

**ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE**

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8

**Piano Utilizzo Intelligenza Artificiale (P.U.I.A.)**

Il Piano d'Istituto per l'Intelligenza Artificiale **definisce la strategia con cui la scuola integra in modo graduale, consapevole e responsabile gli strumenti di IA nella didattica e nell'organizzazione**, in coerenza con quanto sarà riportato nel PTOF e con le Linee guida MIM 2025. Il documento intende valorizzare le opportunità offerte dalle nuove tecnologie per migliorare qualità ed equità dell'offerta formativa, semplificare i processi amministrativi e sviluppare competenze digitali e di cittadinanza, tutelando al contempo la centralità della persona, i diritti fondamentali e la protezione dei dati

0. Indice e sommario

0. Indice e sommario	1
1. Premessa e riferimenti normativi	3
1.1. Finalità del Piano d'Istituto per l'Intelligenza Artificiale.....	3
1.2. Riferimenti europei, nazionali e al Piano Scuola 4.0	3
1.3. Raccordo con PTOF, RAV, PDM e Atto di indirizzo del Dirigente scolastico.....	4
2. Visione pedagogica e principi etici per l'uso dell'IA	4
2.1. Centralità della persona, inclusione e riduzione dei divari	4
2.2. Uso critico, consapevole e responsabile dei sistemi di IA	5
2.3. Tutela dei dati personali, sicurezza, trasparenza e non discriminazione	5
2.4. Rischi, limiti e misure di mitigazione nelle attività didattiche e amministrative	5
3. Obiettivi e ambiti di applicazione dell'IA nella vita dell'istituto	6
3.1. Obiettivi formativi e didattici	6
3.2. Obiettivi organizzativi e amministrativi	6
3.3. Ambiti di applicazione nella didattica	7
3.4. Ambiti di applicazione nell'attività amministrativa e gestionale	7
4. Governance del Piano e ruoli	7
4.1. Ruolo del Dirigente scolastico	8
4.2. Gruppo di lavoro per l'IA e Team per l'innovazione digitale.....	8
4.3. Ruoli di DSGA, personale di segreteria e referenti per privacy e sicurezza	8
4.4. Coinvolgimento degli organi collegiali, dei docenti, degli studenti e delle famiglie	9
5. Formazione, sviluppo professionale e sostenibilità del PUIA.....	9
5.1. Analisi dei fabbisogni formativi del personale	9



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



5.2.	Piano di formazione interno	10
5.3.	Partecipazione a iniziative nazionali, reti e progetti	10
5.4.	Sostenibilità nel tempo e aggiornamento periodico del Piano	10
6.	Azioni operative e cronoprogramma di attuazione	11
6.1.	Azioni a breve termine	11
6.2.	Azioni a medio e a lungo termine.....	11
6.3.	Cronoprogramma indicativo per anno scolastico	12
7.	Monitoraggio, valutazione e revisione del Piano	12
7.1.	Strumenti e indicatori di monitoraggio	12
7.2.	Valutazione degli esiti su studenti, docenti e organizzazione	13
7.3.	Procedure di revisione annuale e aggiornamento del Piano	13
7.4.	Trasparenza e rendicontazione verso la comunità scolastica	13



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



1. Premessa e riferimenti normativi

L'introduzione dell'Intelligenza Artificiale (IA) nei processi didattici e organizzativi dell'istituto si colloca nel più ampio quadro delle politiche nazionali ed europee per la trasformazione digitale della scuola e per lo sviluppo delle competenze digitali e di cittadinanza. L'istituzione scolastica intende governare tale transizione in modo consapevole, responsabile e trasparente, valorizzando le potenzialità dell'IA per migliorare la qualità dell'offerta formativa e dei servizi, nel pieno rispetto della centralità della persona e dei diritti fondamentali, così come indicato anche dalle [Linee guida per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche](#).

1.1. Finalità del Piano d'Istituto per l'Intelligenza Artificiale

Il Piano d'Istituto per l'Utilizzo della Intelligenza Artificiale (di seguito "PUIA") definisce le scelte culturali, pedagogiche, organizzative e tecnologiche con cui la scuola intende orientare l'uso dei sistemi di IA, integrandoli nei curricoli, nella didattica e nei processi gestionali. Il PUIA persegue le seguenti finalità generali:

- promuovere un uso critico, etico e sicuro dell'IA da parte di studenti, docenti e personale, in coerenza con i principi di trasparenza, equità, inclusione e non discriminazione;
- migliorare gli apprendimenti e valorizzare potenzialità, talenti e inclinazioni di ciascuno studente, anche attraverso percorsi personalizzati e strumenti di supporto all'inclusione;
- semplificare e ottimizzare i processi amministrativi e organizzativi dell'istituto, potenziando l'efficienza dei servizi rivolti alla comunità scolastica e al territorio;
- sviluppare le competenze digitali e di cittadinanza digitale, in linea con i documenti di indirizzo nazionali ed europei e con gli obiettivi del PTOF.

Il PUIA costituisce parte integrante del PTOF e ne specifica le linee di sviluppo sull'innovazione digitale, nel rispetto dell'autonomia scolastica e del profilo educativo, culturale e professionale degli indirizzi di studio attivati.

1.2. Riferimenti europei, nazionali e al Piano Scuola 4.0

Il PUIA si ispira 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](#)".



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



semplici le procedure e migliorare i servizi rivolti alla comunità scolastica, senza mai comprimere diritti né generare disparità nell'accesso all'istruzione.

2.2. Uso critico, consapevole e responsabile dei sistemi di IA

L'istituto si impegna a sviluppare competenze critiche verso i sistemi di IA, affinché studenti, docenti e personale amministrativo comprendano potenzialità, limiti e rischi degli strumenti adottati. L'IA è presentata come tecnologia di supporto da vagliare e verificare, non come fonte infallibile: si promuove la capacità di riconoscere *bias*, errori, stereotipi e distorsioni, sia nei contenuti didattici sia nelle funzioni amministrative automatizzate.

Le attività di educazione civica digitale includono moduli dedicati all'impatto sociale delle decisioni algoritmiche e all'uso etico dell'IA, mentre per il personale di segreteria e gli uffici si prevedono momenti formativi specifici sull'uso consapevole di strumenti di automazione, chatbot, sistemi di analisi documentale e gestione dei flussi informativi. In tal modo l'istituto promuove un uso responsabile dell'IA in tutti gli ambiti, evitando deleghe acritiche alle macchine.

2.3. Tutela dei dati personali, sicurezza, trasparenza e non discriminazione

La protezione dei dati personali e la sicurezza delle informazioni sono principi irrinunciabili in ogni utilizzo dell'IA, sia didattico sia amministrativo, in conformità a GDPR, Linee guida MIM e pareri del Garante. I sistemi di IA impiegati per la gestione di pratiche amministrative, iscrizioni, gestione del personale, comunicazioni scuola-famiglia o analisi dati devono rispettare i principi di liceità, minimizzazione, limitazione delle finalità e privacy by design e by default.

L'istituto utilizza preferibilmente piattaforme che garantiscano adeguate misure di sicurezza, tracciabilità e controllo umano, evitando funzionalità invasive quali riconoscimento delle emozioni, profilazioni dettagliate o analisi non necessarie di dati sensibili. Nei confronti di studenti, famiglie e personale è assicurata una comunicazione chiara e comprensibile sulle finalità, le modalità e i limiti di utilizzo degli strumenti di IA, compresi quelli impiegati in segreteria e negli uffici, a tutela della trasparenza e della non discriminazione.

2.4. Rischi, limiti e misure di mitigazione nelle attività didattiche e amministrative

Il PUIA riconosce l'esistenza di rischi connessi all'uso dei sistemi di IA, tra cui disinformazione, dipendenza tecnologica, rafforzamento di stereotipi, errori procedurali, violazioni della privacy e possibili impatti negativi sui diritti delle persone. Tali rischi riguardano sia l'uso didattico (contenuti generati, valutazione, feedback agli studenti) sia l'uso amministrativo (istruttorie automatizzate, gestione documentale, comunicazioni automatizzate), e richiedono una costante valutazione preventiva e periodica.

L'istituto definisce pertanto, attraverso una specifica valutazione d'impatto (DPIA), misure di mitigazione specifiche: selezione accurata degli strumenti, definizione di procedure interne per la supervisione umana delle attività automatizzate, controllo dei risultati prodotti dai sistemi di IA, formazione continua di docenti, dirigente, DSGA, personale ATA e operatori degli uffici. Sono stabiliti canali e protocolli per segnalare criticità o malfunzionamenti legati all'uso dell'IA, nonché per sospenderne l'utilizzo in caso di rischi per la sicurezza, la correttezza delle procedure o la tutela dei diritti, garantendo che innovazione e protezione delle persone procedano insieme.



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



3. Obiettivi e ambiti di applicazione dell'IA nella vita dell'istituto

L'istituto integra l'Intelligenza Artificiale per casi d'uso specifici ed in modo organico nella propria azione educativa e organizzativa, con l'obiettivo di migliorare la qualità degli apprendimenti, l'inclusione, l'efficienza dei processi amministrativi e la qualità dei servizi offerti alla comunità scolastica. Negli specifici casi d'uso, che saranno individuati nel corso del periodo di sperimentazione, la IA è utilizzata come strumento di supporto alla didattica disciplinare e trasversale, alla progettazione e valutazione, nonché alle attività di segreteria, gestione del personale, comunicazione e analisi dei dati, nel rispetto dei principi etici, della normativa vigente e della centralità della persona.

3.1. Obiettivi formativi e didattici

Dal punto di vista formativo, il PUIA mira a individuare le strategie di scelta dei casi d'uso specifici grazie ai quali sviluppare negli studenti competenze digitali avanzate, pensiero critico e consapevolezza rispetto al funzionamento e all'impatto dei sistemi di IA. In particolare, l'istituto intende:

- favorire la personalizzazione degli apprendimenti, attraverso strumenti che adattino contenuti, ritmi e modalità di esercitazione alle caratteristiche dei singoli studenti;
- sostenere l'inclusione e il successo formativo, usando l'IA a supporto di studenti con bisogni educativi speciali, disturbi specifici dell'apprendimento, fragilità linguistiche o situazioni di svantaggio;
- potenziare creatività, *problem solving*, capacità di ricerca, produzione e rielaborazione di contenuti, anche mediante attività laboratoriali che integrino strumenti di IA generativa e analitica.

Tali obiettivi sono declinati nei curricoli, nei progetti di istituto e nei percorsi di educazione civica e cittadinanza digitale, in coerenza con gli indirizzi di studio e con il PTOF.

3.2. Obiettivi organizzativi e amministrativi

Sul versante organizzativo, l'istituto individua casi d'uso specifici affinché l'uso della IA migliori l'efficienza della segreteria e degli uffici, ridurre il carico burocratico e liberare tempo per attività a maggior valore educativo e relazionale. In particolare, il PUIA persegue i seguenti obiettivi:

- semplificare e automatizzare compiti ripetitivi (bozze di circolari, catalogazione di documenti, supporto alla compilazione di modelli, pre-istruttoria di pratiche), mantenendo sempre la supervisione umana;
- migliorare la qualità e la rapidità della comunicazione scuola–famiglie–territorio, anche con strumenti che supportino la traduzione e l'accessibilità linguistica;
- supportare dirigente, DSGA e uffici nell'analisi dei dati (esiti scolastici, frequenze, fabbisogni formativi, indicatori di miglioramento), per una pianificazione più informata e tempestiva.

Tutte le applicazioni amministrative dell'IA sono individuate, progettate e gestite nel rispetto del GDPR, delle Linee guida MIM e delle indicazioni del Garante Privacy, con particolare attenzione alla minimizzazione dei dati e al controllo umano delle decisioni.



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



3.3. Ambiti di applicazione nella didattica

L'IA è integrata nei processi didattici secondo logiche graduali e sperimentali e attraverso casi d'uso (come indicato nelle linee guida ministeriali), con particolare attenzione a:

- IA come oggetto di studio: moduli e percorsi interdisciplinari che introducono concetti di base (dati, algoritmi, modelli, *bias*, AI Act), anche nell'ambito di STEM, informatica, educazione civica e PCTO;
- IA come strumento di supporto alla progettazione didattica: generazione assistita di idee per unità di apprendimento, attività, esempi, esercizi e materiali, sempre validati dal docente;
- IA per la personalizzazione e il feedback: piattaforme che offrono esercizi adattivi e feedback immediato, sotto la guida del docente;
- IA per la valutazione e il monitoraggio: strumenti che aiutano nell'analisi degli esiti e nella costruzione di rubriche, lasciando al docente ogni decisione valutativa.

Le scelte sugli strumenti sono deliberate dagli organi collegiali, nel rispetto delle linee etiche e di sicurezza definite nel PUIA e nella documentazione sulla privacy di istituto.

3.4. Ambiti di applicazione nell'attività amministrativa e gestionale

L'IA è utilizzata anche a supporto dell'organizzazione e dell'amministrazione, con casi d'uso gradualmente introdotti e monitorati. Tra gli ambiti principali si prevedono:

- segreteria didattica e amministrativa: assistenza nella predisposizione di bozze di comunicazioni, circolari, note informative, nel rispetto dei modelli istituzionali; supporto alla classificazione documentale e alla ricerca di informazioni;
- gestione del personale e degli orari: strumenti che aiutino nell'ottimizzazione di orari, turni di sorveglianza, utilizzo di spazi e risorse, sempre con validazione finale da parte dei responsabili;
- analisi e reportistica: strumenti per aggregare e visualizzare dati relativi a iscrizioni, esiti, frequenze, progetti, utili per il RAV, il PDM, la rendicontazione sociale e la programmazione.

In tutti questi ambiti è garantita la supervisione costante da parte del personale competente (dirigente, DSGA, assistenti amministrativi), la possibilità di intervento e correzione delle proposte generate dai sistemi di IA e la tracciabilità delle operazioni, in coerenza con le raccomandazioni nazionali su sicurezza e responsabilità nell'uso dell'IA nella pubblica amministrazione.

4. Governance del Piano e ruoli

La governance del Piano d'Istituto per l'Intelligenza Artificiale (PUIA) si fonda su una chiara distribuzione di ruoli e responsabilità tra le diverse componenti della comunità scolastica, al fine di garantire un'adozione consapevole, etica e sostenibile dei sistemi di IA nella didattica e nell'attività amministrativa. L'istituto opera secondo una logica di collaborazione tra dirigenza, docenti, personale amministrativo, studenti, famiglie e soggetti esterni, valorizzando gli organismi collegiali e i gruppi di lavoro dedicati all'innovazione digitale.



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



4.1. Ruolo del Dirigente scolastico

Il Dirigente scolastico esercita una funzione di leadership strategica nella definizione, attuazione e monitoraggio del PUIA, in coerenza con l'Atto di indirizzo e con il PTOF. A tale figura spetta:

- orientare la comunità scolastica verso un uso consapevole, sicuro ed etico dell'IA, assicurando il rispetto delle norme vigenti e dei principi richiamati dalle Linee guida ministeriali;
- orientare la scelta delle piattaforme tecnologiche da utilizzare verso fornitori che rispettino i principi del GDPR e valutare i rischi dei diversi casi d'uso specifici attraverso la definizione e stesura di una apposita "valutazione del rischio" (DPIA);
- regolamentare l'uso della IA nonché istituire e coordinare il Gruppo di lavoro per l'IA, promuovendo la partecipazione attiva di docenti, personale ATA, DSGA e referenti;
- garantire la istruzione e la autorizzazione al trattamento dei dati a tutto il personale docente, ATA e DSGA relativamente ai casi d'uso regolamentati;
- garantire il raccordo tra PUIA, PTOF, RAV, PDM e documenti sulla privacy, nonché la rendicontazione verso gli organi collegiali e la comunità scolastica.

Il Dirigente si avvale, ove opportuno, di strumenti di IA per attività di analisi e supporto decisionale, mantenendo in ogni caso la responsabilità ultima delle scelte organizzative e pedagogiche.

4.2. Gruppo di lavoro per l'IA e Team per l'innovazione digitale

Presso l'istituto è istituito un Gruppo di lavoro per l'Intelligenza Artificiale, composto dal Dirigente scolastico, dal Referente per la transizione digitale o Animatore digitale, da docenti di diversi indirizzi disciplinari, dal DSGA e da rappresentanti del personale amministrativo, con eventuale supporto del DPO e di esperti esterni.

Il Gruppo di lavoro:

- cura la progettazione, l'aggiornamento e il monitoraggio del PUIA;
- coordina le azioni di sperimentazione didattica e di innovazione amministrativa legate all'uso dell'IA;
- supporta la diffusione delle buone pratiche e la documentazione delle esperienze, promuovendo un confronto sistematico all'interno dei dipartimenti e della segreteria.

Il Team per l'innovazione digitale e l'Animatore digitale, in coerenza con il PNSD, svolgono un ruolo di facilitazione, formazione interna e accompagnamento dei colleghi nell'uso delle tecnologie e degli strumenti di IA nonché di supporto operativo al DS su tutti i punti elencati al paragrafo precedente.

4.3. Ruoli di DSGA, personale di segreteria e referenti per privacy e sicurezza

Il Direttore dei Servizi Generali e Amministrativi (DSGA) e il personale di segreteria sono attori centrali per l'implementazione dell'IA nei processi amministrativi e nella segreteria digitale. In particolare:

- collaborano alla mappatura dei processi che possono essere supportati da strumenti di IA (gestione documentale, comunicazioni, analisi dati, modulistica);



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



- partecipano alla definizione di procedure operative che garantiscano controllo umano, tracciabilità e sicurezza nell'uso dei sistemi di automazione;
- contribuiscono al monitoraggio dei benefici e delle criticità legate all'IA nell'attività amministrativa, proponendo eventuali correttivi.

Il Responsabile della protezione dei dati (DPO) e i referenti per la privacy e la sicurezza informatica affiancano il Dirigente e il Gruppo di lavoro nella valutazione dei rischi, nella verifica della conformità al GDPR e alle Linee guida su IA e privacy, e nella definizione di misure di protezione adeguate.

4.4. Coinvolgimento degli organi collegiali, dei docenti, degli studenti e delle famiglie

Il Collegio dei docenti delibera gli indirizzi pedagogici e didattici relativi all'uso dell'IA, integra le azioni del PUIA nella progettazione curricolare ed extracurricolare e valuta gli esiti delle sperimentazioni. Il Consiglio di istituto definisce le priorità strategiche e le scelte di carattere organizzativo, gestionale e finanziario necessarie per l'attuazione del PUIA, nel rispetto dell'autonomia scolastica.

Docenti, studenti e famiglie sono coinvolti attraverso attività informative, consultazioni, questionari e momenti di confronto sulle opportunità e sui rischi connessi all'uso dell'IA, in un'ottica di corresponsabilità educativa. L'istituto favorisce la partecipazione a reti di scuole, progetti territoriali, percorsi formativi nazionali (ad esempio nell'ambito di Scuola Futura) e collaborazioni con università ed enti di ricerca, per consolidare le competenze e la qualità della governance del PUIA.

5. Formazione, sviluppo professionale e sostenibilità del PUIA

La formazione e lo sviluppo professionale di docenti, personale amministrativo, dirigente e DSGA rappresentano una leva strategica per l'attuazione e il consolidamento del Piano d'Istituto per l'Intelligenza Artificiale. L'istituto promuove percorsi continuativi di aggiornamento che coniughino aspetti tecnico-operativi, pedagogici, organizzativi, etici e giuridici, in coerenza con le Linee guida MIM 2025 e con il PTOF.

5.1. Analisi dei fabbisogni formativi del personale

Ogni anno l'istituto effettua una ricognizione dei fabbisogni formativi relativi all'uso dell'IA, coinvolgendo docenti, personale ATA, DSGA e dirigenza tramite questionari, colloqui e analisi dei bisogni emersi in sede di dipartimento e di collegio. Tale analisi tiene conto:

- dei diversi livelli di competenza digitale e di familiarità con gli strumenti di IA;
- delle esigenze specifiche dei vari indirizzi di studio e dei diversi uffici amministrativi;
- degli obiettivi di miglioramento individuati nel RAV, nel PDM e nei piani di formazione di istituto.

I risultati della ricognizione orientano la programmazione del piano annuale di formazione, con percorsi differenziati e progressivi.



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



5.2. Piano di formazione interno

Sulla base dei fabbisogni rilevati, l'istituto elabora un piano di formazione interno che prevede laboratori, workshop, comunità di pratica e attività di tutoring tra pari sull'uso dell'IA nella didattica e nell'attività amministrativa. Le iniziative, inserite anche in futuri piani di formazione finanziati (come descritto nel seguito del documento), possono riguardare a titolo esemplificativo:

- uso didattico di strumenti di IA generativa e analitica per progettare, personalizzare e valutare percorsi di apprendimento;
- utilizzo di sistemi di IA per la gestione documentale, la semplificazione dei flussi di lavoro di segreteria, la predisposizione di bozze di atti e comunicazioni;
- approfondimenti su privacy, sicurezza, etica dell'IA, con particolare attenzione al trattamento dei dati in ambito scolastico.

Il Team per l'innovazione digitale e il Gruppo di lavoro per l'IA coordinano e documentano le attività formative, favorendo la condivisione di materiali, esempi e buone pratiche tra colleghi.

5.3. Partecipazione a iniziative nazionali, reti e progetti

L'istituto valorizza le opportunità di formazione e aggiornamento offerte a livello nazionale e territoriale, partecipando a percorsi promossi dal MIM, dalla piattaforma Scuola Futura, da reti di scuole, università, enti di ricerca e soggetti qualificati. Particolare attenzione è riservata:

- ai percorsi PNRR e Piano Scuola 4.0 che riguardano competenze digitali, ambienti innovativi, segreteria digitale e IA a scuola;
- ai progetti di ricerca-azione e ai laboratori territoriali sull'uso dell'IA nella didattica disciplinare e interdisciplinare;
- alle iniziative rivolte specificamente al personale amministrativo e ai dirigenti, per l'innovazione dei processi organizzativi e gestionali.

La partecipazione a queste iniziative contribuisce a innalzare il livello di competenza dell'intera comunità scolastica e a mantenere aggiornato il PUIA rispetto all'evoluzione normativa e tecnologica.

5.4. Sostenibilità nel tempo e aggiornamento periodico del Piano

Per garantire la sostenibilità nel tempo del PUIA, l'istituto prevede una revisione periodica delle azioni formative e degli obiettivi di sviluppo professionale, verificandone l'impatto sugli apprendimenti, sui processi amministrativi e sull'organizzazione complessiva. Ogni anno scolastico il Gruppo di lavoro per l'IA, in raccordo con il Collegio dei docenti, il Consiglio di istituto e la segreteria, procede a:

- analizzare esiti, criticità e bisogni emergenti derivanti dall'uso dell'IA in classe e negli uffici;
- aggiornare il piano di formazione, integrando nuove priorità, strumenti, metodologie e indicazioni normative;
- proporre eventuali modifiche al PUIA e al PTOF, in coerenza con il RAV, il PDM e i documenti di indirizzo.



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



La sostenibilità del PUIA è assicurata anche attraverso una programmazione pluriennale delle risorse economiche e strumentali (fondi PNRR, PTOF, bilancio di istituto), l'adesione a reti e partenariati stabili e la progressiva costruzione di competenze interne, in modo da rendere l'innovazione non episodica ma strutturale.

6. Azioni operative e cronoprogramma di attuazione

L'attuazione del Piano d'Istituto per l'Intelligenza Artificiale si articola in fasi operative progressive, che coinvolgono l'intera comunità scolastica e prevedono, in coerenza con il PTOF, una pianificazione triennale con verifiche annuali. Le azioni riguardano sia l'ambito didattico sia quello organizzativo-amministrativo e sono coordinate dal Dirigente scolastico e dal Gruppo di lavoro per l'IA, in raccordo con gli organi collegiali.

6.1. Azioni a breve termine

Nel primo anno di attuazione il PUIA si concentra sull'avvio del percorso, con azioni di analisi, progettazione e prime sperimentazioni. In particolare, sono previste:

- costituzione o aggiornamento del Gruppo di lavoro per l'IA e definizione del piano di comunicazione interna verso docenti, ATA, studenti e famiglie;
- analisi di contesto e mappatura dei bisogni formativi, delle dotazioni tecnologiche, dei processi amministrativi e delle pratiche didattiche esistenti;
- definizione operativa del PUIA (versione 1.0) e sua approvazione negli organi collegiali, con integrazione nel PTOF e nei documenti di istituto;
- avvio di una prima fase di formazione di base per docenti, personale amministrativo e dirigenza sull'uso consapevole dell'IA e sui profili etico-giuridici;
- sperimentazione (sulla base di specifici casi d'uso concordati con la comunità) in classi pilota e in uno o più processi amministrativi a basso rischio (es. supporto alla redazione di bozze di comunicazioni, catalogazione di documenti), con supervisione costante del personale.

Entro la fine del primo anno il Gruppo di lavoro elabora un primo report di monitoraggio, individuando punti di forza, criticità e priorità per l'anno successivo.

6.2. Azioni a medio e a lungo termine

Nel secondo e nel terzo anno di attuazione, il PUIA entra in una fase di consolidamento e strutturale integrazione nella vita dell'istituto, con azioni che si sviluppano in modo progressivo ma continuo.

In questa prospettiva, le azioni a medio e lungo termine si fondono in un unico percorso che prevede: il potenziamento della formazione (intermedia e avanzata) per docenti, personale ATA, DSGA e dirigenza; l'estensione graduale dell'uso dell'IA a tutte le classi e agli indirizzi, con percorsi curricolari e interdisciplinari stabilizzati; l'adozione stabile di strumenti di IA a supporto della personalizzazione degli apprendimenti, della valutazione formativa e del monitoraggio degli esiti; la progressiva integrazione dell'IA nei processi amministrativi e nella segreteria digitale, con procedure codificate, ruoli chiari e standard di qualità; lo sviluppo di comunità di pratica e reti di collaborazione con altre scuole, università ed enti del territorio.



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



Tale fase è accompagnata da una programmazione pluriennale delle risorse economiche e strumentali (anche in collegamento con PNRR e Piano Scuola 4.0) e da cicli periodici di monitoraggio, valutazione e revisione del PUIA e del PTOF, così da rendere l'innovazione non episodica, ma parte integrante e duratura della cultura professionale e organizzativa dell'istituto.

6.3. Cronoprogramma indicativo per anno scolastico

Per ciascun anno scolastico il PUIA è accompagnato da un cronoprogramma operativo che dettaglia tempi, responsabilità e risorse per le principali azioni.

A titolo esemplificativo, nel primo semestre di ciascun anno si prevede:

- conferma/aggiornamento del Gruppo di lavoro e del PUIA;
- individuazione e regolamentazione dei casi d'uso specifici per i quali la valutazione di impatto (DPIA) definisce un basso rischio;
- definizione del piano di formazione annuale;
- avvio delle attività informative verso la comunità scolastica.

Nel secondo semestre si prevede invece:

- la realizzazione delle principali attività formative; avvio o prosecuzione delle sperimentazioni in classe e negli uffici; primo monitoraggio intermedio con raccolta di dati e feedback;
- l'estensione o consolidamento delle pratiche ritenute efficaci; predisposizione di report di monitoraggio; proposta di aggiornamento del PUIA e del PTOF per l'anno successivo.

7. Monitoraggio, valutazione e revisione del Piano

Il monitoraggio e la valutazione del Piano d'Istituto per l'Intelligenza Artificiale sono parte integrante del ciclo di miglioramento dell'istituto e si svolgono in modo sistematico, secondo criteri di trasparenza, partecipazione e misurabilità dei risultati. Le attività di controllo riguardano sia l'impatto dell'IA sugli apprendimenti e sui processi didattici, sia gli effetti sull'organizzazione amministrativa, in coerenza con il RAV, il PDM e la rendicontazione sociale.

7.1. Strumenti e indicatori di monitoraggio

Per il monitoraggio del PUIA l'istituto utilizza un insieme di strumenti qualitativi e quantitativi (questionari, griglie di osservazione, report di utilizzo delle piattaforme, analisi di processo) che consentono di rilevare l'andamento delle azioni e i risultati intermedi. In particolare, vengono definiti indicatori relativi a:

- coinvolgimento di docenti, classi e personale amministrativo nelle attività che prevedono l'uso dell'IA;
- miglioramento percepito nella qualità della didattica, nella personalizzazione degli apprendimenti e nella gestione dei processi amministrativi;



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it
Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



- frequenza e tipologia di utilizzo degli strumenti di IA, con attenzione al rispetto delle regole di sicurezza e privacy.

Gli indicatori sono scelti in coerenza con il quadro di riferimento nazionale per la valutazione delle scuole e con le specificità del PUIA di istituto.

7.2. Valutazione degli esiti su studenti, docenti e organizzazione

Su base almeno annuale il Gruppo di lavoro per l'IA elabora una relazione sugli esiti del Piano, analizzando i dati raccolti e confrontandoli con gli obiettivi previsti. La valutazione tiene conto:

- degli effetti sull'apprendimento degli studenti (esiti scolastici, partecipazione, motivazione, competenze digitali e di cittadinanza digitale), anche attraverso strumenti di autovalutazione e feedback;
- dell'impatto sulla pratica professionale dei docenti, in termini di innovazione metodologica, uso di strumenti digitali e percezione di supporto fornito dall'IA;
- dei benefici e delle criticità riscontrati nell'organizzazione e nei processi amministrativi (semplificazione delle procedure, tempi di risposta, qualità delle comunicazioni).

I risultati della valutazione sono discussi negli organi collegiali e utilizzati per orientare le successive scelte di formazione, di investimento e di organizzazione scolastica.

7.3. Procedure di revisione annuale e aggiornamento del Piano

In esito al monitoraggio e alla valutazione, il PUIA è soggetto a revisione almeno annuale, con la possibilità di aggiornare obiettivi, azioni, strumenti, cronoprogramma e indicatori. Il processo di revisione prevede:

- la raccolta di proposte migliorative da parte di docenti, personale ATA, studenti e famiglie, anche tramite consultazioni e questionari;
- la redazione, da parte del Gruppo di lavoro per l'IA, di una proposta di aggiornamento del Piano (versioni successive 1.0, 2.0, ecc.), da sottoporre al Collegio dei docenti e al Consiglio di istituto;
- il raccordo con il RAV, il PDM e il PTOF in fase di aggiornamento triennale, assicurando coerenza tra priorità, traguardi e azioni connesse all'uso dell'IA.

Le revisioni sono documentate e conservate agli atti dell'istituto, anche ai fini della rendicontazione sociale e degli eventuali controlli connessi a progetti finanziati (PNRR, Piano Scuola 4.0, altre misure).

7.4. Trasparenza e rendicontazione verso la comunità scolastica

L'istituto assicura la massima trasparenza sulle finalità, le azioni e i risultati del PUIA, nel rispetto delle norme sulla pubblicità degli atti e sulla protezione dei dati personali. I principali documenti (versioni del PUIA, sintesi dei monitoraggi, esiti significativi) sono resi disponibili nel sito web di istituto e presentati in forme accessibili alla comunità scolastica.

La rendicontazione dei risultati legati all'uso dell'IA confluisce nella rendicontazione sociale prevista a conclusione del triennio di riferimento, evidenziando il contributo del PUIA al raggiungimento delle priorità e dei traguardi individuati nel RAV e nel PTOF. In questo modo l'uso dell'IA nella scuola è costantemente sottoposto a verifica pubblica e condivisa, a garanzia della responsabilità e della qualità del servizio educativo.



ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444

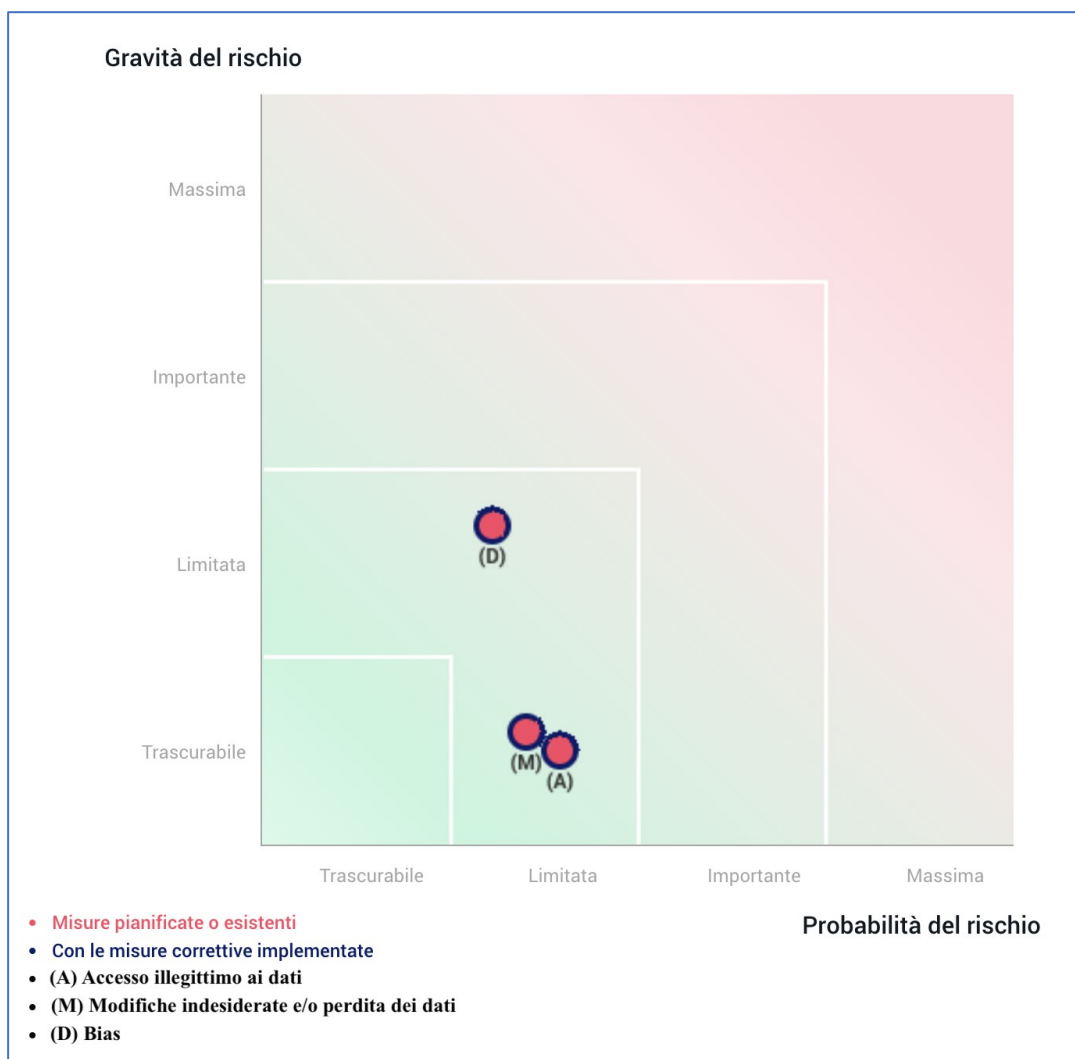
e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it

Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



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 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 delle violazioni dei dati personali

Rischi

 	Accesso illegittimo ai dati
 	Modifiche indesider./perdita dati
 	Bias

Panoramica dei rischi analizzati

Impatti potenziali

Violazione della Privacy: G
Perdita di Dati Sensibili: ...
Violazione dei Regolament
Danno alla Reputazione: U
Perdita di Dati: Le modific
Corruzione dei Dati: I dati.
Errore nei Documenti o Co
Interruzione delle Attività..

Accesso illegittimo ai dati

Gravità : Trascurabile

Probabilità : Limitata

Minaccia

Phishing: Gli attaccanti po.
Violazione delle Credenzia
Attacchi di Forza Bruta: Gl
Vulnerabilità del Software:
Accesso Fisico Non Autori
Accesso a Causa di Errori U
Attacchi Mirati (Spear Phis
Malware: L'installazione di
Accesso da Dispositivi Sm
Accesso da Parte di Ex Dip

Modifiche indesiderate dei dati

Gravità : Trascurabile

Probabilità : Limitata

Perdita di dati

Gravità : Trascurabile

Probabilità : Limitata

Fonti

Phishing: Gli attaccanti po.
Violazione delle Credenzia
Attacchi di Forza Bruta: Gl
Vulnerabilità del Software:
Accesso Fisico Non Autori
Accesso a Causa di Errori U
Attacchi Mirati (Spear Phis
Malware: L'installazione di
Accesso da Dispositivi Sm
Formazione del personale c

Misure

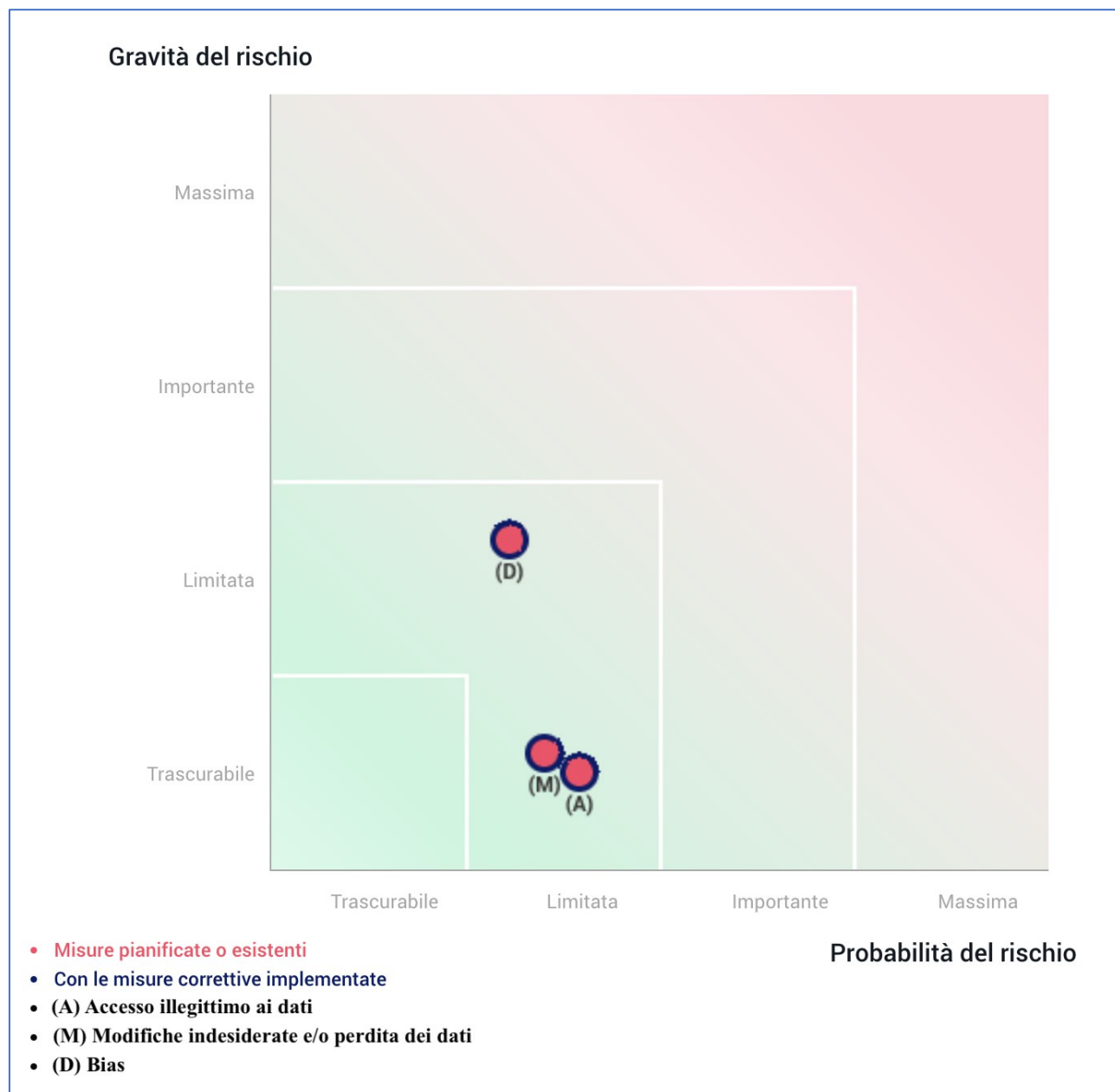
Controllo e gestione degli
Minimizzazione dei dati
Lotta contro il malware
Manutenzione dei sistemi h
Backup dei dati presenti ne
Eliminazione dei document
Tracciabilità delle operazi..
Continuo monitoraggio e ri
Contratto con il responsabi
Politica di tutela della pr...
Formazione specifica del p
Gestione online dei disposi
Sicurezza dei canali inform
Sicurezza dell'hardware
Gestione degli incidenti di.

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 delle 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

NetSense Srl

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

Il Titolare del Trattamento
 Il Dirigente Scolastico
 Dott.ssa Adriana Aprea

documento firmato digitalmente

**ISTITUTO COMPRENSIVO STATALE di PONTASSIEVE**

Via di Rosano, 16/A - 50065 Pontassieve (FI) – Tel. 0558368068 – Fax 0558316444

e-mail: fiic870003@istruzione.it PEC: fiic870003@pec.istruzione.it sito web: www.icpontassieve.it

Cod. Mecc. FIIC870003 – C.F. 94230630488 – Cod. Univoco UFNUM8



Regolamento per l'utilizzo dell'Intelligenza Artificiale in istituto

L'Intelligenza Artificiale rappresenta una delle trasformazioni tecnologiche più rilevanti del contesto educativo contemporaneo, offrendo nuove opportunità di supporto ai processi di insegnamento, apprendimento e organizzazione scolastica. L'Istituzione scolastica è chiamata a governare tale innovazione in modo consapevole e responsabile, in qualità di deployer, ossia quale soggetto che implementa, configura, utilizza e assume la responsabilità dei sistemi di Intelligenza Artificiale adottati all'interno dell'istituzione, garantendone la corretta integrazione nell'ecosistema digitale di istituto, la gestione dei rischi, la supervisione umana e il rispetto delle norme applicabili, comprese quelle in materia di protezione dei dati personali, etica e trasparenza.

In coerenza con le Linee guida del Ministero dell'Istruzione e del Merito, con il Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA) e con la Valutazione d'Impatto sulla Protezione dei Dati (DPIA), il presente Regolamento definisce il quadro di riferimento per l'utilizzo dei sistemi di Intelligenza Artificiale nell'ambito delle attività didattiche, educative, organizzative e amministrative, promuovendo un uso etico, trasparente, spiegabile e sotto controllo umano, orientato alla tutela dei diritti e al miglioramento della qualità dell'azione scolastica.

Indice e sommario

1. Oggetto e finalità	2
2. Ambito di applicazione	3
3. Amministrazione e governo dell'ecosistema di Intelligenza Artificiale	3
4. Ruoli e responsabilità dei soggetti coinvolti	4
5. Alfabetizzazione e formazione in materia di Intelligenza Artificiale	5
6. Utilizzo dell'Intelligenza Artificiale nelle attività didattiche	5
7. Utilizzo dell'Intelligenza Artificiale nelle attività amministrative e organizzative	6
8. Tutela dei dati personali, sicurezza e controllo	7
9. Monitoraggio, segnalazioni, sospensione e aggiornamento	8
10. Uso improprio e misure correttive	8

1. Oggetto e finalità

1. Il presente Regolamento disciplina l'utilizzo dei sistemi di Intelligenza Artificiale (di seguito "IA") all'interno dell'Istituzione scolastica, con riferimento alle attività didattiche, educative, organizzative e amministrative, nel rispetto dei principi di liceità, correttezza, trasparenza, sicurezza e tutela dei diritti e delle libertà fondamentali delle persone.
2. Il Regolamento attua e specifica quanto previsto:
 - dalle Linee guida del Ministero dell'Istruzione e del Merito per l'introduzione dell'Intelligenza Artificiale nelle istituzioni scolastiche;
 - dal Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), parte integrante del PTOF;
 - dalla Valutazione d'Impatto sulla Protezione dei Dati (DPIA) relativa all'utilizzo di sistemi di IA integrati nell'ecosistema digitale di istituto.
3. L'Intelligenza Artificiale è adottata dall'Istituzione scolastica esclusivamente come strumento di supporto ai processi educativi, didattici e amministrativi, e non come sistema decisionale autonomo, nel rispetto del principio di centralità della persona e della necessaria supervisione umana su ogni attività rilevante.
4. Le finalità del presente Regolamento sono:
 - a) promuovere un uso consapevole, critico, etico e responsabile dei sistemi di IA da parte di docenti, studenti e personale scolastico;
 - b) sostenere il miglioramento della qualità dell'offerta formativa, la personalizzazione degli apprendimenti e l'inclusione, in coerenza con il PTOF e il PUIA;
 - c) supportare l'efficienza e la qualità dei processi organizzativi e amministrativi, senza delegare alle tecnologie decisioni che producano effetti giuridici o significativi sugli interessati;
 - d) garantire la protezione dei dati personali, la sicurezza delle informazioni e il rispetto dei principi di privacy by design e by default;
 - e) definire un quadro chiaro di ruoli, responsabilità, limiti e controlli nell'utilizzo dell'IA in ambito scolastico.
5. L'utilizzo dei sistemi di IA rientra nelle attività istituzionali dell'Istituzione scolastica ed è fondato sulla base giuridica dell'esecuzione di un compito di interesse pubblico ai sensi dell'art. 6, par. 1, lett. e) del Regolamento (UE) 2016/679 e dell'art. 2-ter del D.lgs. 196/2003 e ss.mm.ii, come già descritto nella Valutazione d'Impatto sulla Protezione dei Dati DPIA) che deve considerarsi parte integrante e supporto al presente Regolamento. Pertanto, non è richiesto il consenso degli interessati, ferma restando l'obbligatoria informazione e l'esercizio dei diritti previsti dalla normativa vigente.
6. Ogni utilizzo dell'Intelligenza Artificiale all'interno dell'Istituzione scolastica deve avvenire nel rispetto del presente Regolamento, delle deliberazioni degli organi collegiali competenti e delle misure tecniche e organizzative definite nei documenti di istituto in materia di innovazione digitale e protezione dei dati personali.
7. Il presente Regolamento si applica nel rispetto della normativa europea e nazionale vigente in materia di Intelligenza Artificiale e di protezione dei dati personali e deve essere interpretato in modo coerente con le disposizioni del Regolamento (UE) 2016/679, con la normativa nazionale di attuazione, con il Regolamento (UE) 2024/1689 (AI Act), con la Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", e con le Linee guida del Ministero dell'Istruzione e del Merito per l'introduzione dell'Intelligenza Artificiale nelle istituzioni scolastiche, che ne costituiscono il quadro di riferimento sovraordinato. In particolare, ai sensi dell'art. 14 della Legge 132/2025, l'utilizzo dell'Intelligenza Artificiale avviene in funzione strumentale e di supporto all'attività istituzionale, nel rispetto dell'autonomia e del potere decisionale della persona.

2. Ambito di applicazione

1. L'utilizzo dei sistemi di Intelligenza Artificiale è consentito esclusivamente all'interno di un **ecosistema digitale di istituto chiuso, controllato e amministrato, individuato e configurato dall'Istituzione scolastica**. Tale ecosistema è, allo stato attuale, costituito dall'ambiente Google Workspace for Education, all'interno del quale sono attivati e gestiti gli strumenti di Intelligenza Artificiale ed è implementato in modo da garantire l'accesso mediante account istituzionali, la gestione centralizzata delle autorizzazioni, la tracciabilità delle operazioni effettuate dagli utenti e l'adozione di adeguate misure di sicurezza e protezione dei dati personali, in coerenza con la normativa vigente e con la Valutazione d'Impatto sulla Protezione dei Dati (DPIA) di istituto.
2. I sistemi di Intelligenza Artificiale possono essere utilizzati esclusivamente nell'ambito dei **casi d'uso individuati nella Valutazione d'Impatto sulla Protezione dei Dati (DPIA) di istituto e disciplinati nel seguito del presente Regolamento**, previa deliberazione degli organi collegiali competenti.
3. È fatto **divieto** di utilizzare, per finalità didattiche, educative, organizzative o amministrative riconducibili all'Istituzione scolastica:
 - a) strumenti di Intelligenza Artificiale non ricompresi nell'ecosistema digitale di istituto o non espressamente autorizzati;
 - b) account personali o non istituzionali per l'accesso a sistemi di IA connessi ad attività scolastiche;
 - c) sistemi di IA che prevedano decisioni automatizzate o trattamenti non conformi ai principi di liceità, minimizzazione, trasparenza e controllo umano.
4. L'utilizzo dei sistemi di Intelligenza Artificiale nell'ambito del presente Regolamento è soggetto a specifiche **misure di sicurezza e controllo**, che comprendono in particolare:
 - a) la gestione centralizzata degli account e dei profili di accesso da parte dell'amministratore di sistema designato;
 - b) la tracciabilità delle operazioni e degli accessi, nei limiti e con le modalità previste dalla normativa vigente;
 - c) la possibilità di sospendere o limitare l'utilizzo dei sistemi di IA in caso di criticità, rischi per la sicurezza o non conformità alle disposizioni del presente Regolamento, del PUIA o della DPIA.
5. Il presente Regolamento si applica ai seguenti soggetti, nei limiti delle rispettive funzioni, responsabilità e autorizzazioni al trattamento dei dati personali:
 - a) il Dirigente scolastico;
 - b) il personale docente;
 - c) il Direttore dei Servizi Generali e Amministrativi e il personale ATA;
 - d) gli studenti, nell'ambito delle attività didattiche e formative autorizzate;
 - e) eventuali altri soggetti espressamente autorizzati ai sensi della normativa vigente.

3. Amministrazione e governo dell'ecosistema di Intelligenza Artificiale

1. Il governo e la gestione dell'ecosistema di Intelligenza Artificiale dell'Istituzione scolastica sono esercitati dal Dirigente scolastico, in qualità di titolare del trattamento dei dati personali, nel rispetto delle disposizioni normative vigenti, del presente Regolamento, del PUIA e della Valutazione d'Impatto sulla Protezione dei Dati (DPIA).
2. Il Dirigente scolastico designa uno o più **amministratori di sistema**, ai sensi dell'art. 2-quaterdecies del D.lgs. 196/2003 e ss.mm.ii., attribuendo loro specifici compiti di gestione tecnica dell'ecosistema di Intelligenza Artificiale, nel rispetto delle istruzioni impartite e delle misure di sicurezza definite dall'Istituzione scolastica.

3. All'amministratore di sistema competono le attività di configurazione, manutenzione e gestione tecnica dei sistemi di Intelligenza Artificiale autorizzati, nonché la gestione degli accessi e delle credenziali, in coerenza con i profili e le funzioni degli utenti, senza alcun potere decisionale sui contenuti o sugli esiti delle attività didattiche e amministrative.
4. L'Istituzione scolastica mantiene un elenco aggiornato degli strumenti di Intelligenza Artificiale autorizzati all'interno dell'ecosistema digitale di istituto, coerente con i casi d'uso individuati nella Valutazione d'Impatto sulla Protezione dei Dati (DPIA). Tale elenco è gestito dall'amministratore di sistema secondo le indicazioni del Dirigente scolastico e costituisce riferimento per l'attivazione, la configurazione, l'aggiornamento e l'eventuale disattivazione dei sistemi di IA.
5. Il Dirigente scolastico, anche su segnalazione dell'amministratore di sistema, del Responsabile della protezione dei dati (DPO) o del Gruppo di lavoro per l'Intelligenza Artificiale, istituito ai sensi del PUIA, può disporre la sospensione, la limitazione o la disattivazione di singoli sistemi o funzionalità di Intelligenza Artificiale. Il Gruppo di lavoro svolge funzioni di supporto tecnico, pedagogico e organizzativo alla governance dell'uso dell'IA, secondo i compiti e le modalità definiti nel Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale, senza assumere poteri decisionali o responsabilità dirette sui trattamenti.
6. Le attività di amministrazione e di controllo sull'utilizzo dei sistemi di Intelligenza Artificiale sono svolte nel rispetto dei principi di necessità, proporzionalità e trasparenza, garantendo la tracciabilità delle operazioni nei limiti consentiti dalla normativa vigente.

4. Ruoli e responsabilità dei soggetti coinvolti

L'utilizzo dei sistemi di Intelligenza Artificiale all'interno dell'Istituzione scolastica avviene nel rispetto di una chiara attribuzione di ruoli e responsabilità, in coerenza con il presente Regolamento, con il Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA) e con la Valutazione d'Impatto sulla Protezione dei Dati (DPIA), nel quadro delle disposizioni normative vigenti.

1. **Il Dirigente scolastico**, in qualità di titolare del trattamento dei dati personali, esercita la governance complessiva dell'utilizzo dell'Intelligenza Artificiale nell'istituto, assicurando la conformità normativa, pedagogica e organizzativa delle scelte adottate. Egli autorizza i casi d'uso dei sistemi di IA, nel rispetto delle deliberazioni degli organi collegiali, designa gli amministratori di sistema, impartisce le necessarie istruzioni operative e dispone, ove necessario, la sospensione o la limitazione dell'utilizzo dei sistemi di Intelligenza Artificiale.
2. **L'amministratore di sistema**, designato dal Dirigente scolastico ai sensi dell'art. 2-quaterdecies del D.lgs. 196/2003 e ss.mm.ii., svolge funzioni di gestione tecnica dell'ecosistema di Intelligenza Artificiale dell'Istituzione scolastica. Egli opera sulla base delle istruzioni impartite dal Dirigente scolastico, nel rispetto della normativa vigente e delle misure previste dal presente Regolamento, dal PUIA e dalla DPIA, ed è responsabile della configurazione tecnica dei sistemi, della gestione degli accessi e dell'attuazione delle misure di sicurezza, senza assumere in alcun caso poteri decisionali sui contenuti, sulle attività didattiche o sui procedimenti amministrativi.
3. **Il personale docente** utilizza i sistemi di Intelligenza Artificiale esclusivamente per finalità didattiche e formative autorizzate, mantenendo in ogni caso la piena responsabilità pedagogica e didattica delle attività svolte. I docenti sono tenuti a verificare e contestualizzare criticamente gli output generati dai sistemi di IA, a evitare qualunque delega automatica di decisioni valutative o educative e a vigilare sull'uso corretto degli strumenti da parte degli studenti, nel rispetto delle regole di istituto e dei principi di correttezza e trasparenza.
4. **Il Direttore dei Servizi Generali e Amministrativi e il personale ATA** utilizzano i sistemi di Intelligenza Artificiale esclusivamente per finalità organizzative e amministrative autorizzate, operando sotto la supervisione del Dirigente scolastico e nel rispetto delle procedure interne. L'IA è impiegata come strumento di supporto alle attività istruttorie, documentali e organizzative, ferma restando la responsabilità umana per gli atti e i procedimenti amministrativi, che non possono in alcun caso essere delegati ai sistemi automatizzati.

5. **Gli studenti** possono utilizzare i sistemi di Intelligenza Artificiale esclusivamente nell'ambito delle attività didattiche e formative autorizzate dall'Istituzione scolastica e sotto la guida dei docenti. L'uso dell'IA da parte degli studenti è finalizzato allo sviluppo di competenze, al supporto all'apprendimento e al potenziamento del pensiero critico e non può in alcun modo sostituire il lavoro personale, né essere impiegato per eludere le verifiche o le responsabilità individuali.
6. **Il Responsabile della protezione dei dati personali (DPO)** svolge funzioni di consulenza e supporto in materia di protezione dei dati, affiancando il Dirigente scolastico nella valutazione dei rischi, nella verifica della conformità dei trattamenti e nella gestione delle segnalazioni o delle criticità connesse all'utilizzo dei sistemi di Intelligenza Artificiale.

Tutti i soggetti coinvolti nell'utilizzo dei sistemi di Intelligenza Artificiale sono tenuti a rispettare il presente Regolamento, le istruzioni operative impartite dall'Istituzione scolastica e le misure di sicurezza previste, collaborando attivamente alla prevenzione di utilizzi impropri e alla segnalazione di eventuali anomalie o criticità.

Supervisione umana su due livelli: la supervisione dell'utilizzo dei sistemi di Intelligenza Artificiale si articola su due livelli complementari: una supervisione di natura pedagogica e didattica, esercitata dai docenti nell'ambito delle attività educative, e una supervisione di natura istituzionale e organizzativa, esercitata dal Dirigente scolastico, con il supporto dell'amministratore di sistema e del Responsabile della protezione dei dati personali, al fine di garantire la conformità normativa, la sicurezza e il rispetto delle finalità istituzionali.

5. Alfabetizzazione e formazione in materia di Intelligenza Artificiale

L'Istituzione scolastica promuove un adeguato livello di alfabetizzazione e formazione in materia di Intelligenza Artificiale, in attuazione della normativa europea e nazionale vigente, a favore del personale coinvolto nell'utilizzo dei sistemi di IA. La formazione è orientata a sviluppare la conoscenza del funzionamento, delle potenzialità e dei limiti dell'Intelligenza Artificiale, nonché la capacità di un utilizzo critico, responsabile e conforme ai principi del Regolamento, con particolare attenzione alla tutela dei dati personali, alla supervisione umana e alla verifica degli output generati.

Nell'ambito del Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA) e del Piano di formazione del personale, l'Istituzione scolastica individua percorsi formativi differenziati in relazione ai ruoli e alle funzioni, avvalendosi delle risorse offerte dal Ministero dell'Istruzione e del Merito, dagli Uffici Scolastici Regionali, dalle reti di scuole e da altri soggetti qualificati. L'accesso all'utilizzo dei sistemi di Intelligenza Artificiale da parte del personale è subordinato alla partecipazione alle attività formative di base previste.

Parallelamente, la scuola promuove, nell'ambito delle attività didattiche e in coerenza con il curriculum di educazione civica e di cittadinanza digitale, percorsi di alfabetizzazione e sensibilizzazione rivolti agli studenti, finalizzati allo sviluppo di un approccio critico, consapevole e responsabile all'uso dei sistemi di Intelligenza Artificiale.

6. Utilizzo dell'Intelligenza Artificiale nelle attività didattiche

L'Intelligenza Artificiale è utilizzata nell'ambito delle attività didattiche esclusivamente come strumento di supporto ai processi di insegnamento e apprendimento, al fine di favorire la personalizzazione degli apprendimenti, l'inclusione, lo sviluppo delle competenze digitali e del pensiero critico, nonché il supporto alla progettazione didattica e alla riflessione metodologica da parte dei docenti. **In ogni caso, l'IA non può sostituire il ruolo educativo, relazionale e valutativo del docente, che rimane pienamente responsabile delle scelte didattiche e degli esiti formativi.**

I docenti possono utilizzare i sistemi di Intelligenza Artificiale per attività di supporto alla progettazione di percorsi didattici, alla predisposizione di materiali, alla costruzione di esempi, esercitazioni e attività di approfondimento, nonché per l'analisi orientativa degli esiti di apprendimento, ferma restando la necessità di verifica, validazione e contestualizzazione critica dei contenuti e delle indicazioni generate dai sistemi automatizzati.

L'utilizzo dell'Intelligenza Artificiale da parte degli studenti è consentito esclusivamente nell'ambito delle attività didattiche autorizzate dall'Istituzione scolastica e sotto la guida dei docenti, con finalità formative ed educative. Tale utilizzo deve essere orientato allo sviluppo dell'autonomia, della consapevolezza critica e della capacità di comprendere il funzionamento, i limiti e i rischi dei sistemi di IA, e non può in alcun modo sostituire il lavoro personale dello studente.

È fatto espresso divieto di utilizzare sistemi di Intelligenza Artificiale per l'elaborazione automatica di valutazioni, giudizi o voti, nonché per l'adozione di decisioni educative o disciplinari che producano effetti diretti sugli studenti. Ogni valutazione, formativa o sommativa, resta di esclusiva competenza del docente, che ne assume la piena responsabilità.

L'uso dell'Intelligenza Artificiale nelle verifiche, nei compiti e nelle prove di valutazione è disciplinato dai docenti nel rispetto delle regole di istituto e delle finalità educative, tenendo conto del principio di correttezza e di responsabilità individuale. L'eventuale utilizzo non autorizzato di sistemi di IA da parte degli studenti costituisce comportamento non conforme alle regole scolastiche ed è valutato secondo le disposizioni vigenti in materia di comportamento e responsabilità disciplinare.

Le attività didattiche che prevedono l'impiego di sistemi di Intelligenza Artificiale sono progettate in modo da garantire la tutela dei dati personali degli studenti, evitando l'inserimento di dati non necessari, sensibili o eccedenti le finalità didattiche, e assicurando che ogni trattamento avvenga nel rispetto delle misure di sicurezza previste e sotto il controllo dell'Istituzione scolastica.

7. Utilizzo dell'Intelligenza Artificiale nelle attività amministrative e organizzative

L'Intelligenza Artificiale può essere utilizzata nell'ambito delle attività amministrative, organizzative e gestionali dell'Istituzione scolastica esclusivamente come strumento di supporto ai processi interni, in coerenza con il PTOF, con il Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), con i casi d'uso individuati nella Valutazione d'Impatto sulla Protezione dei Dati (DPIA) e con il presente Regolamento.

L'impiego dei sistemi di Intelligenza Artificiale nelle attività amministrative è finalizzato alla semplificazione dei processi, alla riduzione del carico burocratico, al miglioramento dell'organizzazione del lavoro e alla qualità dei servizi resi alla comunità scolastica. In ogni caso, l'IA non può sostituire il ruolo decisionale, valutativo e di responsabilità del Dirigente scolastico, del Direttore dei Servizi Generali e Amministrativi e del personale amministrativo, che restano pienamente responsabili degli atti, dei procedimenti e delle decisioni adottate.

I sistemi di Intelligenza Artificiale possono essere utilizzati a supporto della predisposizione di bozze di documenti, comunicazioni, circolari, atti interni, nonché per attività di supporto alla gestione documentale, alla ricerca di informazioni, all'analisi orientativa di dati aggregati e alla pianificazione organizzativa, **ferma restando la necessità di verifica, validazione e controllo umano su ogni contenuto o proposta generata.**

È in ogni caso escluso l'utilizzo dell'Intelligenza Artificiale per l'adozione automatica di decisioni amministrative o gestionali che producano effetti giuridici o comunque significativi nei confronti di studenti, famiglie o personale. Ogni procedimento amministrativo, incluse le attività istruttorie e le determinazioni finali, deve essere condotto e concluso da soggetti umani competenti, nel rispetto delle norme vigenti e delle procedure di istituto.

L'utilizzo dell'Intelligenza Artificiale nelle attività amministrative avviene nel rispetto dei principi di minimizzazione dei dati, limitazione delle finalità, sicurezza e riservatezza, evitando l'inserimento di dati personali non necessari, sensibili o eccedenti rispetto alle finalità perseguite. In particolare, è escluso l'impiego di sistemi di IA per attività di profilazione dettagliata, valutazione automatica delle persone o analisi non necessarie di dati personali.

Le attività amministrative e organizzative che prevedono l'impiego di sistemi di Intelligenza Artificiale sono soggette a supervisione costante da parte del Dirigente scolastico, del DSGA e, per gli aspetti di competenza, del Responsabile della protezione dei dati personali (DPO), nonché alle misure di sicurezza e di controllo definite nel presente Regolamento, nel PUIA e nella DPIA.

8. Tutela dei dati personali, sicurezza e controllo

L'utilizzo dei sistemi di Intelligenza Artificiale all'interno dell'Istituzione scolastica avviene nel pieno rispetto della normativa vigente in materia di protezione dei dati personali, nonché dei principi di liceità, correttezza, trasparenza, minimizzazione dei dati, limitazione delle finalità, sicurezza e responsabilizzazione, come definiti dal Regolamento (UE) 2016/679, dal D.lgs. 196/2003 e ss.mm.ii., dalle Linee guida del Ministero dell'Istruzione e del Merito e dai documenti di istituto.

Ogni trattamento di dati personali connesso all'utilizzo dei sistemi di Intelligenza Artificiale è fondato sulla base giuridica dell'esecuzione di un compito di interesse pubblico ed è disciplinato dalla Valutazione d'Impatto sulla Protezione dei Dati (DPIA) adottata dall'Istituzione scolastica, che individua i casi d'uso, i rischi potenziali e le misure tecniche e organizzative di mitigazione.

È in ogni caso escluso l'utilizzo di sistemi di Intelligenza Artificiale per finalità di identificazione biometrica, riconoscimento delle emozioni, profilazione automatizzata delle persone, valutazione o scoring comportamentale, proctoring automatizzato o altre forme di trattamento che producano effetti giuridici o comunque significativi sugli interessati senza un adeguato controllo umano, in coerenza con la normativa vigente e con le disposizioni applicabili in materia di tutela dei diritti fondamentali.

L'Istituzione scolastica adotta misure di sicurezza adeguate a garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati mediante sistemi di Intelligenza Artificiale, assicurando che l'accesso ai sistemi sia consentito esclusivamente a soggetti autorizzati, mediante account istituzionali e secondo profili di accesso coerenti con le funzioni svolte. Inoltre, L'Istituzione scolastica garantisce che ogni utilizzo dei sistemi di Intelligenza Artificiale sia sottoposto a controllo umano effettivo, sia nella fase di configurazione e gestione dei sistemi, sia nella fase di utilizzo operativo, assicurando la possibilità di intervento, verifica e correzione degli output generati.

L'utilizzo dei sistemi di Intelligenza Artificiale è improntato ai principi di privacy by design e by default, evitando l'inserimento o il trattamento di dati personali non necessari, sensibili o eccedenti rispetto alle finalità istituzionali perseguite. In particolare, è escluso l'impiego di funzionalità invasive o non pertinenti, quali il riconoscimento delle emozioni, la profilazione dettagliata delle persone o l'analisi automatizzata di comportamenti e caratteristiche individuali non strettamente necessarie. Inoltre, i sistemi di Intelligenza Artificiale sono configurati in modo da escludere l'utilizzo dei dati personali degli studenti, del personale e delle famiglie per finalità di addestramento, perfezionamento o sviluppo di modelli di Intelligenza Artificiale da parte dei fornitori o di soggetti terzi. L'Istituzione scolastica verifica, in sede di selezione e configurazione dei sistemi di IA, che siano disattivate le funzionalità che consentono la conservazione dei prompt e della cronologia delle conversazioni per finalità di training, salvo i casi in cui ciò non sia tecnicamente possibile per specifiche funzionalità, garantendo in ogni caso il rispetto del principio di minimizzazione e delle misure di tutela previste dalla Valutazione d'Impatto sulla Protezione dei Dati (DPIA).

Il Dirigente scolastico, con il supporto dell'amministratore di sistema e del Responsabile della protezione dei dati personali (DPO), vigila sul rispetto delle disposizioni del presente Regolamento, del PUIA e della DPIA, adottando le misure necessarie a prevenire e gestire rischi per la sicurezza delle informazioni, per la protezione dei dati personali e per i diritti e le libertà degli interessati.

L'Istituzione scolastica assicura un'adeguata informazione agli studenti e alle famiglie in merito all'utilizzo dei sistemi di Intelligenza Artificiale nell'ambito delle attività istituzionali, garantendo trasparenza sulle finalità, sulle modalità di impiego, sulle misure di tutela adottate e sui principi essenziali di funzionamento dei sistemi utilizzati, in termini chiari e comprensibili. Tale informazione è fornita nel rispetto della normativa vigente in materia di protezione dei dati personali e non comporta la richiesta di consenso, ferma restando la piena conoscibilità dei diritti esercitabili dagli interessati. L'utilizzo dei sistemi di Intelligenza Artificiale avviene nel rispetto dei principi di trasparenza e spiegabilità, assicurando che le logiche di funzionamento essenziali, le finalità e i limiti dei sistemi siano comprensibili in relazione al contesto di utilizzo, senza richiedere conoscenze tecniche specialistiche.

In caso di violazioni della sicurezza, anomalie, malfunzionamenti o utilizzi non conformi dei sistemi di Intelligenza Artificiale che possano incidere sulla protezione dei dati personali o sulla correttezza dei trattamenti,

L'Istituzione scolastica attiva le procedure previste dalla normativa vigente e dai protocolli interni, inclusa, ove necessario, la sospensione dell'utilizzo dei sistemi interessati e la comunicazione agli organi competenti.

9. Monitoraggio, segnalazioni, sospensione e aggiornamento

L'Istituzione scolastica assicura un monitoraggio continuo e proporzionato dell'utilizzo dei sistemi di Intelligenza Artificiale, al fine di verificarne la conformità al presente Regolamento, al Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), alla Valutazione d'Impatto sulla Protezione dei Dati (DPIA) e alla normativa vigente.

Il monitoraggio è finalizzato a individuare eventuali criticità, anomalie o utilizzi non conformi dei sistemi di Intelligenza Artificiale, nonché a valutare l'efficacia delle misure di sicurezza, di controllo umano e di tutela dei diritti delle persone, nel rispetto dei principi di necessità e proporzionalità e senza finalità di sorveglianza generalizzata.

Eventuali segnalazioni relative a malfunzionamenti, utilizzi impropri, rischi per la protezione dei dati personali o violazioni delle disposizioni del presente Regolamento possono essere effettuate dai soggetti coinvolti nell'utilizzo dei sistemi di Intelligenza Artificiale secondo le modalità organizzative definite dall'Istituzione scolastica. Tali segnalazioni sono valutate dal Dirigente scolastico, anche con il supporto dell'amministratore di sistema, del Responsabile della protezione dei dati personali (DPO) e, ove opportuno, del Gruppo di lavoro per l'Intelligenza Artificiale.

Qualora dal monitoraggio o dalle segnalazioni emergano criticità rilevanti in termini di sicurezza, conformità normativa, tutela dei dati personali o coerenza con le finalità istituzionali, il Dirigente scolastico può disporre, anche in via cautelativa, la sospensione temporanea, la limitazione o la disattivazione dell'utilizzo di singoli sistemi di Intelligenza Artificiale o di specifiche funzionalità, fino al ripristino delle condizioni di conformità.

Le misure di sospensione o limitazione dell'utilizzo dei sistemi di Intelligenza Artificiale sono adottate in modo proporzionato e motivato, garantendo, ove possibile, la continuità delle attività didattiche e amministrative mediante strumenti alternativi, e sono accompagnate, se necessario, da azioni correttive, aggiornamenti delle configurazioni o revisione dei casi d'uso e della DPIA.

In coerenza con il PUIA, l'Istituzione scolastica assicura il periodico aggiornamento delle modalità di utilizzo dei sistemi di Intelligenza Artificiale, dei casi d'uso autorizzati e delle misure di tutela adottate, tenendo conto dell'evoluzione tecnologica, delle indicazioni del Ministero dell'Istruzione e del Merito, delle risultanze del monitoraggio e degli eventuali aggiornamenti della Valutazione d'Impatto sulla Protezione dei Dati. Gli aggiornamenti sono adottati secondo le competenze degli organi collegiali e, ove necessario, recepiti nel presente Regolamento o nei documenti di istituto ad esso collegati.

Il monitoraggio e le eventuali misure adottate ai sensi del presente articolo non incidono sulle responsabilità individuali derivanti da comportamenti non conformi alle disposizioni del Regolamento, che restano disciplinate dalle norme vigenti e dai regolamenti di istituto.

10. Uso improprio e misure correttive

L'utilizzo dei sistemi di Intelligenza Artificiale in difformità dalle disposizioni del presente Regolamento, dal Piano d'Istituto per l'Utilizzo dell'Intelligenza Artificiale (PUIA), dalla Valutazione d'Impatto sulla Protezione dei Dati (DPIA) o dalle istruzioni operative impartite dall'Istituzione scolastica costituisce uso improprio e comporta l'adozione delle misure correttive previste dalle norme vigenti e dai regolamenti di istituto.

Le misure correttive sono adottate in modo proporzionato alla gravità del comportamento, alla natura dell'attività svolta e alle eventuali conseguenze prodotte, tenendo conto del contesto educativo e della finalità formativa dell'azione scolastica, nonché dei principi di responsabilità e gradualità.

In relazione all'uso improprio dei sistemi di Intelligenza Artificiale da parte del personale scolastico, le eventuali responsabilità sono valutate secondo le disposizioni normative e contrattuali vigenti e i regolamenti

interni dell'Istituzione scolastica, ferma restando la possibilità di adottare misure organizzative o correttive finalizzate al ripristino delle condizioni di conformità.

In relazione all'uso improprio dei sistemi di Intelligenza Artificiale da parte degli studenti, le eventuali conseguenze sono valutate nel rispetto dello Statuto delle studentesse e degli studenti e delle disposizioni in materia di comportamento e responsabilità disciplinare, privilegiando, ove possibile, interventi di natura educativa e di accompagnamento.

Qualora l'uso improprio dei sistemi di Intelligenza Artificiale comporti rischi o violazioni in materia di protezione dei dati personali, l'Istituzione scolastica attiva le procedure previste dalla normativa vigente, inclusa, ove necessario, la gestione degli incidenti di sicurezza e le comunicazioni agli organi competenti.

Resta ferma la responsabilità individuale per gli atti e i comportamenti posti in essere in violazione del presente Regolamento, senza che l'utilizzo di sistemi di Intelligenza Artificiale possa in alcun modo escludere o attenuare tale responsabilità.

Approvato dal C.I. con delibera numero 4 del 05/03/2026