano rischi non adeguatamente mitigabili.

Al termine del caso d'uso, o qualora venga meno la necessità che ne ha giustificato l'attivazione, l'accesso agli strumenti è disattivato e i dati personali trattati sono cancellati, anonimizzati o conservati esclusivamente per il tempo strettamente necessario, nel rispetto dei principi di limitazione della conservazione e di responsabilizzazione, fermo restando che ogni prosecuzione o modifica sostanziale del caso d'uso è subordinata a una nuova valutazione preventiva dell'impatto sul trattamento dei dati personali.

Quali sono le risorse di supporto ai dati?

Di solito, si utilizzano servizi basati su cloud per agevolare la condivisione e l'organizzazione dei compiti assegnati. Queste tecnologie possono, in alcune occasioni, fare affidamento su server situati al di fuori dell'Unione Europea, ed è di fondamentale importanza verificare che rispettino la normativa europea in materia di gestione dei dati.

Gli utenti accedono a tali servizi utilizzando una vasta gamma di dispositivi informatici, tra cui tablet, computer e smartphone, che possono a loro volta essere basati su diversi sistemi operativi e consentire l'accesso ai servizi tramite vari browser o applicazioni.

Principi Fondamentali - Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono specifici, espliciti e legittimi in quanto l'utilizzo di strumenti e approcci innovativi basati sull'Intelligenza Artificiale e su sistemi digitali online è funzionale al perseguimento delle finalità istituzionali dell'Istituzione scolastica, come definite nel PTOF e nel Piano di Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA).

In ambito didattico e formativo, tali strumenti sono impiegati per promuovere una comprensione consapevole e critica delle tecnologie digitali, per sviluppare competenze di cittadinanza digitale e per potenziare la capacità degli studenti di analizzare, valutare e utilizzare in modo responsabile le fonti informative, favorendo al contempo la personalizzazione degli apprendimenti e l'inclusione.

In ambito organizzativo e amministrativo, l'utilizzo dell'Intelligenza Artificiale è finalizzato a supportare e semplificare i processi interni dell'istituto, migliorando l'efficienza delle attività di segreteria, la gestione documentale, la comunicazione e l'analisi dei dati a supporto delle decisioni, senza sostituire il ruolo professionale e decisionale del personale scolastico e garantendo in ogni caso il controllo umano.

L'obiettivo principale del trattamento resta l'erogazione di un servizio educativo e amministrativo di qualità, efficace ed equo, con il risultato di accrescere le competenze digitali di studenti e personale e di ottimizzare l'organizzazione scolastica nel rispetto dei principi di liceità, proporzionalità e tutela dei diritti degli interessati.

Quale è la base giuridica che rende lecito il trattamento?

La base giuridica per il trattamento in esame risiede nella lettera e) del Regolamento EU 679/2016 (GDPR) "trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", ai sensi di quanto specificato dal codice privacy italiano all'art. 2-ter. Nello specifico, si fa riferimento al quadro strategico europeo in tema di competenze digitali, innovazione educativa e uso responsabile dell'IA, tenendo conto del processo di attuazione del Regolamento europeo sull'Intelligenza Artificiale (AI Act) e delle iniziative UE per l'educazione al digitale e al pensiero critico.

A livello nazionale, il Piano richiama in particolare il quadro normativo che costituisce la base giuridica a supporto dell'utilizzo della IA nelle istituzioni scolastiche:

- il Piano Nazionale Scuola Digitale e i successivi atti di indirizzo per l'innovazione tecnologica nella didattica;

- il PIANO "Scuola 4.0" e le misure del PNRR dedicate alla trasformazione degli ambienti di apprendimento e alle competenze digitali;

- l'AI ACT, Regolamento (UE) 2024/1689 del parlamento europeo e del consiglio del 13 giugno 2024;

- la legge 132 del 23/09/2025, "Disposizioni e deleghe al Governo in materia di intelligenza artificiale".

Il quadro strategico europeo si completa anche con le seguenti linee guida, che sono alla base della stesura del presente documento:

- le Linee guida del Garante europeo del 3 giugno 2024;
- le Linee guida del MIM per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche.

Tali riferimenti costituiscono il quadro di coerenza entro cui l'istituto elabora la propria attività, calibrandola sulle caratteristiche dell'utenza e del contesto territoriale.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati personali trattati sono adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità perseguite, in conformità al principio di minimizzazione di cui all'art. 5, par. 1, lett. c) del GDPR.

L'Istituzione scolastica adotta configurazioni di sicurezza e di utilizzo coerenti con le Linee guida del Ministero dell'Istruzione e del Merito per l'impiego dell'Intelligenza Artificiale a scuola, prevedendo in particolare l'assenza di inserimento intenzionale nei prompt di dati personali non necessari, l'esclusione di funzionalità di profilazione degli utenti e la disattivazione o limitazione delle cronologie di utilizzo, ove non indispensabili alle finalità dichiarate.

Per quanto riguarda la gestione degli account, sono trattati esclusivamente i dati identificativi essenziali, quali nome e cognome dell'utente, senza richiedere il conferimento di informazioni ulteriori come numeri di telefono personali, indirizzi di posta elettronica privati o dati relativi a dispositivi personali. L'accesso ai servizi avviene mediante credenziali istituzionali, nel rispetto dei principi di privacy by design e by default.

Docenti e personale di segreteria sono specificamente istruiti affinché la raccolta e l'utilizzo dei dati personali nell'ambito delle attività didattiche e amministrative supportate dall'Intelligenza Artificiale avvengano nella misura minima necessaria allo svolgimento delle rispettive funzioni, con particolare attenzione all'eventuale trattamento incidentale di dati sensibili, che è evitato ove non strettamente indispensabile e comunque soggetto a misure di cautela rafforzate.

I dati sono esatti e aggiornati?

L'Istituzione scolastica assicura che i dati personali trattati siano esatti e, ove necessario, aggiornati, in conformità al principio di cui all'art. 5, par. 1, lett. d) del GDPR. In particolare, l'amministratore di sistema designato dal Dirigente scolastico ai sensi dell'art. 2-quaterdecies del Codice in materia di protezione dei dati personali è responsabile della correttezza e dell'aggiornamento dei dati identificativi associati agli account di studenti, docenti e personale, provvedendo alle necessarie rettifiche anche a seguito di segnalazioni da parte degli interessati o degli utenti autorizzati.

Per quanto riguarda i dati contenuti nei materiali didattici e amministrativi prodotti in modalità collaborativa, l'esattezza delle informazioni è garantita dal controllo umano esercitato dai soggetti coinvolti nel processo di creazione e revisione, nonché dall'utilizzo di strumenti che consentono la tracciabilità delle modifiche, il versioning dei documenti e il ripristino delle versioni precedenti.

Gli strumenti di Intelligenza Artificiale eventualmente impiegati operano esclusivamente come supporto e non aggiornano né modificano autonomamente dati personali senza la verifica e la validazione da parte del personale scolastico, garantendo così la possibilità di correzione tempestiva di eventuali inesattezze.

Qual è il periodo di conservazione dei dati?

Il periodo di conservazione dei dati personali è definito nel rispetto del principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e) del GDPR ed è commisurato alle finalità specifiche dei singoli casi d'uso dell'Intelligenza Artificiale autorizzati dall'Istituzione scolastica.

In coerenza con le Linee guida del Ministero dell'Istruzione e del Merito per l'introduzione dell'IA nelle istituzioni scolastiche, l'Istituto adotta, ove tecnicamente possibile, configurazioni che **non prevedono la conservazione delle cronologie delle interazioni (chat) con i sistemi di IA**, evitando il mantenimento di log o storici non strettamente necessari alle finalità didattiche, organizzative o amministrative dichiarate.

Qualora, per specifiche esigenze tecniche o di monitoraggio, siano temporaneamente disponibili dati relativi alle interazioni, essi sono conservati per un periodo limitato e proporzionato, esclusivamente per il tempo necessario al perseguimento delle finalità legittime del trattamento, e successivamente cancellati o anonimizzati. In ogni caso, non è prevista la conservazione sistematica e prolungata delle conversazioni con l'IA né il loro riutilizzo per finalità ulteriori rispetto a quelle istituzionali, nel rispetto dei principi di minimizzazione, responsabilizzazione e tutela dei diritti degli interessati.

Principi Fondamentali - Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati del trattamento dei dati personali connesso all'utilizzo di strumenti di Intelligenza Artificiale attraverso informative chiare, accessibili e facilmente comprensibili, predisposte dall'Istituzione scolastica in conformità all'Articolo 13 del Regolamento UE 2016/679 e rese disponibili mediante sezione privacy del sito WEB di istituto, il registro elettronico e le comunicazioni scuola–famiglia, nonché attraverso momenti informativi dedicati rivolti a studenti, famiglie e personale.

In coerenza con il principio di trasparenza e con il principio di spiegabilità richiamato dalle Linee guida del Ministero dell'Istruzione e del Merito, l'informazione fornita non si limita agli aspetti formali del trattamento, ma include una descrizione comprensibile delle finalità dell'uso dell'Intelligenza Artificiale, delle modalità di funzionamento degli strumenti impiegati, del ruolo di supporto svolto dall'IA e della presenza costante del controllo umano. In particolare, agli studenti è garantita un'informazione adeguata all'età e al livello di maturità, volta a favorire la comprensione dei limiti dei sistemi di IA, dei possibili rischi e del carattere non vincolante degli output generati.

Il personale scolastico è informato e formato sulle modalità corrette di utilizzo degli strumenti e sugli obblighi in materia di protezione dei dati, mentre alle famiglie è assicurata una comunicazione trasparente sulle finalità educative e organizzative del trattamento, sui diritti degli interessati e sulle modalità per esercitarli. Tale approccio informativo contribuisce a rendere l'uso dell'Intelligenza Artificiale intelligibile, controllabile e responsabile, rafforzando la fiducia degli interessati e la tutela dei loro diritti.

Ove applicabile: come si ottiene il consenso degli interessati?

La base giuridica per il trattamento non è costituita dal consenso dell'interessato.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati possono sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati hanno la possibilità di contattare l'amministrazione utilizzando il metodo di comunicazione di loro scelta per esercitare tali diritti.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati hanno la possibilità di contattare l'amministrazione utilizzando il metodo di comunicazione di loro scelta per esercitare tali diritti.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

La selezione dei servizi digitali e degli strumenti di Intelligenza Artificiale utilizzati dall'Istituzione scolastica avviene previa verifica dell'esistenza di un rapporto contrattuale con il fornitore del servizio e della formale designazione dello stesso quale Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679, anche mediante accettazione in formato elettronico. Tali documenti contrattuali disciplinano in modo puntuale le rispettive responsabilità delle parti e definiscono gli obblighi in materia di protezione dei dati personali, sicurezza e limitazione delle finalità del trattamento.

Con riferimento agli strumenti di Intelligenza Artificiale integrati nella piattaforma Google Workspace for Education, l'Istituzione scolastica fa riferimento al contratto di servizio e al relativo Data Processing Addendum predisposti da Google, nei quali sono chiaramente individuati i ruoli, le misure di sicurezza adottate e gli impegni del fornitore al rispetto dei principi del Regolamento (UE) 2016/679, garantendo così un quadro contrattuale coerente con le esigenze di tutela dei dati personali in ambito scolastico.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I servizi offerti nell'ambito di Google Workspace for Education, comprese le funzionalità di Intelligenza Artificiale integrate nella piattaforma, si basano su un'infrastruttura cloud che può comportare il trattamento dei dati personali anche su server localizzati al di fuori dell'Unione europea, inclusi gli Stati Uniti d'America. In relazione a tali trasferimenti, nel luglio 2023 la Commissione europea ha adottato la decisione di adeguatezza denominata *EU–US Data Privacy Framework*, riconoscendo che le organizzazioni statunitensi aderenti a tale quadro garantiscono un livello di protezione dei dati personali sostanzialmente equivalente a quello assicurato nell'Unione europea. Tale decisione ha superato le criticità evidenziate dalla sentenza della Corte di Giustizia dell'Unione europea C-311/18 (*Schrems II*), che aveva dichiarato invalida la precedente decisione di adeguatezza *Privacy Shield*.

Alla luce di ciò, i trasferimenti di dati personali connessi all'utilizzo di Google Workspace for Education e delle relative funzionalità di IA avvengono in un quadro giuridico riconosciuto come adeguato ai sensi dell'art. 45 del Regolamento (UE) 2016/679.

Misure di sicurezza esistenti o pianificate

Controllo e gestione degli account di accesso

L'accesso alle funzionalità delle piattaforme digitali utilizzate dall'Istituzione scolastica, comprese le funzionalità di Intelligenza Artificiale integrate in Google Workspace for Education, è regolato mediante l'attivazione di account nominativi dotati di credenziali di autenticazione e di permessi specifici, gestiti centralmente dall'amministratore di sistema designato dal Dirigente scolastico ai sensi dell'art. 2-quaterdecies del Codice in materia di protezione dei dati personali.

L'amministratore della piattaforma definisce e assegna profili di autorizzazione differenziati in base ai ruoli e alle funzioni svolte, assicurando la separazione delle attività e delle aree di responsabilità e limitando l'accesso degli utenti ai soli dati e alle sole funzionalità strettamente necessarie allo svolgimento dei compiti istituzionali, incluse quelle relative all'uso dell'Intelligenza Artificiale. Le autorizzazioni di accesso sono tempestivamente revocate qualora un utente cessi di essere legittimato all'utilizzo delle risorse digitali o dei servizi IT dell'Istituto.

È inoltre prevista una revisione periodica, almeno annuale, delle abilitazioni e degli account attivi, finalizzata a individuare ed eliminare eventuali account non più utilizzati e a riallineare i privilegi concessi alle effettive mansioni e responsabilità degli utenti, nel rispetto dei principi di sicurezza, minimizzazione e responsabilizzazione.

Minimizzazione dei dati

Il trattamento dei dati personali connesso all'utilizzo di strumenti di Intelligenza Artificiale è effettuato nel rispetto del principio di minimizzazione di cui all'art. 5, par. 1, lett. c) del GDPR, assicurando che siano trattati esclusivamente dati adeguati, pertinenti e limitati a quanto strettamente necessario per il perseguimento delle finalità didattiche, formative, organizzative e amministrative dichiarate dall'Istituzione scolastica. Nell'ambito dei casi d'uso autorizzati, l'Istituto adotta configurazioni tecniche e misure organizzative volte a ridurre la quantità e la tipologia di dati personali trattati, escludendo il trattamento di categorie particolari di dati ai sensi dell'art. 9 del GDPR e prevedendo, ove possibile, l'utilizzo di dati anonimizzati o pseudonimizzati. In coerenza con le Linee guida del Ministero dell'Istruzione e del Merito, sono escluse funzionalità di profilazione degli utenti e sono disattivate o limitate le cronologie di utilizzo e delle interazioni con i sistemi di IA, salvo i casi in cui la loro conservazione risulti strettamente indispensabile per le finalità dichiarate o per esigenze di sicurezza e monitoraggio, nel rispetto dei principi di proporzionalità, responsabilizzazione e tutela dei diritti degli interessati.

Lotta contro il malware

L'Istituzione scolastica adotta misure tecniche e organizzative volte a prevenire e contrastare le minacce informatiche, inclusi i rischi derivanti da malware, nell'ambito dell'utilizzo delle piattaforme digitali e degli strumenti di Intelligenza Artificiale impiegati per le attività didattiche, organizzative e amministrative. La sicurezza dei sistemi è garantita mediante un insieme coordinato di protezioni hardware e software, tra cui l'impiego di firewall, sistemi di rilevamento e prevenzione delle intrusioni e soluzioni antivirus costantemente aggiornate, nonché attraverso le misure di sicurezza

integrate nell'infrastruttura cloud di Google Workspace for Education. A tali misure si affiancano iniziative di informazione e formazione rivolte a studenti, docenti e personale scolastico, finalizzate a promuovere un uso consapevole e sicuro delle risorse digitali e a ridurre i rischi connessi a comportamenti non corretti. In tale contesto, l'utilizzo dei software e delle funzionalità, comprese quelle di Intelligenza Artificiale, messi a disposizione all'interno della suite Google Workspace for Education e configurati dall'amministratore di sistema secondo le politiche di sicurezza dell'Istituto, non comporta un incremento significativo del rischio di infezioni da malware rispetto all'uso ordinario delle piattaforme digitali scolastiche.

Manutenzione dei sistemi hardware in uso a scuola

L'Istituzione scolastica assicura lo svolgimento regolare di attività di manutenzione sui sistemi hardware in uso presso le sedi scolastiche, al fine di garantirne il corretto funzionamento, la sicurezza e l'affidabilità nell'ambito delle attività didattiche, organizzative e amministrative, incluse quelle che prevedono l'utilizzo di strumenti digitali e di Intelligenza Artificiale. Tali attività comprendono interventi di aggiornamento, controllo e verifica delle dotazioni informatiche, nonché la gestione di eventuali guasti o malfunzionamenti, secondo le procedure interne dell'Istituto.

Per quanto riguarda i servizi software e le funzionalità di Intelligenza Artificiale erogate in modalità cloud tramite Google Workspace for Education, il fornitore del servizio, in qualità di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679, garantisce la disponibilità, la manutenzione e l'aggiornamento dell'infrastruttura applicativa e dei sistemi sottostanti, in conformità agli accordi contrattuali e alle misure di sicurezza previste.

Backup dei dati presenti nella piattaforma

La piattaforma Google Workspace for Education, utilizzata dall'Istituzione scolastica per le attività didattiche, organizzative e amministrative, integra nativamente sistemi avanzati di replica e backup dei dati, finalizzati a garantire la disponibilità, l'integrità e la resilienza delle informazioni trattate, comprese quelle connesse all'utilizzo delle funzionalità di Intelligenza Artificiale. Tali sistemi consentono il ripristino dei dati in caso di incidenti tecnici, errori operativi o eventi imprevisti, in conformità alle misure di sicurezza previste dal fornitore del servizio in qualità di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679.

L'Istituzione scolastica si avvale di tali funzionalità nel rispetto dei principi di minimizzazione e limitazione della conservazione, assicurando che i backup siano utilizzati esclusivamente per finalità di continuità operativa e protezione dei dati, e non per trattamenti ulteriori o incompatibili con le finalità istituzionali dichiarate.

Eliminazione dei documenti nell'ottica di ridurre il ciclo di vita del trattamento dei dati

L'Istituzione scolastica adotta misure organizzative e tecniche volte a limitare il ciclo di vita del trattamento dei dati personali, prevedendo la cancellazione o l'anonimizzazione dei documenti e dei contenuti digitali non più necessari al perseguimento delle finalità didattiche, formative, organizzative e amministrative per le quali sono stati trattati. In particolare, al termine dell'anno scolastico, i dati personali contenuti nei materiali didattici, nei documenti di lavoro e nelle

interazioni con gli strumenti digitali e di Intelligenza Artificiale sono oggetto di revisione e, ove non sussistano ulteriori esigenze istituzionali o obblighi normativi di conservazione, sono eliminati o resi non riconducibili agli interessati. Restano esclusi da tale cancellazione i dati identificativi associati agli account istituzionali, che sono conservati per il tempo strettamente necessario alla gestione del rapporto scolastico e nel rispetto dei principi di limitazione della conservazione e responsabilizzazione di cui all'art. 5 del Regolamento (UE) 2016/679.

Tracciabilità delle operazioni effettuate online

La piattaforma Google Workspace for Education integra sistemi nativi di tracciabilità delle operazioni effettuate dagli utenti, finalizzati a garantire la sicurezza, l'integrità dei sistemi e la corretta gestione degli accessi e delle attività svolte, comprese quelle connesse all'utilizzo delle funzionalità di Intelligenza Artificiale. Tali sistemi di logging sono configurati e utilizzati nel rispetto dei principi di liceità, minimizzazione e proporzionalità, evitando forme di monitoraggio eccedenti o non giustificate dalle finalità istituzionali.

I log di tracciamento sono accessibili esclusivamente al personale autorizzato, in particolare all'amministratore di sistema designato dal Dirigente scolastico ai sensi dell'art. 2-quaterdecies del Codice in materia di protezione dei dati personali, e sono consultati solo in caso di necessità connesse a esigenze di sicurezza, gestione tecnica o verifica di eventuali anomalie. La conservazione dei log avviene per un periodo limitato e proporzionato alle finalità sopra indicate, in coerenza con il principio di limitazione della conservazione e con le politiche di sicurezza dell'Istituto.

Continuo monitoraggio e risoluzione delle vulnerabilità del sistema

L'Istituzione scolastica garantisce un monitoraggio continuo delle vulnerabilità dei sistemi digitali utilizzati, comprese le piattaforme cloud e le funzionalità di Intelligenza Artificiale integrate in Google Workspace for Education, al fine di prevenire e ridurre i rischi per la sicurezza dei dati personali trattati. Tale attività si realizza attraverso l'adozione di misure tecniche e organizzative adeguate, la verifica periodica delle configurazioni di sicurezza e l'applicazione tempestiva di aggiornamenti e patch correttive, in coordinamento con il fornitore del servizio, che opera in qualità di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679. Eventuali vulnerabilità o criticità rilevate sono gestite secondo procedure definite, volte a garantire la continuità operativa, la protezione dei dati e la riduzione dell'impatto sui diritti e sulle libertà degli interessati.

Contratto con il responsabile del trattamento

In accordo con quanto previsto dall'articolo 28 del GDPR, il Titolare del Trattamento sceglie fornitori di sistemi di IA che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del GDPR e a garantire la tutela dei diritti dell'interessato. Essi hanno la responsabilità di trattare i dati in modo sicuro e conforme alle disposizioni normative, sulla base di un accordo redatto di Responsabile del Trattamento ai sensi dall'articolo 28 del GDPR. Si ricorda inoltre che le Pubbliche amministrazioni possono avvalersi esclusivamente di fornitori qualificati per i servizi digitali della Pubblica Amministrazione (PA), che prima seguivano le regole AGID (Agenzia per l'Italia Digitale) e ora sono gestite e qualificate dall'ACN

(Agenzia per la Cybersicurezza Nazionale) per garantire sicurezza e affidabilità con processi che prevedono requisiti stringenti definiti da decreti e circolari. Nel caso in questione il Responsabile esterno è la Google LLC con sede in Mountain View in California (USA).

Politica di tutela della privacy: misure tecniche ed organizzative da adottare

Il Dirigente scolastico, in qualità di Titolare del trattamento, ha adottato un insieme strutturato di misure tecniche e organizzative finalizzate a garantire la protezione dei dati personali trattati nell'ambito dell'utilizzo delle piattaforme digitali e degli strumenti di Intelligenza Artificiale impiegati dall'Istituzione scolastica. Tali misure sono definite nel regolamento interno di utilizzo dei sistemi di IA e nelle ulteriori procedure e policy adottate dall'Istituto, in coerenza con il Piano di Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA). In particolare, l'Istituto configura la piattaforma in modo da escludere funzionalità di profilazione degli utenti e da disattivare o limitare la conservazione delle cronologie di utilizzo e delle interazioni con i sistemi di IA, salvo i casi in cui tali funzionalità risultino strettamente indispensabili per il perseguimento delle finalità didattiche, organizzative o amministrative dichiarate, ovvero per esigenze di sicurezza e gestione tecnica.

Il Dirigente scolastico assicura inoltre l'adeguata informazione e formazione del personale docente e del personale scolastico, nonché la sensibilizzazione delle famiglie e degli studenti in merito al corretto e responsabile utilizzo degli strumenti digitali, inclusi quelli basati sull'Intelligenza Artificiale.

È stata (o sarà) infine formalmente designata la figura dell'Amministratore di sistema, ai sensi dell'art. 2-quaterdecies del D.lgs. 196/2003, con specifici compiti di gestione tecnica, configurazione e controllo della piattaforma, nel rispetto dei principi di sicurezza, minimizzazione e responsabilizzazione previsti dal Regolamento (UE) 2016/679.

Formazione specifica del personale e degli interessati

La formazione e lo sviluppo professionale dei docenti, del personale amministrativo, del Dirigente scolastico e del DSGA rappresentano una leva strategica per il corretto utilizzo delle tecnologie che integrano sistemi di Intelligenza Artificiale, nel rispetto dei principi del Regolamento (UE) 2016/679. Il piano di formazione è descritto in modo organico nel Piano di Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), integrato nel PTOF.

Gestione online dei dispositivi mobili che hanno accesso alla piattaforma

L'approccio educativo adottato dall'Istituzione scolastica nell'utilizzo delle piattaforme digitali per l'istruzione, incluse le funzionalità di Intelligenza Artificiale integrate in Google Workspace for Education, prevede l'accesso ai servizi e ai processi di apprendimento mediante dispositivi informatici connessi alla rete, quali computer e tablet, sia di proprietà degli utenti sia concessi in comodato d'uso dalla scuola. In tale contesto, l'Istituto applica politiche di gestione e sicurezza dei dispositivi che accedono da remoto alla piattaforma, al fine di garantire un livello adeguato di protezione dei dati personali trattati, anche attraverso l'adozione di configurazioni coerenti con le funzionalità di gestione dei dispositivi previste dall'ecosistema Google Workspace. Per i dispositivi forniti in comodato d'uso dall'Istituto, sono adottate specifiche misure di sicurezza, tra cui

l'installazione e l'aggiornamento di software antivirus e antimalware, l'utilizzo di sistemi di protezione firewall e lo svolgimento di attività periodiche di manutenzione da parte di personale autorizzato o specializzato, al fine di ridurre i rischi di accessi non autorizzati, infezioni da malware o compromissione dei dati.

Sicurezza dei canali informatici

Di seguito alcune misure di sicurezza associate ai canali informatici di Google Workspace for Education che l'istituto ha preso in esame per la stesura della presente DPIA:

Crittografia: Google Workspace utilizza crittografia per proteggere i dati in transito. Questo significa che le informazioni vengono criptate durante la trasmissione per impedire a terzi non autorizzati di accedervi.

Autenticazione a Due Fattori (2FA): L'abilitazione dell'autenticazione a due fattori, sebbene renda più difficile l'accesso non autorizzato richiedendo un secondo passaggio di verifica oltre alle credenziali di accesso standard, non viene implementata per i motivi esposti nei paragrafi precedenti.

Protezione Anti-Phishing: Google Workspace include filtri anti-phishing per rilevare e bloccare tentativi di phishing e di attacchi di spear-phishing.

Firewall e Protezione Antivirus: L'uso di firewall e software antivirus aiuta a proteggere da malware e minacce online.

Gestione degli incidenti di sicurezza e delle violazioni dei dati personali

L'amministrazione ha emesso un regolamento interno per la gestione dei data breach, al cui interno sono specificate le modalità di gestione di tali fenomeni.

Rischi - Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

La concretizzazione del rischio di accesso illegittimo ai dati potrebbe comportare una compromissione della riservatezza delle informazioni personali degli interessati, inclusi studenti minorenni, con possibile esposizione di dati identificativi, contenuti didattici, comunicazioni e informazioni generate o trattate mediante strumenti di Intelligenza Artificiale. Tale evenienza potrebbe determinare utilizzi impropri delle informazioni, fenomeni di profilazione indebita o valutazioni distorte, nonché arrecare danni reputazionali e psicologici agli interessati, incidendo negativamente sul benessere individuale e sul rapporto di fiducia tra famiglie, studenti e istituzione scolastica.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le principali minacce che potrebbero consentire la concretizzazione del rischio di accesso illegittimo ai dati includono attacchi di phishing e spear phishing finalizzati all'acquisizione fraudolenta delle credenziali di accesso degli utenti, la compromissione delle password tramite attacchi di forza bruta o dizionario, nonché la presenza di vulnerabilità nei software e nei servizi utilizzati all'interno dell'ecosistema Google Workspace for Education e degli strumenti di Intelligenza Artificiale integrati. Ulteriori minacce sono rappresentate dall'installazione di malware sui dispositivi utilizzati da studenti e docenti, dall'accesso non autorizzato a dispositivi smarriti o rubati, da errori umani nella configurazione delle autorizzazioni e dei profili di accesso, nonché dall'eventuale mancata disattivazione tempestiva degli account di utenti non più autorizzati. In ambito scolastico, tali minacce risultano amplificate dall'elevato numero di utenti, dall'utilizzo di dispositivi personali e dalla diversa consapevolezza digitale degli interessati.

Quali sono le fonti di rischio?

Le principali fonti di rischio sono riconducibili a soggetti interni ed esterni all'istituzione scolastica e a condizioni organizzative e tecnologiche del contesto di trattamento. In particolare, costituiscono fonti di rischio gli utenti della piattaforma (studenti, docenti e personale scolastico), caratterizzati da livelli eterogenei di competenza digitale, l'utilizzo diffuso di dispositivi personali per l'accesso ai servizi cloud e agli strumenti di Intelligenza Artificiale, nonché eventuali carenze nella formazione e nella consapevolezza in materia di sicurezza e protezione dei dati personali. Ulteriori fonti di rischio sono rappresentate dai fornitori esterni di servizi tecnologici, dalla complessità dell'ecosistema digitale adottato e dalla possibilità di configurazioni non corrette dei sistemi e dei profili di accesso.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

L'istituto scolastico adotta un insieme integrato di misure tecniche, organizzative e formative, coerenti con il PUIA e con i principi del GDPR, finalizzate a ridurre la probabilità e l'impatto del rischio di accesso illegittimo ai dati nell'utilizzo degli strumenti di Intelligenza Artificiale. In particolare:

Controllo e gestione degli account di accesso, mediante l'uso di credenziali istituzionali, profili differenziati per ruolo e principi di least privilege, al fine di limitare l'uso degli strumenti di IA ai soli soggetti autorizzati e alle finalità previste.

Principio di minimizzazione dei dati, applicato sia nella fase di inserimento delle informazioni nei sistemi di IA sia nella condivisione dei contenuti, evitando l'uso di dati personali non necessari o particolari che potrebbero amplificare distorsioni o trattamenti iniqui.

Contrattualizzazione del Responsabile del trattamento ai sensi dell'art. 28 GDPR, con specifiche clausole in materia di sicurezza, limitazione delle finalità e protezione dei dati, inclusa la disciplina dell'uso delle funzionalità di IA integrate nella piattaforma.

Adozione di politiche interne di tutela della privacy, comprensive di misure tecniche e organizzative che regolano l'utilizzo consapevole degli strumenti digitali e di IA, in coerenza con il PUIA e con le Linee guida ministeriali.

Tracciabilità delle operazioni effettuate online, mediante sistemi di logging e controllo degli accessi, al fine di consentire verifiche a posteriori e individuare eventuali utilizzi impropri o non conformi degli strumenti di IA.

Formazione specifica e continua del personale scolastico e degli utenti, finalizzata a sviluppare competenze critiche sull'uso dell'IA, sulla natura probabilistica dei risultati e sui rischi di bias, promuovendo la supervisione umana e l'uso consapevole dei contenuti generati.

Gestione sicura delle infrastrutture tecnologiche, comprendente la manutenzione dei sistemi hardware, la protezione da malware, la sicurezza dei canali informatici e la gestione dei dispositivi mobili che accedono alla piattaforma, al fine di prevenire alterazioni o compromissioni dei dati.

Monitoraggio continuo delle vulnerabilità dei sistemi e gestione degli incidenti di sicurezza, comprese le violazioni dei dati personali (data breach), con procedure di risposta e mitigazione tempestive, in coordinamento con il Titolare del trattamento e il RPD.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Considerati gli impatti potenziali sugli interessati, in particolare sugli studenti minorenni, il rischio di accesso illegittimo ai dati presenta, in astratto, una possibile incidenza sulla riservatezza delle informazioni personali. Tuttavia, il contesto di utilizzo degli strumenti di Intelligenza Artificiale è configurato in modo da escludere sistematicamente il trattamento di dati personali, salvo casi meramente incidentali e non intenzionali, privilegiando l'impiego di contenuti generici e didattici. Inoltre, ove tecnicamente possibile, è prevista la disattivazione della cronologia dei prompt e delle interazioni, riducendo ulteriormente la persistenza e l'esposizione delle informazioni trattate. Tali scelte, unitamente all'adozione di un insieme strutturato e coerente di misure tecniche, organizzative e formative integrate nel Piano per l'Utilizzo dell'Intelligenza Artificiale (PUIA) e conformi ai principi del GDPR — tra cui il controllo degli accessi, la minimizzazione dei dati, la tracciabilità delle operazioni, le politiche di conservazione limitata, la formazione continua degli utenti e le procedure di gestione degli incidenti — consentono di ridurre in modo significativo l'estensione, la durata e la reversibilità degli effetti di un'eventuale violazione. Alla luce di tali elementi, la gravità residua del rischio è pertanto stimata come trascurabile, risultando adeguatamente mitigata e proporzionata al contesto di trattamento.

In sintesi: trascurabile.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

La probabilità di concretizzazione del rischio di accesso illegittimo ai dati è valutata tenendo conto delle minacce individuate, delle fonti di rischio e delle misure tecniche, organizzative e formative adottate dall'istituto. Sebbene il contesto scolastico e l'utilizzo di piattaforme cloud possano esporre a minacce comuni quali phishing, malware, errori umani o compromissione delle credenziali, tali eventi risultano significativamente mitigati dalla gestione centralizzata degli account, dall'adozione di profili di accesso differenziati, dalla tracciabilità delle operazioni, dalla protezione delle infrastrutture e dal monitoraggio continuo delle vulnerabilità. Inoltre, l'utilizzo degli strumenti di Intelligenza Artificiale avviene secondo criteri di minimizzazione, privilegiando l'assenza di dati personali nei prompt e, ove possibile, la disattivazione della cronologia delle interazioni, riducendo ulteriormente le superfici di esposizione. Alla luce di tali elementi e della formazione continua degli utenti, la probabilità residua del rischio è pertanto stimata come limitata, risultando coerente con il livello di controllo esercitato e con le misure di prevenzione adottate.

In sintesi: limitata.

Rischi - Modifiche indesiderate e/o perdita dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

La concretizzazione del rischio di modifiche indesiderate e/o perdita dei dati potrebbe incidere negativamente sulla correttezza, completezza e disponibilità delle informazioni relative agli interessati, determinando possibili disagi nello svolgimento delle attività didattiche e amministrative. In particolare, la perdita o l'alterazione di materiali didattici, elaborati degli studenti o contenuti generati nell'ambito dell'utilizzo di strumenti di Intelligenza Artificiale potrebbe compromettere la continuità dei percorsi formativi, generare formulazioni non corrette o non verificabili e incidere sul diritto degli interessati a un trattamento accurato e affidabile dei propri dati. Tali eventi potrebbero inoltre arrecare un pregiudizio organizzativo ed emotivo agli interessati, soprattutto nel caso di studenti minorenni, incidendo sul rapporto di fiducia nei confronti dell'istituzione scolastica.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Le principali minacce che potrebbero condurre a modifiche indesiderate o alla perdita dei dati includono accessi non autorizzati ai sistemi, errori umani nella gestione dei contenuti o delle autorizzazioni, malfunzionamenti o vulnerabilità delle piattaforme cloud e degli strumenti di Intelligenza Artificiale utilizzati, nonché eventi tecnici quali guasti hardware, interruzioni di servizio o problemi di sincronizzazione dei dati. Ulteriori minacce sono rappresentate da attacchi informatici, quali malware o ransomware, che possono alterare o rendere indisponibili le informazioni, nonché da configurazioni errate dei sistemi di backup o delle politiche di conservazione. In ambito scolastico, tali minacce risultano amplificate dalla molteplicità degli utenti coinvolti, dall'uso di dispositivi personali e dalla complessità dell'ecosistema digitale adottato.

Quali sono le fonti di rischio?

Le principali fonti di rischio sono riconducibili a soggetti interni ed esterni all'istituzione scolastica e a condizioni organizzative e tecnologiche del contesto di trattamento. In particolare, costituiscono fonti di rischio gli utenti della piattaforma (studenti, docenti e personale scolastico), caratterizzati da livelli eterogenei di competenza digitale, l'utilizzo diffuso di dispositivi personali per l'accesso ai servizi cloud e agli strumenti di Intelligenza Artificiale, nonché eventuali carenze nella formazione e nella consapevolezza in materia di sicurezza e protezione dei dati personali. Ulteriori fonti di rischio sono rappresentate dai fornitori esterni di servizi tecnologici, dalla complessità dell'ecosistema digitale adottato e dalla possibilità di configurazioni non corrette dei sistemi e dei profili di accesso.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

L'istituto scolastico adotta un insieme integrato di misure tecniche, organizzative e formative, coerenti con il PUIA e con i principi del GDPR, finalizzate a ridurre la probabilità e l'impatto del rischio di modifiche indesiderate e/o perdita dei dati durante l'utilizzo degli strumenti di Intelligenza Artificiale. In particolare:

Controllo e gestione degli account di accesso, mediante l'uso di credenziali istituzionali, profili differenziati per ruolo e principi di least privilege, al fine di limitare l'uso degli strumenti di IA ai soli soggetti autorizzati e alle finalità previste.

Principio di minimizzazione dei dati, applicato sia nella fase di inserimento delle informazioni nei sistemi di IA sia nella condivisione dei contenuti, evitando l'uso di dati personali non necessari o particolari che potrebbero amplificare distorsioni o trattamenti iniqui.

Contrattualizzazione del Responsabile del trattamento ai sensi dell'art. 28 GDPR, con specifiche clausole in materia di sicurezza, limitazione delle finalità e protezione dei dati, inclusa la disciplina dell'uso delle funzionalità di IA integrate nella piattaforma.

Adozione di politiche interne di tutela della privacy, comprensive di misure tecniche e organizzative che regolano l'utilizzo consapevole degli strumenti digitali e di IA, in coerenza con il PUIA e con le Linee guida ministeriali.

Tracciabilità delle operazioni effettuate online, mediante sistemi di logging e controllo degli accessi, al fine di consentire verifiche a posteriori e individuare eventuali utilizzi impropri o non conformi degli strumenti di IA.

Formazione specifica e continua del personale scolastico e degli utenti, finalizzata a sviluppare competenze critiche sull'uso dell'IA, sulla natura probabilistica dei risultati e sui rischi di bias, promuovendo la supervisione umana e l'uso consapevole dei contenuti generati.

Gestione sicura delle infrastrutture tecnologiche, comprendente la manutenzione dei sistemi hardware, la protezione da malware, la sicurezza dei canali informatici e la gestione dei dispositivi mobili che accedono alla piattaforma, al fine di prevenire alterazioni o compromissioni dei dati.

Backup periodico dei dati e politiche di conservazione limitata, inclusa l'eliminazione dei documenti non più necessari, per ridurre il ciclo di vita del trattamento e prevenire l'uso reiterato di informazioni obsolete o non pertinenti.

Monitoraggio continuo delle vulnerabilità dei sistemi e gestione degli incidenti di sicurezza, comprese le violazioni dei dati personali (data breach), con procedure di risposta e mitigazione tempestive, in coordinamento con il Titolare del trattamento e il RPD.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Considerati gli impatti potenziali sugli interessati, in particolare sugli studenti minorenni, il rischio di modifica e/o perdita dei dati presenta, in astratto, una possibile incidenza sull'integrità e disponibilità delle informazioni personali. Tuttavia, il contesto di utilizzo degli strumenti di Intelligenza Artificiale è configurato in modo da escludere sistematicamente il trattamento di dati personali, salvo casi meramente incidentali e non intenzionali, privilegiando l'impiego di contenuti generici e didattici. Inoltre, ove tecnicamente possibile, sono implementate misure di backup,

versioning e disattivazione della cronologia dei prompt e delle interazioni, riducendo ulteriormente la probabilità di perdita o alterazione dei dati trattati. Tali scelte, unitamente all'adozione di un insieme strutturato e coerente di misure tecniche, organizzative e formative integrate nel Piano per l'Utilizzo dell'Intelligenza Artificiale (PUIA) e conformi ai principi del GDPR — tra cui il controllo degli accessi, la minimizzazione dei dati, la tracciabilità delle operazioni, le politiche di conservazione limitata, la formazione continua degli utenti e le procedure di gestione degli incidenti — consentono di ridurre in modo significativo l'estensione, la durata e la reversibilità degli effetti di un'eventuale modifica o perdita. Alla luce di tali elementi, la gravità residua del rischio è pertanto stimata come trascurabile, risultando adeguatamente mitigata e proporzionata al contesto di trattamento.

In sintesi: trascurabile.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

La probabilità di concretizzazione del rischio di modifica e/o perdita dei dati è valutata tenendo conto delle minacce individuate, delle fonti di rischio e delle misure tecniche, organizzative e formative adottate dall'istituto. Sebbene il contesto scolastico e l'utilizzo di piattaforme cloud possano esporre a minacce comuni quali errori umani, malfunzionamenti tecnici, malware o compromissione delle credenziali, tali eventi risultano significativamente mitigati dalla gestione centralizzata degli account, dall'adozione di profili di accesso differenziati, dalla tracciabilità delle operazioni, dalla protezione delle infrastrutture e dal monitoraggio continuo delle vulnerabilità. Inoltre, l'utilizzo degli strumenti di Intelligenza Artificiale avviene secondo criteri di minimizzazione, privilegiando l'assenza di dati personali nei prompt e, ove possibile, implementando backup, versioning e disattivazione della cronologia delle interazioni, riducendo ulteriormente la probabilità di perdita o alterazione dei dati. Alla luce di tali elementi e della formazione continua degli utenti, la probabilità residua del rischio è pertanto stimata come limitata, risultando coerente con il livello di controllo esercitato e con le misure di prevenzione adottate.

In sintesi: limitata.

Rischi – BIAS (rischio specifico nelle IA)

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

La presenza di bias nei sistemi di Intelligenza Artificiale utilizzati in ambito scolastico può determinare impatti negativi sui diritti e sulle libertà degli interessati, in particolare degli studenti, spesso minori, quali il rischio di trattamenti iniqui o discriminatori, anche indiretti, basati su caratteristiche culturali, linguistiche, sociali o su specifici bisogni educativi. Tali bias possono influenzare la qualità e l'imparzialità dei contenuti, dei suggerimenti e dei feedback prodotti dall'IA, incidendo sul processo di apprendimento, sulla percezione delle capacità individuali e sul livello di inclusione educativa, nonché rafforzare stereotipi o modelli culturali distorti. Inoltre, la difficoltà di individuare e spiegare l'origine di tali distorsioni può compromettere i principi di correttezza e trasparenza del trattamento, limitando la capacità degli interessati di comprendere e contestare gli esiti dell'uso dell'IA e incidendo sul rapporto di fiducia tra scuola, studenti e famiglie.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Le principali minacce che possono consentire la concretizzazione del rischio di bias nei sistemi di Intelligenza Artificiale utilizzati in ambito scolastico includono l'impiego di modelli addestrati su dati non rappresentativi o sbilanciati dal punto di vista culturale, linguistico o sociale, la limitata trasparenza e spiegabilità dei meccanismi di funzionamento dell'IA, l'uso improprio o non sufficientemente guidato degli strumenti da parte degli utenti, nonché la tendenza all'accettazione acritica dei risultati generati (automation bias), che riduce la supervisione umana. A tali fattori si aggiungono l'assenza o l'inadeguatezza di procedure strutturate di verifica e validazione dei contenuti prodotti, la possibile riproduzione di stereotipi presenti nei dati di origine e una non completa attuazione delle misure organizzative e formative previste dal PUIA, elementi che, nel loro insieme, possono favorire la diffusione di risultati distorti e incidere negativamente sui diritti e sulle libertà degli interessati, in particolare degli studenti.

Quali sono le fonti di rischio?

Nel contesto della DPIA relativa all'uso dell'Intelligenza Artificiale in ambito scolastico, le principali fonti di rischio sono riconducibili sia a componenti tecnologiche sia a fattori organizzativi e umani. In particolare, il rischio può originare dai fornitori e dai modelli di IA utilizzati, in relazione alle modalità di progettazione, addestramento e aggiornamento dei sistemi e alla limitata trasparenza dei loro funzionamenti interni; dalle piattaforme digitali e infrastrutture cloud che ospitano gli strumenti di IA, per quanto riguarda configurazioni, impostazioni predefinite e integrazioni con altri servizi; dalle modalità di utilizzo da parte degli utenti, inclusi docenti, studenti e personale scolastico, qualora l'impiego dell'IA avvenga senza adeguate istruzioni, formazione o consapevolezza critica; nonché dai processi organizzativi dell'istituto, qualora le misure di governance, supervisione umana, controllo e monitoraggio previste dal PUIA non siano pienamente attuate o aggiornate. Tali fonti, considerate nel loro insieme, possono contribuire alla

materializzazione dei rischi per i diritti e le libertà degli interessati, rendendo necessario un approccio integrato di prevenzione e mitigazione.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

L'istituto scolastico adotta un insieme integrato di misure tecniche, organizzative e formative, coerenti con il PUIA e con i principi del GDPR, finalizzate a ridurre la probabilità e l'impatto del rischio di bias nell'utilizzo degli strumenti di Intelligenza Artificiale. In particolare:

Controllo e gestione degli account di accesso, mediante l'uso di credenziali istituzionali, profili differenziati per ruolo e principi di least privilege, al fine di limitare l'uso degli strumenti di IA ai soli soggetti autorizzati e alle finalità previste.

Principio di minimizzazione dei dati, applicato sia nella fase di inserimento delle informazioni nei sistemi di IA sia nella condivisione dei contenuti, evitando l'uso di dati personali non necessari o particolari che potrebbero amplificare distorsioni o trattamenti iniqui.

Contrattualizzazione del Responsabile del trattamento ai sensi dell'art. 28 GDPR, con specifiche clausole in materia di sicurezza, limitazione delle finalità e protezione dei dati, inclusa la disciplina dell'uso delle funzionalità di IA integrate nella piattaforma.

Adozione di politiche interne di tutela della privacy, comprensive di misure tecniche e organizzative che regolano l'utilizzo consapevole degli strumenti digitali e di IA, in coerenza con il PUIA e con le Linee guida ministeriali.

Tracciabilità delle operazioni effettuate online, mediante sistemi di logging e controllo degli accessi, al fine di consentire verifiche a posteriori e individuare eventuali utilizzi impropri o non conformi degli strumenti di IA.

Formazione specifica e continua del personale scolastico e degli utenti, finalizzata a sviluppare competenze critiche sull'uso dell'IA, sulla natura probabilistica dei risultati e sui rischi di bias, promuovendo la supervisione umana e l'uso consapevole dei contenuti generati.

Procedure di verifica e validazione dei risultati prodotti dall'IA, che prevedono il controllo umano dei contenuti, dei suggerimenti e dei feedback, evitando l'accettazione automatica o acritica degli output e riducendo il rischio di automation bias.

Gestione sicura delle infrastrutture tecnologiche, comprendente la manutenzione dei sistemi hardware, la protezione da malware, la sicurezza dei canali informatici e la gestione dei dispositivi mobili che accedono alla piattaforma, al fine di prevenire alterazioni o compromissioni dei dati.

Backup periodico dei dati e politiche di conservazione limitata, inclusa l'eliminazione dei documenti non più necessari, per ridurre il ciclo di vita del trattamento e prevenire l'uso reiterato di informazioni obsolete o non pertinenti.

Monitoraggio continuo delle vulnerabilità dei sistemi e gestione degli incidenti di sicurezza, comprese le violazioni dei dati personali (data breach), con procedure di risposta e mitigazione tempestive, in coordinamento con il Titolare del trattamento e il RPD.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Tenendo conto dell'impatto potenziale sugli interessati, della capacità delle misure adottate di intercettare e correggere eventuali distorsioni, del fatto che l'IA è utilizzata come strumento di supporto e non come decisore e della supervisione dei docenti nel caso di utilizzo nella didattica, la gravità residua del rischio di bias può essere stimata come limitato, con un livello di accettabilità ritenuto proporzionato rispetto alle finalità educative perseguite e al contesto di utilizzo.

In sintesi: limitato.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

In considerazione delle caratteristiche intrinseche dei sistemi di Intelligenza Artificiale, delle minacce individuate e delle fonti di rischio connesse all'uso di modelli algoritmici, la probabilità di concretizzazione del rischio di bias, in assenza di misure, è strutturale e pertanto valutata come media. Tuttavia, alla luce delle misure tecniche, organizzative e formative pianificate e adottate dall'istituto, nonché della governance definita dal PUIA, che prevede supervisione umana, limitazione dei casi d'uso, formazione sull'uso critico dell'IA e procedure di verifica e tracciabilità, la probabilità residua del rischio è stimata come limitata e ritenuta accettabile e proporzionata rispetto alle finalità perseguite.

In sintesi: limitata.

Panoramica dei principi, misure e rischi analizzati

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Diritto di accesso e diritto alla portabilità dei dati
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

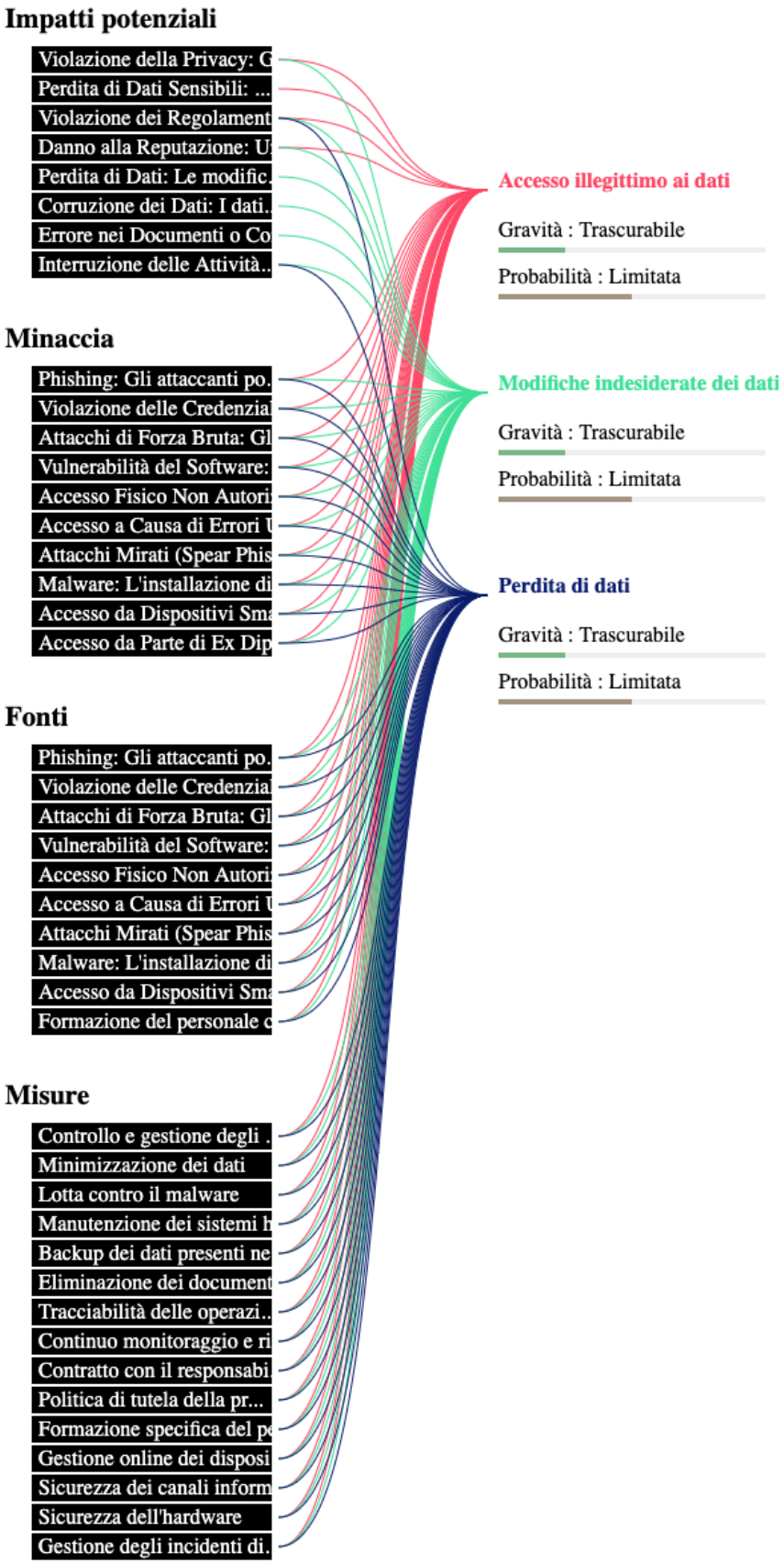
Misure esistenti o pianificate

- Controllo e gestione degli account di accesso
- Minimizzazione dei dati
- Lotta contro il malware
- Manutenzione dei sistemi hardware in uso a scuola
- Backup dei dati presenti nella piattaforma
- Eliminazione dei documenti nell'ottica di ridurre il ciclo di vita del trattamento dei dati
- Tracciabilità delle operazioni effettuate online
- Continuo monitoraggio e risoluzione delle vulnerabilità del sistema
- Contratto con il responsabile del trattamento
- Politica di tutela della privacy: misure tecniche ed organizzative da adottare
- Formazione specifica del personale e degli interessati
- Gestione online dei dispositivi mobili che hanno accesso alla piattaforma
- Sicurezza dei canali informatici
- Gestione degli incidenti di sicurezza e dele violazioni dei dati personali

Rischi

- Accesso illegittimo ai dati
- Modifiche indesider./perdita dati
- Bias

Panoramica dei rischi analizzati

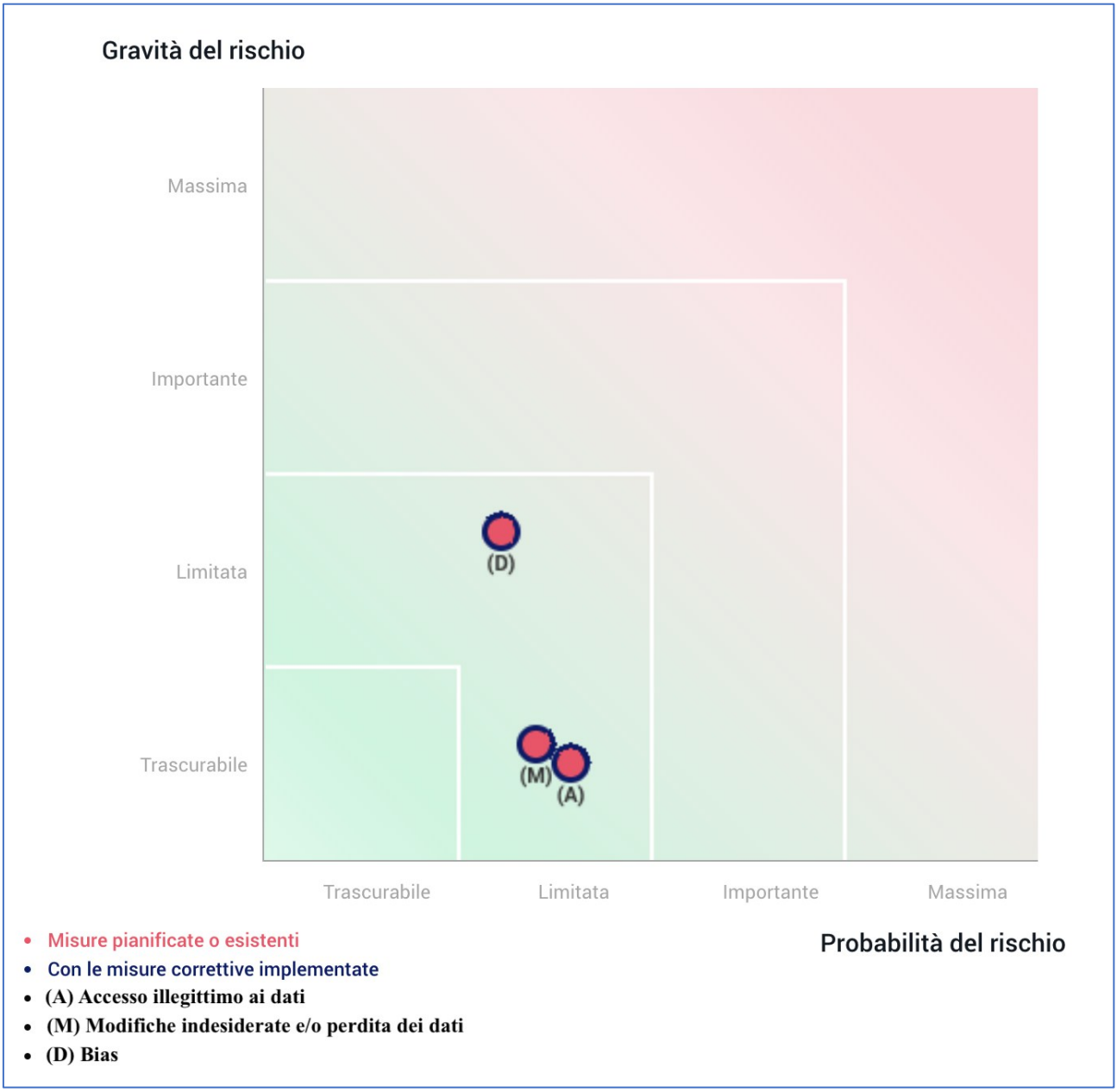


Panoramica dei piani di azione

Titolo	Commento sul piano di azione	Soggetto responsabile
Misure esistenti o pianificate		
Controllo e gestione degli account di accesso	misura always on	Amministratore della piattaforma
Minimizzazione dei dati	misura always on	Docenti, personale ATA in segreteria, studenti
Lotta contro il malware	misura always on	Responsabile del Trattamento
Manutenzione dei sistemi hardware in uso a scuola	misura always on	Animatore Digitale, personale tecnico, ditte esterne incaricate
Backup dei dati presenti nella piattaforma	misura always on	Responsabile del Trattamento
Eliminazione cronologie nell'ottica di ridurre il ciclo di vita del trattamento dei dati	misura always on	Amministratore della piattaforma
Tracciabilità delle operazioni effettuate online	misura always on	Responsabile del Trattamento
Continuo monitoraggio e risoluzione delle vulnerabilità del sistema	misura always on	Responsabile del Trattamento
Contratto con il responsabile del trattamento	All'atto dell'attivazione della piattaforma	Dirigente Scolastico
Politica di tutela della privacy: misure tecniche ed organizzative da adottare	misura always on	Dirigente Scolastico
Formazione specifica del personale e degli interessati	annuale	Dirigente Scolastico
Gestione online dei dispositivi mobili che hanno accesso alla piattaforma	misura always on	Amministratore della piattaforma
Sicurezza dei canali informatici	misura always on	Responsabile del Trattamento
Sicurezza dell'hardware	misura always on	Animatore Digitale, personale tecnico, ditte esterne incaricate

Gestione degli incidenti di sicurezza e dele violazioni dei dati personali	misura always on	Dirigente Scolastico, Amministratore della Piattaforma
Gestione del rischio "Accesso illegittimo ai dati"		
Accesso illegittimo ai dati	misura always on	Dirigente Scolastico, Amministratore della Piattaforma
Gestione del rischio "Modifiche indesiderate e/o perdita dei dati"		
Modifiche indesiderate dei dati	misura always on	Dirigente Scolastico, Amministratore della Piattaforma
Gestione del rischio "Bias"		
Bias	misura always on	Dirigente Scolastico, Amministratore della Piattaforma

Mappa dei rischi



Data: si veda segnatura di protocollo

Approvata dal DPO (firma)

NetSense s.r.l.

netsense s.r.l.
Via Novaluce, 38
95030 Tremestieri Etneo (CT)
Part IVA 04253850871

Il Titolare del Trattamento

Il Dirigente Scolastico pro tempore

Dott. Danilo Guido

Firmato da:
GUIDO DANILO
Codice fiscale: GDUDNL62R24A887S
09/07/2026 10:27:34