PIANO D'ISTITUTO PER L'INTELLIGENZA ARTIFICIALE

Ai sensi delle Linee guida MIM 2025

Rev.	Data	Descrizione della modifica	Approvato
0	27/03/2026	Prima emissione	Si
1			
2			
3			
4			
5			

Sommario

1. Introduzione e finalità

L'intelligenza artificiale (IA) rappresenta una delle innovazioni più significative che la scuola è chiamata ad affrontare, configurandosi come un profondo cambiamento culturale che può influenzare l'insegnamento, l'apprendimento e l'organizzazione della vita scolastica. Il Ministero dell'Istruzione e del Merito (MIM), attraverso le Linee guida 2025 (DM 166/2025), ha invitato ogni istituzione scolastica a definire il proprio Piano d'Istituto per l'Intelligenza Artificiale (PIA) al fine di promuovere un utilizzo consapevole, etico e sicuro delle applicazioni di Intelligenza Artificiale

2. Scopo del Piano d'Istituto per l'intelligenza artificiale

Il presente piano descrive sinteticamente le attività a cui è chiamato l'Istituto per integrare nelle proprie attività l'utilizzo degli strumenti di Intelligenza Artificiale, per governarne l'introduzione e l'uso in maniera consapevole e rispettosa delle parti interessate, con particolare attenzione ai soggetti minori, ai soggetti svantaggiati e in generale alla dignità della persona.
A tal fine l'organizzazione ha implementato un sistema di gestione dell'Intelligenza Artificiale come illustrato nel presente piano, conformemente alle normative sotto richiamate per:

- dimostrare la sua capacità nell'utilizzare i sistemi di IA conformemente ai requisiti delle leggi e regolamenti applicabili;
- tutelare tutti gli interessati attraverso l'efficace applicazione del sistema e dei processi di miglioramento continuo e assicurando il rispetto dei requisiti indicati dalle leggi e regolamenti applicabili;
- gestire gli adempimenti relativi al governo degli strumenti di IA stabilendo degli obiettivi di monitoraggio e miglioramento specifici;
- gestire e tenere sotto controllo gli adempimenti relativi alla sicurezza delle informazioni e alla protezione dei dati personali;
- 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 presente documento definisce:

- la politica adottata per guidare la comunità scolastica nell'introduzione dell'IA come strumento educativo e di supporto, enfatizzando che non è un sostituto del pensiero umano;
- l'organizzazione dell'Istituto per il governo della IA
- i processi e le relazioni tra loro
- le responsabilità specifiche

3. Riferimenti normativi

L'Istituto per la gestione della IA e per l'esecuzione delle attività, si attiene a riferimenti normativi e norme cogenti.

- Regolamento Generale sulla Protezione dei Dati (GDPR – Reg. UE 2016/679): Regolamento dell'Unione europea in materia di trattamento dei dati personali e privacy.
- D.Lgs. 196/2003 (Codice della Privacy), modificato dal D.Lgs. 101/2018: Adeguamento della normativa nazionale italiana al GDPR.
- Regolamento (UE) 2024/1689 - AI Act: Regolamento dell'Unione europea volto ad armonizzare l'approccio alla regolamentazione dell'IA e alla protezione dei cittadini.
- Legge 23 settembre 2025, n. 132: Legge italiana sull'IA entrata in vigore il 10 ottobre 2025 che recepisce l'AI Act europeo e introduce norme specifiche per il contesto nazionale.
- Linee Guida per l'Introduzione dell'Intelligenza Artificiale nelle Istituzioni Scolastiche (MIM 2025): Riferimento metodologico e strategico per lo sviluppo del progetto IA nelle Istituzioni Scolastiche.
- "Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law" Consiglio d'Europa – 5 settembre 2024.-Trattato internazionale che garantisce che l'IA sia sviluppata e utilizzata nel rispetto dei diritti umani, della democrazia e dello Stato di diritto.
- Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for Educators – Linee guida della Commissione europea concepite per aiutare gli educatori a comprendere il potenziale che le applicazioni dell'intelligenza artificiale possono avere nell'istruzione e per aumentare la consapevolezza dei possibili rischi.
- Recommendation on the Ethics of Artificial Intelligence – UNESCO. Affronta le questioni etiche relative all'implementazione e alla diffusione a livello globale dell'IA.
- Piano Nazionale Scuola Digitale (PNSD) – Documento di indirizzo del Ministero dell'Istruzione italiano redatto nel 2015, finalizzato alla trasformazione digitale della scuola.

I riferimenti cogenti a cui l'Istituto si riferisce per la gestione della IA sono gestiti mediante i documenti di sistema, nonché attraverso la consultazione sistematica e periodica delle norme cogenti applicabili.
il modulo **mod_01 Elenco documentazione** contiene i documenti elaborati e il loro stato di revisione.

4. Termini e definizioni

Le definizioni e gli acronimi che verranno utilizzati per la redazione della documentazione del sistema di gestione dell'Intelligenza Artificiale sono:

Acronimi

AgID	Agenzia per l'Italia Digitale
ACN	Agenzia per la cybersicurezza nazionale
AI Act	Regolamento Europeo sull'Intelligenza Artificiale
DPIA	Data Protection Impact Assessment (Valutazione d'Impatto sulla Protezione dei Dati)
FRIA	Fundamental Rights Impact Assesasment (Valutazione dell'Impatto sui Diritti Fondamentali)
DPO	Data Protection Officer (Responsabile della protezione dei dati)
DSGA	Direttore dei Servizi Generali e Amministrativi
GDPR	General Data Protection Regulation (Regolamento Generale sulla Protezione dei Dati)
IA	Intelligenza Artificiale
LLM	Large Language Models (Modelli Linguistici di Grandi Dimensioni)
MIM	Ministero dell'istruzione e del merito
PTOF	Piano Triennale dell'Offerta Formativa
RAV	Rapporto di Autovalutazione
SaaS	Software as a Service

Glossario dei termini

Audit dei dati	Processo di valutazione e controllo dei dataset impiegati, finalizzato ad assicurare l'accuratezza, la qualità, la completezza e la conformità dei dati
Bias	Distorsioni sistematiche nei dati o negli algoritmi che possono portare a risultati ingiusti, discriminatori o non rappresentativi della realtà
Chatbot	Software che simula ed elabora le conversazioni umane, consentendo agli utenti di interagire con i dispositivi digitali
Content curation	Processo di raccolta, selezione, organizzazione e personalizzazione di contenuti digitali
Milestone	Punti chiave all'interno di un progetto che segnano il completamento di fasi significative o il raggiungimento di obiettivi intermedi
Privacy by design	Principio secondo cui la protezione dei dati personali deve essere integrata fin dalla fase di progettazione di un sistema o di un servizio
Privacy by default	Principio secondo cui, per impostazione predefinita, un sistema o servizio deve raccogliere solo i dati strettamente necessari e limitarne l'accesso e l'uso
Spiegabilità (XAI Explainable AI)	Capacità di un sistema di IA di fornire ragioni chiare e comprensibili per le sue decisioni e azioni
Accountability	Titolarità di un trattamento dei dati effettuato direttamente o tramite soggetti autorizzati
Stakeholder	Soggetti o gruppi direttamente o indirettamente influenzati dal progetto o attività
Deployer	persona fisica o giuridica che utilizza un sistema di IA sotto la propria autorità
AI Literacy	insieme di competenze fondamentali che tutti i membri della comunità scolastica devono acquisire per utilizzare l'IA in modo informato, sicuro ed etico, comprendendone limiti e potenzialità
Sistemi ad Alto Rischio	i sistemi di IA che, come definiti dall'AI Act, possono che avere un impatto negativo significativo sulla salute, la sicurezza e, nel nostro contesto, sui diritti fondamentali degli studenti (es. accesso all'istruzione, valutazione)

5. Parti interessate

L'Istituto ha individuato le parti interessate e le loro esigenze e aspettative.
In particolare, nella tabella seguente sono individuate:

a) le parti interessate rilevanti per il sistema di gestione dell'Intelligenza Artificiale
b) i ruoli e/o le responsabilità di tali parti interessate rilevanti per il sistema di gestione
c) le aspettative delle parti interessate

Parte interessata	Ruolo e responsabilità	Aspettative
Dirigente Scolastico	Coordina l'attuazione del Piano, autorizza gli strumenti e promuove la formazione	Corretta attuazione degli Atti di indirizzo e del PTOF, tutela legale, tutela del personale, degli studenti e delle famiglie
Referente per l'IA	Svolge funzioni di raccordo, coordinamento e supporto tecnico-pedagogico. Coordina il Gruppo di lavoro per l'IA	Mandato chiaro da parte del Dirigente scolastico, formazione specialistica, strumenti e supporto tecnico dove occorrente
Gruppo di Lavoro per l'IA	Ha funzioni di organizzazione, supporto e monitoraggio delle azioni previste dalle Linee guida MIM 2025 e attuazione del PIA	Mandato chiaro da parte del Dirigente scolastico, formazione specialistica, strumenti e supporto tecnico dove occorrente
DPO	Presta consulenza e collabora all'eventuale stesura di DPIA e FRIA	Rispetto della normativa cogente, informazioni chiare e coordinamento con la Dirigenza scolastica
Docenti	Integrano l'IA nelle attività didattiche in modo consapevole, documentando e condividendo le esperienze	Mandato chiaro da parte del Dirigente scolastico, formazione specialistica, strumenti e supporto tecnico dove occorrente
DSGA	Coordina le acquisizioni delle IA e i rapporti con i fornitori	Tutela legale e mandato chiaro, rispetto dei termini economici proposti da Consip
ATA	Attua le acquisizioni delle IA, utilizza gli strumenti nelle attività amministrative	Mandato chiaro da parte del DSGA, formazione specialistica, strumenti e supporto tecnico dove occorrente
Fornitori	Fornitura degli strumenti IA con adeguata documentazione circa la spiegabilità dei sistemi offerti, certificazioni ISO 2001, ISO 42001 e altre certificazioni pertinenti. Documentazione tecnica adeguata e sufficiente a garantire l'assenza di bias, carenze in termini di cybersecurity o di protezione dei dati personali	Affidabilità dei pagamenti Continuità del rapporto
Studenti	Utilizzo corretto e trasparente degli strumenti di IA proposti dall'Istituto	Spiegabilità dei sistemi utilizzati, formazione, regole chiare per l'utilizzo e i limiti dello stesso, tutela della privacy e dei diritti fondamentali
Famiglie	Trasparenza nell'uso degli strumenti di IA proposti dall'Istituto o utilizzati dagli studenti per le loro attività	Trasparenza e spiegabilità degli strumenti di IA proposti dall'Istituto, monitoraggio e correzione di bias e tutela della privacy e dei diritti fondamentali degli studenti e delle famiglie

Organi di vigilanza e controllo (Agid, Garante per la privacy, ACN, MIM)	Emanazione di regole chiare e tempestive; supporto agli altri stakeholders per le loro attività con gli strumenti di IA	Trasparenza e spiegabilità degli strumenti di IA proposti dall'Istituto. Rispetto delle norme e dei regolamenti in ambito di sicurezza delle informazioni E in ambito di utilizzo degli strumenti di IA. Corretta gestione degli incidenti e delle Non conformità

Il monitoraggio e il riesame delle informazioni che riguardano le parti interessate e i loro requisiti rilevanti viene effettuato almeno una volta l'anno.

6. Scopo e campo di applicazione del sistema di gestione dell'intelligenza artificiale

L'istituzione scolastica considera l'IA un alleato educativo che mira a migliorare l'efficacia dell'insegnamento e a personalizzare i percorsi di apprendimento, nel rispetto dei principi di centralità dell'alunno, trasparenza e sicurezza digitale.
L'Istituto ha deciso di dotarsi di un Sistema di gestione dell'Intelligenza Artificiale per migliorare la propria efficacia didattica e professionale, il rispetto delle aspettative delle parti interessate, l'efficienza nell'utilizzo delle risorse, la gestione degli adempimenti e degli impatti e per una corretta gestione della sicurezza delle informazioni.
Lo scopo del Sistema di gestione dell'Intelligenza Artificiale è:

- Il miglioramento dell'apprendimento con la promozione l'utilizzo dell'IA per l'analisi dei bisogni formativi e per la creazione di percorsi didattici;
- La promozione dell'inclusione attraverso l'adozione di sistemi di IA che favoriscano l'integrazione degli studenti con bisogni educativi speciali (BES) e che contrastino la dispersione scolastica;
- La semplificazione Amministrativa attraverso l'ottimizzazione e digitalizzazione dei processi interni (es. per la gestione assenze, l'elaborazione orari, l'assistenza all'archiviazione) per ridurre il carico burocratico del personale;
- L'incremento della formazione e la crescita delle competenze, conoscenze e consapevolezze necessarie per comprendere, utilizzare e riflettere criticamente sull'IA in modo informato e responsabile) per docenti, personale ATA, studenti e famiglie (AI Literacy).

Importante: L'IA non deve mai diventare uno strumento di sostituzione o di controllo, né un canale di raccolta dati non necessari.

7. Analisi della Situazione di Partenza e Obiettivi

La scuola dispone già di infrastrutture e strumenti digitali consolidati (reti Wi-Fi, piattaforme educative, registro elettronico, account istituzionali) e ha maturato esperienze positive di didattica digitale, soprattutto a partire dal Piano Scuola 4.0.
L'introduzione dell'IA nelle attività previste dall'Istituto scolastico, pur partendo da infrastrutture digitali consolidate, richiede una serie di azioni specifiche:

1. Formazione: Attivare e/o incrementare a tutti i livelli la formazione del personale sull'uso corretto e responsabile degli strumenti di IA;
2. Regole Chiare: Definire e diffondere regole per l'utilizzo degli strumenti di IA da parte di docenti, personale ATA e studenti;

3. Mappatura e Valutazione del rischio: Individuazione degli strumenti effettivamente impiegati e dei relativi livelli di rischio in termini di Cybersecurity, protezione dei dati personali, tutela dei diritti fondamentali di tutte le parti interessate;
4. Sperimentazione: Attuazione di un percorso graduale di sperimentazione didattica controllata, con l'individuazione dei migliori strumenti, il loro monitoraggio e l'esplicitazione di chiare regole di utilizzo;
5. Consapevolezza: Attivare azioni per promuovere l'educazione civica digitale e la consapevolezza etica negli studenti;
6. Miglioramento continuo: Sviluppare buone pratiche didattiche che valorizzino il ruolo attivo dei docenti, del personale amministrativo e degli studenti.

7.1 Focalizzazione sulle persone

L'IA può essere impiegata come: supporto alla progettazione di lezioni o verifiche; strumento di assistenza linguistica, traduzione o sintesi vocale; mezzo per generare esempi o mappe concettuali; ausilio per attività laboratoriali e interdisciplinari; interazione con chatbot didattici; soluzione per sperimentazione e simulazione scientifica, risorsa inclusiva per alunni con DSA o BES.
Tutte le attività dovranno essere svolte sotto la guida e il monitoraggio continuo del docente e non potranno mai sostituire il processo di apprendimento personale.

7.2 Atto di indirizzo

7.2.1 Stabilire l'Atto di indirizzo

La Dirigenza scolastica ha definito, condivide e mantiene attivo un atto di indirizzo del dirigente scolastico per la predisposizione del Piano d'Istituto per l'Intelligenza Artificiale ai sensi delle Linee guida del Ministero dell'Istruzione e del Merito (MIM 2025) appropriato alle attività ed agli scopi dell'Istituto, oltre che alle esigenze di tutte le parti interessate come sopra individuate.

Tale Atto di indirizzo comprende l'impegno a:

- garantire omogeneità alle modalità di utilizzazione sia nell'attività didattica che in ambito amministrativo,
- Assicurare il rispetto del quadro normativo europeo e nazionale riguardo la protezione dei dati, la tutela della *privacy*, delle libertà e dei diritti fondamentali di tutti i soggetti interessati (studenti, famiglie, docenti, personale ATA)
- elaborare un progetto che assicuri agli studenti la formazione di una coscienza critica necessaria per muoversi con consapevolezza in un mondo in cui l'IA offre nuove opportunità, nuove sfide, nuovi rischi
- Promuovere l'IA come prezioso alleato per introdurre nuove forme di insegnamento, creare strumenti didattici interattivi e innovativi, e ridurre i carichi di lavoro ripetitivi del personale docente e di segreteria

e fornisce il quadro fondamentale per la definizione ed il riesame degli obiettivi e le aree di applicazione nell'utilizzo delle IA. Questi principi sono giudicati basilari dal vertice dell'Istituto e quindi mantenuti come costanti anche nel caso di aggiornamenti dell'Atto di indirizzo.

7.2.2 Comunicare l'Atto di indirizzo

l'Atto di indirizzo, allegato al presente Piano di Istituto, viene reso disponibile al Collegio Docenti, costituisce fondamento e parte integrante del piano triennale dell'offerta formativa ai sensi del DPR n. 275/1999 e viene reso disponibile in forma trasparente, in applicazione del principio open

by default ai sensi dell'articolo 52 del decreto legislativo 7 marzo 2005, n. 82 (CAD) a tutte le persone interessate, tramite pubblicazione sul sito istituzionale.
Inoltre l'Atto di indirizzo viene riesaminato almeno a cadenza triennale in occasione dell'aggiornamento del piano triennale dell'offerta formativa.

7.2.3 Raccordo con PTOF, RAV, PDM e Atto di indirizzo del Dirigente scolastico

Il Piano d'Istituto per la IA discende dall'Atto di indirizzo del Dirigente scolastico e ne costituisce articolazione operativa. Gli obiettivi e le azioni previste dal Piano d'Istituto per la IA sono integrati nel PTOF, per quanto riguarda:

- il potenziamento delle competenze chiave degli studenti, con attenzione alle competenze digitali e di cittadinanza;
- l'innovazione metodologica e organizzativa, con l'impiego di ambienti e strumenti digitali avanzati;
- il miglioramento dei risultati scolastici e la riduzione del digital divide, che costituisce fonte per le disuguaglianze nell'accesso e nell'uso delle tecnologie digitali, creando una divisione tra chi può sfruttarne i benefici (istruzione, lavoro, informazione) e chi è escluso, anche mediante l'uso mirato di tecnologie basate su IA.

Il Piano d'Istituto per la IA contribuisce, infine, alla rendicontazione sociale dell'istituto, attraverso il monitoraggio e la documentazione delle azioni realizzate, dei risultati conseguiti e dell'impatto sull'apprendimento degli studenti e sulla qualità dei servizi erogati.

7.2.4 Pianificazione per l'identificazione dei pericoli e per la valutazione dei rischi

L'Istituto ha stabilito nella **Pr_02 Valutazione del Rischio** le modalità per l'identificazione continua dei pericoli, per la valutazione dei rischi, l'implementazione delle necessarie misure di controllo e la valutazione delle opportunità. L'effettuazione di tale attività e dei risultati emersi, sono documentate, conservate e mantenute aggiornate.
La metodologia utilizzata per l'identificazione dei pericoli e per la valutazione dei rischi:

- È definita in base alle finalità, natura e tipologie degli strumenti di IA prescelti, prima della messa in esercizio degli stessi, in modo da assicurare che essa sia propositiva piuttosto che reattiva
- Provvede all'identificazione, classificazione e documentazione dei rischi e ad applicare i relativi controlli in modo appropriato
- Per la gestione dei cambiamenti, prima della loro introduzione, l'organizzazione identifica i pericoli ed i rischi associati ai cambiamenti, oltre che alle conseguenze sui diritti fondamentali degli interessati e sulla loro tutela in termini di riservatezza e dignità.

Sono prese in considerazione per l'identificazione dei pericoli e la valutazione dei rischi per l'utilizzo delle intelligenze artificiali:

- Gli utilizzi previsti delle IA
- Le attività, anche potenziali, di tutto il personale che accede all'uso di tali strumenti
- I comportamenti umani, idoneità, formazione, bias ed altri fattori umani
- Pericoli creati nell'uso degli strumenti IA che possono essere relazionati ad attività sotto il controllo dell'organizzazione
- L'identificazione dei pericoli originati dagli utilizzatori delle IA aventi influenza sulla sicurezza, sui diritti fondamentali, sulla dignità delle persone sotto il controllo dell'Istituto, o che operano all'interno del controllo diretto dell'Istituto
- Strumenti, attrezzature e materiali utilizzati in relazione all'uso delle IA, inclusi quelli forniti da terzi
- Cambiamento o proposte di cambiamento nell'organizzazione, nelle sue attività, o materiali
- I requisiti legali applicabili alla valutazione del rischio ed all'implementazione di controlli relativi

- La progettazione di nuovi utilizzi delle IA, installazioni, aggiornamenti, procedure ed organizzazione delle attività, incluse le capacità ed idoneità delle risorse umane.

L'Istituto assicura che i risultati della valutazione siano considerati quando vengono definite le relative misure di controllo.
Quando vengono determinate le misure di controllo, o modificate, sono effettuate le necessarie considerazioni al fine della riduzione dei rischi secondo la gerarchia di seguito riportata:

1. eliminazione del rischio
2. adozione di misure tecnologiche per il monitoraggio o blocco dei fattori di rischio
3. adozione di controlli procedurali/organizzativi
4. adozione di dispositivi di blocco e monitoraggio delle IA

7.2.5 Prescrizioni legali e altre prescrizioni

L'organizzazione ha stabilito, attua e mantiene attiva una procedura documentata (**Pr_01 Gestione delle informazioni documentate**, a cui si rimanda) al fine di:

- identificare ed avere accesso alle prescrizioni legali applicabili ed alle altre prescrizioni eventualmente sottoscritte, in merito ai propri aspetti relativi alla gestione degli strumenti di Intelligenza Artificiale.
- determinare come tali prescrizioni si applicano ai propri aspetti relativi alla gestione degli strumenti di Intelligenza Artificiale.

Esse sono tenute in considerazione nello stabilire, attuare e mantenere attivo il sistema di gestione.

7.3 Ruoli, Responsabilità e autorità nell'organizzazione

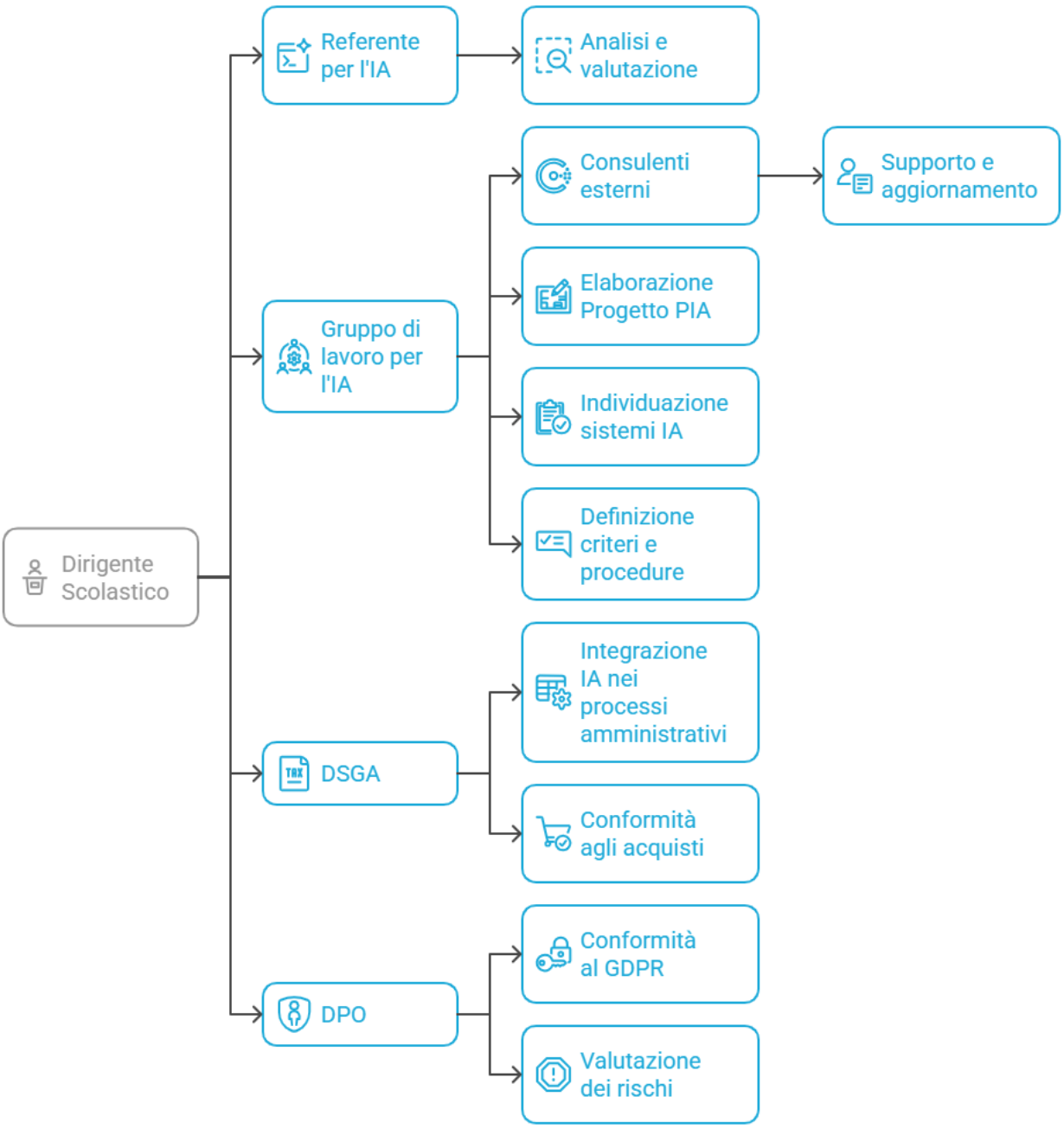
La struttura organizzativa, le responsabilità, le autorità, i ruoli ed i rapporti reciproci del personale le cui attività hanno diretta influenza sul sistema di gestione, sono stabilite e documentate nell'**organigramma e nel funzionigramma dell'Istituto**. I compiti e le responsabilità sono descritti di seguito**.**

7.3.1 Compiti e Responsabilità

Soggetto	Ruolo e funzione	Compiti
Dirigente Scolastico	Responsabile della *governance* etica, normativa e strategica dei sistemi di IA adottati. Promuove un utilizzo consapevole, responsabile ed etico dell'IA, garantendo la chiara definizione dei ruoli, la valutazione d'impatto e il continuo monitoraggio degli esiti.	• Redazione degli Atti di indirizzo • Rappresenta l'Istituto verso terzi • Nomina del Referente per l'IA • Individuazione e approvazione dei membri del gruppo di lavoro per l'IA • Coordina la comunicazione con le famiglie, gli studenti, il personale docente • Sottoscrive le DPIA e le FRIA
Referente per l'IA / Animatore Digitale	Referente per l'IA e per la Transizione Digitale. Funzioni di coordinamento didattico e tecnico, verifica della coerenza con le linee di indirizzo MIM.	• Ha l'autorità di analizzare, valutare e decidere ogni iniziativa concernente l'uso dell'IA • Coordina i lavori dei membri del gruppo di lavoro per l'IA • Coordina i consulenti esterni eventuali • Garantisce la coerenza delle IA con le indicazioni ricevute dalla Dirigenza e dal DPO • Riferisce alla Dirigenza sulle prestazioni del Sistema di Gestione della IA
Gruppo di lavoro per l'IA	Unità operativa interdisciplinare, composta da Animatore Digitale, DSGA, Funzioni Strumentali, Team per l'innovazione e docenti esperti, con il compito di elaborare il Progetto PIA, individuare i sistemi da adottare, definire criteri e procedure di impiego pedagogicamente motivato e tecnicamente sicuro. Collabora con i Dipartimenti disciplinari per le scelte didattiche e il DPO per la conformità normativa in tema di protezione dei dati personali.	• Individua gli strumenti IA • Raccoglie la documentazione degli strumenti prescelti e la analizza • Verifica la coerenza delle IA con le indicazioni ricevute dalla Dirigenza e dal DPO • Verifica la coerenza delle IA con le Linee guida del MIM e le altre normative applicabili • Individua e vigila i criteri di monitoraggio e di controllo delle IA • Individua e promuove i piani formativi • Redige e monitora modulistiche, materiale formativo e informativo • Individua i fattori di rischio e le misure di sicurezza, ai fini della valutazione dei rischi della IA • Redige le valutazioni dei rischi, le DPIA e le FRIA con la consulenza del DPO • identifica i problemi relativi ai casi di "non conformità", all'analisi della cause di incidenti nell'uso delle IA • Verifica le segnalazioni dei bias e le altre segnalazioni ricevute dalle parti interessate

Soggetto	Ruolo e funzione	Compiti
DSGA (Direttore dei Servizi Generali e Amministrativi)	Responsabile dell'integrazione dei sistemi di IA nei processi amministrativi, della conformità agli acquisti, e del coordinamento della gestione contrattuale.	• Coordina le acquisizioni delle IA prescelte • valutare e qualificare i fornitori, in collaborazione con il Referente per l'IA • Coordina la formazione del personale ATA • Approva il materiale informativo e formativo per il personale ATA • Assicura la disponibilità delle necessarie risorse • Gestisce la documentazione circa la formazione erogata al personale
DPO (Data Protection Officer)	Garantisce la conformità al GDPR e rilascia pareri vincolanti sulla valutazione dei rischi dei sistemi di IA adottati. È essenziale per la redazione e/o approvazione di DPIA (Valutazione d'Impatto sulla protezione dei dati) e FRIA (Valutazione d'Impatto sui Diritti Fondamentali).	• Vigila sulla protezione dei dati personali nell'uso delle IA • Verifica e approva le DPIA e le FRIA • Verifica e approva le modulistiche in tema protezione dei dati personali nell'uso delle IA • Informa la Dirigenza scolastica sugli aggiornamenti normativi • Supporta la Dirigenza nella segnalazione di eventuali data breach
Consulenti esterni specializzati	Il gruppo di lavoro potrà avvalersi di consulenti esterni in materia normativa, tecnologica, pedagogica e organizzativa, per la definizione di procedure e l'analisi dei rischi.	• Supporta, informa e aggiorna il Gruppo di lavoro per l'IA e la Dirigenza scolastica • Fornisce pareri e supporto tecnico specialistico

Flusso di Responsabilità e Compiti nell'Adozione dell'IA



8. Consultazione e partecipazione docenti, personale ATA e studenti

8.1 Comunicazione interna

Relativamente alle comunicazioni alla partecipazione ed alla consultazione relative al SGIA, il personale e gli studenti sono coinvolti in maniera significativa nella gestione dell'Intelligenza artificiale attraverso le seguenti iniziative:

- Incontri e riunioni formalizzate con il personale e gli studenti;
- Consigli di classe, consigli di Istituto;
- incontri informali con valenza prevalentemente informativa;
- Ordini di servizio del Dirigente scolastico e del DSGA;
- Istruzioni per il personale e per gli studenti;
- Comunicati alle famiglie .

Viene inoltre mantenuto il:

- Coinvolgimento diretto del DPO nell'ambito del sistema di gestione dell'IA il piano formativo, l'analisi degli incidenti e l'analisi degli strumenti adottati;
- Coinvolgimento diretto del personale docente e del personale ATA per le modalità di implementazione del sistema di gestione;
- Coinvolgimento nell'ambito dei corsi di formazione dovuta per legge;
- Coinvolgimento dei diretti interessati ai fini dell'analisi delle cause e per le misure di prevenzione di incidenti o perdite di dati.

Relativamente a incidenti, perdite di dati o data breach, gli stessi sono analizzati nella **Scheda analisi incidente/modulo azione correttiva** e registrati nel **Registro Non conformità, Incidenti e Data breach**
Tali eventi sono registrati aprendo una non conformità come indicato nella procedura **Pr_03 gestione incidenti e data breach.**

8.2 Comunicazione esterna

La comunicazione esterna ed i principali strumenti utilizzati per la sua gestione possono essere:

- Azioni di coordinamento con il MIM, con l'Ufficio scolastico Regionale;
- Comunicazione da e verso i fornitori delle piattaforme di IA utilizzate;
- Comunicazioni nei confronti dell'Autorità Garante per la privacy, il CSIRT e l'ACN in caso di incidenti o data breach;
- Comunicazioni in ingresso e in uscita con le famiglie degli studenti;

Le comunicazioni dirette sono gestite e quando pertinente protocollate dalla segreteria.

9. Conservazione documentale

Il lavoro e le consultazioni degli strumenti IA sono regolati secondo i seguenti principi, indicati dalle Linee guida del MIM e del Garante per la privacy:

- **Minimizzazione dei dati**: Devono essere raccolti ed elaborati solo i dati personali strettamente necessari per scopi educativi specifici e legittimi o per attività gestionali esplicitate e attentamente valutate in termini di riservatezza e di criticità dei dati inseriti per l'elaborazione.
- **Limitazione della finalità**: I dati raccolti non devono essere utilizzati per scopi diversi da quelli originariamente comunicati ai lavoratori, agli studenti e alle famiglie, a meno che non vi sia una attenta valutazione della base giuridica ed eventualmente un esplicito da parte degli interessati.

- **Conservazione limitata**: I dati devono essere conservati per il solo periodo necessario al raggiungimento delle finalità per cui sono stati raccolti. Una volta esaurito tale scopo (ad esempio, il completamento di un'attività didattica, l'elaborazione di un orario di lavoro), i dati inseriti devono essere cancellati o resi anonimi in modo sicuro e irreversibile.
- **Trasparenza e responsabilità**: L'Istituto ha l'obbligo di informare chiaramente gli interessati (studenti, genitori, personale) sulle modalità e i tempi di trattamento e conservazione dei loro dati personali.
- **Spiegabilità** Deve essere mantenuta traccia dei processi decisionali e delle strategie che hanno portato ai risultati, in modo da poter ricostruire anche a distanza di tempo i risultati e le origini degli stessi.

Per quel che riguarda documentazione prodotta, sia essa costituita da documenti cartacei o da registrazioni elettroniche, la segreteria, coordinata dal DSGA, si occupa dell'archiviazione e conservazione documentale rispettando i parametri richiesti dal massimario di scarto per le istituzioni scolastiche pubblicato dal MIM, dalle linee guida del CAD D.Lgs. 82/2005, D.P.C.M. 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico"; al D.P.R. 445 del 20 dicembre 2000 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa; dal D.P.C.M. del 13 novembre 2014 – Regole tecniche in materia di sistema di conservazione e dalla Circolare del M.I.B.A.C. n. 44/2005.

L'eliminazione documentale è soggetta alla autorizzazione della Soprintendenza archivistica, ai sensi dell'art. 21, comma 1, D.lgs. 42/2004 "Codice dei beni culturali".

Per i dettagli si rimanda al manuale di gestione del protocollo informatico, dei documenti e dell'archivio adottato, mantenuto dal Responsabile della gestione documentale.

10. Pianificazione

10.1 Azioni per evidenziare e trattare i rischi

Durante la pianificazione del Sistema di gestione, la nostra organizzazione ha considerato le parti interessate e il campo di applicazione del Sistema, per trattare i rischi, al fine di:

- Dare assicurazione che il Sistema di gestione della IA raggiunga i risultati attesi
- Prevenire, o ridurre, effetti indesiderati
- Mettere in atto il miglioramento continuo

È stato utilizzato l'approccio del risk management secondo la norma ISO 31000, ed in particolare gli strumenti indicati nella linea guida ISO 31010 e quelli individuati nella ISO 27001 per i rischi "RID+D" ovvero i rischi in termini di perdita di Riservatezza, Integrità delle informazioni, Disponibilità delle stesse, oltre a valutare il rischio per la Dignità e i Diritti fondamentali dei soggetti interessati.
Secondo tali riferimenti la gestione dei rischi è il processo logico che identifica gli elementi critici e le opportunità dovuti alle attività svolte ed al contesto aziendale.

Il processo di valutazione dei rischi è descritto nella procedura **Pr_02 Valutazione del rischio** alla quale si rimanda per ogni dettaglio.

In ogni caso, l'organizzazione:

a) Stabilisce e mantiene i criteri di rischio che includano:
   1. I criteri per l'accettazione del rischio;
   2. I criteri per effettuare valutazioni del rischio relativo alla sicurezza nell'uso delle IA;
b) Assicura che le ripetute valutazioni del rischio producano risultati coerenti, validi e confrontabili tra di loro;

c) Identifica i rischi relativi alla sicurezza nell'uso della IA, associando i rischi alla potenziale perdita di riservatezza, integrità e disponibilità delle informazioni ed identificando possibili rischi per la dignità e i diritti fondamentali degli interessati;
d) Analizza i rischi determinandone il livello di rischio sulla base della valutazione delle loro conseguenze e probabilità;
e) Pondera i rischi confrontandoli con i criteri di rischio e li ordina per dare la corretta priorità per il loro trattamento.

10.2 Classificazione del rischio

Il Gruppo di lavoro per la IA valuta il rischio connesso all'uso dei sistemi IA, adottando misure proporzionate al livello di rischio stabilito dall'AI Act:
I livelli di rischio sono i seguenti:

Sistemi a **Rischio Inaccettabile** (VIETATI)
È posto il divieto assoluto di utilizzare sistemi che costituiscono una chiara minaccia ai diritti fondamentali, come il riconoscimento biometrico e/o emotivo negli ambienti educativi e i sistemi di social scoring

Sistemi ad **Alto Rischio** (OBBLIGHI STRINGENTI E LIMITAZIONI)
La scuola adotta una politica di esclusione preferenziale per i sistemi classificati come Alto Rischio (quelli che influenzano significativamente la vita o la carriera educativa degli studenti)

- È posto il divieto assoluto sull'uso di sistemi di IA per prendere decisioni finali o sommative relative a promozione, non ammissione o assegnazione di voti finali; l'IA può solo fungere da supporto e analisi per il docente.
- Sono esclusi sistemi che generano profilazioni comportamentali o cognitive invasive degli studenti per scopi diversi dal supporto immediato all'apprendimento individualizzato.
- Se l'adozione di un sistema ad Alto Rischio è necessaria (e non esistono alternative a rischio inferiore), è obbligatorio eseguire una rigorosa Valutazione d'Impatto sulla Protezione dei Dati (DPIA) e una Valutazione d'Impatto sui Diritti Fondamentali (FRIA). Deve essere garantito un Controllo Umano Rafforzato (Human Oversight), assicurando che la decisione finale sia sempre presa da un docente formato e responsabile, con l'autorità di ignorare l'output dell'IA.
- Trasparenza: I docenti devono essere in grado di comprendere e spiegare le basi logiche (spiegabilità) su cui l'IA ha formulato suggerimenti.

Sistemi a **Rischio Limitato**
L'utilizzo di tali sistemi deve garantire l'obbligo di trasparenza (informando gli utilizzatori che si interagisce con un sistema IA) e l'etichettatura (i contenuti generati devono essere chiaramente individuati come tali).

10.3 Attività di pianificazione

L'organizzazione pianifica l'inserimento di ogni nuova IA con la raccolta delle informazioni sulla stessa, della documentazione tecnica disponibile, dell'eventuale spiegabilità dei processi decisionali.
Qualora l'Istituzione decida di adottare un sistema classificato come Alto Rischio (es. per l'ottimizzazione di percorsi didattici individualizzati per alunni con DSA, ove non esistano alternative), deve:

Eseguire una **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)** (Art. 35 GDPR) e una **Valutazione d'Impatto sui Diritti Fondamentali (FRIA)**. Tali valutazioni devono dimostrare che i rischi residui sono minimi e accettabili, e che l'intervento umano è garantito.

Attivare un Controllo Umano Rafforzato (Human Oversight):

La supervisione umana non deve essere meramente formale. Il docente deve avere la capacità tecnica e l'autorità effettiva di ignorare, modificare o invalidare qualsiasi output del sistema IA. Deve essere previsto un meccanismo di "Human in the Loop" (intervento umano nei processi automatizzati) che assicuri che la decisione finale sia sempre presa da un docente formato e responsabile, non dall'algoritmo.

Trasparenza Totale e Spiegabilità:
Il sistema deve essere spiegabile; i docenti devono essere in grado di comprendere e, se necessario, spiegare a studenti e famiglie le basi logiche su cui l'IA ha formulato i suoi suggerimenti o previsioni.
Studenti e famiglie devono ricevere una informativa dettagliata e preventiva sull'uso del sistema ad Alto Rischio, con possibilità di accesso a un ricorso umano effettivo contro le decisioni basate sull'IA.

10.4 Contenuto della DPIA

In coerenza con le linee guida del Garante Privacy e dell'EDPB, la DPIA deve contemplare:

A) Descrizione Sistematica del Trattamento In questa fase vengono analizzate le finalità dell'IA in analisi	
Natura dei dati interessati nell'uso della IA	generici, correlabili a personali, anonimizzati, ecc. ed eventuali nuovi dati personali generati o dedotti dall'utilizzo delle IA
Fonti dei dati	web scraping, database interni, analisi di una selezione di documenti – immagini – video, ecc.
Interazione umana	presenza di "Human-in-the-loop" (l'uomo approva ogni decisione), "Human-on-the-loop" (l'uomo supervisiona) o se il processo è totalmente automatizzato
B) Valutazione di Necessità e Proporzionalità Valutazione, in base ai dati inseriti e al loro trattamento della proporzionalità e della necessità nell'uso degli stessi	
Minimizzazione	Quali processi di anonimizzazione e/o monitoraggio e limitazione dei dati inseriti sono adottati
Base giuridica	Basi giuridiche nel trattamento dei dati personali ai sensi art. 6 e 9 del GDPR e altre eventuali basi giuridiche se applicabili. Particolare attenzione se sono tratttati dati particolari (ex art. 9 GDPR), poiché l'IA spesso ne deduce di nuovi tramite inferenza
C) Analisi dei rischi e delle libertà	
Discriminazione e Bias	Rischio che l'algoritmo riproduca pregiudizi presenti nei dati di addestramento
Opacità (Mancanza di Trasparenza)	Valutazione di come lo strumento prende una decisione o elabora i dati immessi
Accuratezza	Valutazione di possibili allucinazioni o falsi positivi/negativi
Sicurezza Informatica	Rischi specifici come il data poisoning (corruzione dei dati di input) o l'adversarial attacks (manipolazioni intenzionali e sottili dei dati di input progettate per indurre in errore i modelli di machine learning e le reti neurali, portandoli a produrre previsioni o classificazioni errate)

D) Misure di mitigazione e compliance	
Explainability (XAI)	Quali strumenti sono implementati per rendere spiegabile la logica dell'algoritmo
Audit e Test	Verifica di necessità di procedure o test periodici per individuare derive dell'algoritmo (*model drift*) o bias emergenti
Diritto di Opposizione	Quali strumenti sono messi a disposizione dell'utente per garantire la non partecipazione, la cancellazione, l'opposizione al trattamento
E) Valutazione dei rischi residui in termini di RID+D Esplicitazione della valutazione del rischio per la Riservatezza, Integrità dei dati, Disponibilità dei risultati e loro ripercorribilità, Diginità delle persone	

10.5 Contenuto della FRIA

Mentre la DPIA si concentra sulla protezione dei dati, la FRIA ha un respiro più ampio: analizza l'impatto del sistema sulla dignità umana, l'uguaglianza e i diritti democratici.
In coerenza con le linee guida del Garante Privacy e dell'EDPB, la FRIA (Fundamental Rights Impact Assessment) deve contemplare:

A) Descrizione dell'uso previsto e del contesto	
Target	Chi sono i soggetti interessati? (es. studenti minorenni, categorie vulnerabili)
Ambito	In che modo il sistema influenzerà il loro futuro? (es. l'esito del test IA determina l'ammissione a una facoltà prestigiosa)
Limiti geografici e temporali	Per quanto tempo e in quali sedi verrà usato il sistema o saranno conservati i risultati delle elaborazioni
B) Identificazione dei Diritti Fondamentali Coinvolti quali diritti della Carta dei diritti fondamentali dell'UE potrebbero essere intaccati	
Dignità umana	Il sistema riduce le persone interessate a un mero "numero" o "punteggio" applicando processi decisionali basati sullo scoring?
Non discriminazione (Art. 21)	Esiste il rischio che l'IA penalizzi le persone in base a sesso, razza, origine etnica, religione, disabilità, età o orientamento sessuale?
Diritti del minore (Art. 24)	Il sistema agisce nel superiore interesse del minore? Protegge il suo benessere e sviluppo?
Diritto all'istruzione (Art. 14)	L'IA facilita l'accesso allo studio o crea barriere ingiuste?
Diritto alla libertà e alla sicurezza (Art. 6)	L'uso della IA può ledere alla sicurezza o alla libertà delle persone? (per esempio rivelando dati che non devono essere divulgati sull'interessato o sulla famiglia quali lo status di rifugiato, di persona sotto protezione, ecc.)
Rispetto della vita privata e della vita familiare (Art. 7)	L'uso della IA può rivalare domicilio, informazioni sulle comunicazioni private o altri aspetti riservati della famiglia delle persone?
Protezione dei dati di carattere personale (Art. 8)	L'IA può in generale rilevare o manipolare dati di carattere personale eccedenti all'uso consentito e previsto? È necessario un consenso esplicito al trattamento?
C) Valutazione dell'impatto Per ogni diritto identificato è necessario analizzare:	
Rischi	Possibili distorsioni (bias), esclusione sociale, perdita di autostima dell'interessato, automazione del pregiudizio, pericoli per la sicurezza fisica e sociale della persona
D) Misure di mitigazione specifiche per i diritti	

Supervisione umana qualificata	Presenza di docenti e responsabili qualificati, formati, informati e autorizzati
Accessibilità	Garanzia di accesso egalitario, fondato su una parità effettiva, non solo formale, di diritti e opportunità per tutti gli utilizzatori, compresi quelli con ADHD o altre potenziali limitazioni e bisogni speciali
Trasparenza algoritmica	Presenza della garanzia che l'utente sappia di interagire con una IA
Altre eventuali misure di mitigazione	Ulteriori misure di mitigazione emergenti dalla DPIA e dalla FRIA
E) Piano di Monitoraggio	
Meccanismi di reclamo	Presenza di meccanismi di non partecipazione e/o di reclamo
Revisione periodica	Verifica che i sistemi di IA non creino disparità o deviazioni rispetto ai risultati prevedibili

11. Supporto

11.1 Risorse

11.1.1 Generalità

La Direzione dell'Istituto ha provveduto ad individuare le risorse necessarie a garantire che il Sistema di gestione dell'Intelligenza Artificiale sia attuato e mantenuto aggiornato.
Il monitoraggio per l'aggiornamento viene ripetuto annualmente e formalizzato con un verbale, in modo che le risorse rese disponibili siano sempre adeguate in funzione dei mutamenti a cui è soggetto l'Istituto nell'utilizzo dei sistemi di IA.

11.1.2 Persone

Tutto il Personale che L'Istituto impiega per svolgere attività in cui è previsto l'uso delle IA o che hanno influenza sulla selezione e utilizzo degli strumenti IA e sulla sicurezza dei dati ivi trattati, viene selezionato, qualificato, formato e sensibilizzato al fine di assicurarsi il possesso delle appropriate caratteristiche, competenze, capacità e consapevolezza del proprio operato.
Tale attività si estende anche agli studenti e agli utilizzatori dei sistemi IA a qualunque titolo, sotto la pertinenza e il controllo dell'Istituto.

11.1.3 Infrastrutture

La Dirigenze definisce, col supporto del DSGA, del Referente per l'IA, del Team per la IA, con la consultazione del DPO, le infrastrutture necessarie per l'utilizzo dei sistemi di IA nel rispetto della sicurezza e della dignità degli utilizzatori.

11.1.4 Ambiente per il funzionamento della IA

I sistemi di IA adottati sono fatti oggetto di valutazione dei rischi, DPIA, eventuale FRIA e viene mantenuto un **Registro delle Intelligenze artificiali - Elenco aggiornato delle piattaforme e strumenti autorizzati**
adottate e delle informazioni relative correlate.
Il Registro delle Intelligenze Artificiali contiene:

1. Nominativo fornitore del sistema AI
2. Nome del sistema / APP
3. Logica utilizzata

4. Procedura decisionale adottata dal sistema
5. Tecniche di spiegabilità
6. Funzioni attive
7. Limiti intrinseci
8. Bias potenziali
9. Tipologia di dati trattati
10. Minimizzazione dei dati adottata
11. Tempo di conservazione dei dati
12. Qualità dei dati utilizzati
13. Modalità di interazione
14. Presenza di sorveglianza umana
15. Procedura di emergenza in caso di anomalie
16. Scopo previsto nell'utilizzo
17. Parti interessate
18. Frequenza d'uso prevista

11.1.5 Conoscenza organizzativa

L'Organizzazione prima dell'utilizzo dei sistemi di IA, individua le fonti e i tipi di conoscenze necessari ai fini di valutare la funzionalità per i propri scopi e della redazione della valutazione del rischio per la sicurezza e la dignità delle persone.
Tali conoscenze sono sintetizzate nel **Registro delle Intelligenze artificiali**, nei documenti di valutazione, nelle DPIA, nelle eventuali FRIA e nella documentazione tecnica e conoscitiva messa a disposizione dai fornitori dei sistemi di IA.

L'insieme di queste informazioni costituisce la parte più importante della conoscenza organizzativa dell'Istituto.
La valutazione delle conoscenze necessarie viene mantenuta aggiornata e comunque effettuata prima di ogni cambiamento significativo del sistema di gestione della IA o in seguito a modifiche per esigenze specifiche.

11.2 Competenza

L'Istituto sulla base dei fabbisogni rilevati, elabora un piano di formazione che prevede laboratori, workshop, comunità di pratica e attività di tutoring sull'uso dell'IA nella didattica e ed in particolare**:**

- Determina la competenza necessaria per il personale che svolge attività che prevedono l'uso dei sistemi di IA;
- le competenze e la formazione erogata sono monitorate nell'ambito del **Piano formativo.**
- Fornisce formazione-addestramento o intraprende altre azioni per far acquisire la necessaria competenza e consapevolezza del personale, in relazione agli impatti sulla sicurezza e la dignità delle persone
- Valuta l'efficacia delle azioni intraprese
- Assicura che il personale sia consapevole della rilevanza e dell'importanza:
    - ✓ Della conformità agli indirizzi, alle procedure e ai requisiti per la gestione della IA e di come i ruoli e le responsabilità dei vari soggetti contribuiscano a garantire tale conformità, inclusi i requisiti per l'allertamento e la risposta in caso di emergenza
    - ✓ Delle sue attività e di quali siano i rischi significativi ad esse associati
    - ✓ Delle conseguenze potenziali di scostamenti rispetto alle procedure specificate
    - ✓ Sull'uso didattico di strumenti di IA generativa e analitica per progettare, personalizzare e valutare percorsi di apprendimento;
    - ✓ Sull'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;
    - ✓ Svolger inoltre approfondimenti su privacy, sicurezza, etica dell'IA, con particolare attenzione al trattamento dei dati in ambito scolastico.

Verranno promosse attività di formazione annuali per docenti e ATA su:

- uso educativo e didattico dell'IA;
- rischi etici e *bias* algoritmici;
- strumenti inclusivi e compensativi intelligenti.

In merito agli studenti, l'uso dell'IA sarà integrato nel curricolo di Educazione civica e Digitale, con percorsi volti ad aiutare gli studenti a comprendere il funzionamento e i limiti dei sistemi IA, a riconoscere *fake news* o contenuti generati artificialmente, e a sviluppare un pensiero critico.
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.
La segreteria mantiene le registrazioni dell'istruzione, della formazione-addestramento svolti.

11.3 Consapevolezza

L'Istituto si attiva per garantire che il personale sia consapevole dell'importanza del proprio lavoro come contributo all'efficacia del sistema di gestione della IA.
Consci della criticità di questo principio, viene data molta importanza alla formazione ed informazione degli addetti anche con iniziative volte a favorire il coinvolgimento massimo di tutti.

11.4 Comunicazione

La Dirigenza è impegnata per la diffusione di adeguate metodologie e strumenti per la comunicazione interna ed esterna, ritenendola fondamentale garantire la conformità ed il miglioramento continuo.
Le informazioni relative al Sistema di Gestione della IA possono essere diffuse all'esterno a seguito di richiesta proveniente dall'esterno oppure per volontà o esigenza dell'Istituto. La diffusione volontaria viene decisa dalla Dirigenza, che definisce a quali interlocutori indirizzarla, quali informazioni fornire, attraverso quali canali effettuarla, ecc.
La comunicazione esterna, quando necessario mantenerne traccia, deve essere gestita tramite la funzione segreteria e protocollata.

11.4.1 Partecipazione e consultazione

L'Istituto ha stabilito, implementa e mantiene la Partecipazione, comunicazione e consultazione, del Gruppo di lavoro per l'IA, coordinato dal Referente per l'IA che prevede incontri almeno annuali per:

- ✓ Individuare gli strumenti IA, monitorarne la funzionalità e le necessità di cambiamento
- ✓ Raccogliere e analizzare la documentazione degli strumenti prescelti
- ✓ Verificare la coerenza delle IA con le indicazioni ricevute dalla Dirigenza e dal DPO
- ✓ Verificare la coerenza delle IA con le Linee guida del MIM e le altre normative applicabili
- ✓ Individuare e vigilare circa i criteri di monitoraggio e di controllo delle IA
- ✓ Individuare e promuovere i piani formativi per studenti e lavoratori
- ✓ Redigere e mantenere aggiornate modulistiche, materiale formativo e informativo
- ✓ Individuare i fattori di rischio e le misure di sicurezza, ai fini della valutazione dei rischi della IA
- ✓ Redigere le valutazioni dei rischi, le DPIA e le FRIA con la consulenza del DPO
- ✓ identificare i problemi relativi ai casi di "non conformità", effettuare l'analisi delle cause di incidenti nell'uso delle IA
- ✓ Verificare le segnalazioni dei bias e le altre segnalazioni ricevute dalle parti interessate
- ✓ Consultare i fornitori qualora siano introdotti cambiamenti negli strumenti di IAù
- ✓ Consultare il DPO in merito alla protezione dei dati personali

11.5 Informazioni documentate

11.5.1 Generalità

Le informazioni documentate del Sistema di gestione dell'Intelligenza Artificiale dell'Istituto includono:

- ✓ Atto di indirizzo del Dirigente scolastico
- ✓ PTOF
- ✓ Patto di corresponsabilità
- ✓ Organigramma e funzionigramma
- ✓ Piano d'Istituto per l'intelligenza artificiale
- ✓ Procedure documentate
- ✓ Istruzioni Operative, che descrivono in dettaglio ove necessario, le operazioni per la gestione di emergenze, misure di sicurezza, comportamenti da adottare per la gestione degli strumenti di IA
- ✓ Il Registro delle Intelligenze artificiali - Elenco aggiornato delle piattaforme e strumenti autorizzati
- ✓ Il Registro dei trattamento ai sensi Art. 30 del GDPR
- ✓ Valutazione dei rischi, DPIA e FRIA
- ✓ Tutti i documenti necessari per assicurare l'efficace pianificazione, funzionamento e controllo dei processi (normative, leggi e regolamenti, documenti forniti dal fornitore, manuali di funzionamento, licenze)
- ✓ Gli atti di nomina per i referenti IA
- ✓ Il materiale informativo e didattico per studenti, famiglie e lavoratori

11.5.2 Creazione ed aggiornamento

Tutte le informazioni documentate richieste dal Sistema di gestione dell'Intelligenza Artificiale sono tenute sotto controllo con le modalità descritte nella procedura **Pr_01 Gestione delle informazioni documentate**, in particolare per:

- ✓ Approvare, riesaminare ed aggiornare le informazioni documentate
- ✓ Assicurare l'identificazione delle modifiche e dello stato di revisione vigenti
- ✓ Assicurare che le versioni pertinenti dei documenti applicabili siano disponibili nei luoghi di utilizzo, leggibili e facilmente identificabili
- ✓ Assicurare che i documenti di origine esterna necessari siano identificati e che la loro distribuzione sia controllata
- ✓ Prevenire l'utilizzo involontario di documenti obsoleti ed identificarli come tali, se conservati.

E' inoltre emesso e gestito dal Responsabile del Sistema di gestione dell'Intelligenza Artificiale un elenco che riporta tutte le informazioni documentate al fine del controllo stesso (**Mod_01 Elenco informazioni documentate**).

11.5.3 Controllo delle informazioni documentate

Le informazioni documentate del Sistema di gestione, ossia i documenti che forniscono evidenza oggettiva di attività eseguite o di risultati conseguiti, sono appropriatamente conservati, identificati e gestiti, come riportato in procedura **Pr_01 Gestione delle informazioni documentate**.

Esse possono essere elaborate su moduli appositamente predisposti che ne garantiscono la loro leggibilità, poiché prevedono campi standardizzati da compilare, e la facile rintracciabilità, grazie ai codici ed alle date di predisposizione.
In alternativa, possono essere documenti di altro tipo quali Licenze, contratti, allegati tecnici o anche schermate dei programmi utilizzati.
L'identificazione delle registrazioni è determinata dall'eventuale codice del modulo oppure dal nome e dalla data di predisposizione.

Ogni informazione documentata è generalmente archiviata dal Referente per l'IA; tale funzione ha il compito di proteggere le registrazioni, di permetterne la reperibilità alle funzioni interessate e di eliminarle al termine del periodo di conservazione.

12. Attività operative

12.1 Pianificazione e controlli operativi

L'Istituto pianifica i processi necessari alla realizzazione dei propri servizi considerando:
- I requisiti di funzionalità, sicurezza dei dati e delle informazioni che il servizio deve possedere
- I criteri operativi ed i relativi controlli
- Gli obiettivi che l'uso delle IA deve raggiungere
- I processi, documenti e risorse necessari alla realizzazione
- Le operazioni di controllo, verifica, validazione, monitoraggio, ispezione e prove specifiche ritenuti necessari nelle fasi di implementazione e i relativi criteri di accettazione
- Le informazioni documentate che dimostrano la corrispondenza tra il risultato ottenuto ed i requisiti iniziali.

Gli elementi in uscita dalla pianificazione sono rappresentati dalle informazioni documentate del sistema di gestione della IA. Il risultato della pianificazione complessiva del sistema di gestione è infatti costituito dal presente Piano d'Istituto, dalle eventuali procedure/istruzioni operative, dai moduli di registrazione, etc. come indicato nei paragrafi precedenti.

12.2 Valutazione e trattamento del rischio relativo alla sicurezza delle IA

L'Istituto ha determinato la frequenza di valutazione del rischio relativo alla sicurezza delle IA:
- ❖ Ogni anno in sede di coordinamento del Gruppo di lavoro per l'IA, in assenza di non conformità;
- ❖ Al verificarsi di una non conformità;
- ❖ Al verificarsi di un cambiamento significativo degli asset individuati;
- ❖ Al verificarsi di un cambiamento significativo del contesto interno/esterno;
- ❖ In caso di data breach o incidente di cyber security.

La valutazione viene condotta secondo le indicazioni della **Pr 2 Procedura valutazione del rischio**

12.2.1 Determinazione dei requisiti relativi ai sistemi di IA

La selezione delle IA da adottare viene effettuata dal Gruppo di lavoro per l'IA in accordo con il Responsabile, con DSGA e con la Dirigenza scolastica.
Le modalità di selezione delle IA prevedono i seguenti passaggi:
- ❖ Raccolta delle informazioni tecniche sui sistemi IA individuati con particolare attenzione agli aspetti di
  - ➢ Spiegabilità e logica adottata
  - ➢ Funzionalità
  - ➢ Trasparenza
  - ➢ Limiti
  - ➢ Gestibilità dei bias
  - ➢ Conservazione dei dati da parte del produttore
  - ➢ Comunicazione e diffusione dei dati
  - ➢ Possibilità di intervento di cancellazione, accesso, modifica dei dati

- ❖ Effettuazione da parte del Gruppo di lavoro per l'IA della
  - ➢ Valutazione dei rischi
  - ➢ DPIA
  - ➢ Eventualmente della FRIA

- ❖ Eventuale modifica dei piani di gestione incidente, gestione dei BIAS, gestione di emergenze
- ❖ Acquisizione dei sistemi di IA ove previsto, con la partecipazione di DSGA
- ❖ Registrazione della IA adottata nel Registro delle Intelligenze artificiali
- ❖ Formazione, informazione e addestramento ai soggetti interessati all'utilizzo delle IA

12.2.2 Riesame dei requisiti relativi alle AI individuate

- Le piattaforme individuate siano conformi con gli obblighi cogenti, in particolare che siano rispettose dei dettati del Reg. UE 2016/679 (GDPR)
- La localizzazione geografica nello spazio UE dei server o la presenza di decisioni di adeguatezza o altre garanzie nella protezione dei dati personali, in conformità con il GDPR
- L'assenza, ovvero la possibilità di disattivazione di funzioni di profilazione o pubblicità
- I requisiti delle piattaforme AI siano coerenti siano correttamente definiti compresi quelli eventualmente non documentati
- Non ci siano divergenze tra i requisiti richiesti e quelli offerti, sia esplicitamente che in maniera implicita
- I fornitori forniscano adeguata documentazione sia in merito alle proprie garanzie di affidabilità generali (es. certificazioni ISO 27001, ISO 42001, NIST altre certificazioni) che in merito ai prodotti individuati (trasparenza, spiegabilità, possibilità di controllo e revisione del prodotto, ecc.)

12.2.3 Gestione delle modifiche nella IA

Qualora sia necessario procedere alla modifica ai sistemi, ai modelli e alle componenti di IA utilizzati dall'Istituto Scolastico, le modifiche stesse sono attuate secondo la linea di indirizzo della procedura **Pr 5 Gestione del controllo delle modifiche alle IA**

12.3 Utilizzo delle AI

L'istituzione scolastica persegue l'integrazione dell'Intelligenza Artificiale (IA) secondo un approccio organico e sistemico, volto a potenziare sia la qualità dell'offerta formativa sia l'efficienza dei processi gestionali. Tale iniziativa si fonda sul principio della centralità della persona e sul rigoroso rispetto dei parametri etici e normativi vigenti, con l'obiettivo di migliorare l'inclusione e i servizi destinati all'intera comunità scolastica.

In sintesi, l'adozione dell'IA si articola lungo le seguenti direttrici fondamentali:

12.3.1 Formazione e didattica

- Sviluppo di competenze e personalizzazione didattica: l'istituto intende dotare gli studenti di competenze digitali avanzate e promuovere un pensiero critico consapevole verso l'impatto tecnologico. L'IA viene impiegata per personalizzare l'apprendimento, adattando metodologie e ritmi alle specificità dei singoli alunni, e per garantire il successo formativo di studenti con Bisogni Educativi Speciali (BES), disturbi dell'apprendimento o fragilità linguistiche.
- Supporto alla Creatività e Progettazione: L'IA viene utilizzata come catalizzatore per il problem solving e la produzione di contenuti in contesti laboratoriali.
- Docenti e organi collegiali si avvalgono di strumenti per la progettazione didattica assistita e la valutazione (es. creazione di rubriche e analisi degli esiti), fermo restando che ogni decisione valutativa e ogni validazione dei materiali rimangono di esclusiva pertinenza del docente.
- È tassativamente vietato a docenti o studenti inserire in strumenti di IA dati personali, relazioni riservate, PEI, PDP o informazioni personali o sensibili.
- In caso di utilizzo di strumenti IA per un elaborato, l'alunno è tenuto a dichiarare l'uso effettuato (es. supporto linguistico, generazione di idee). L'uso non dichiarato o improprio dell'IA sarà considerato scorretto ai fini della valutazione.

12.3.2 Didattica e innovazione

L'IA potrà essere impiegata come:

- supporto alla progettazione di lezioni, materiali o verifiche;
- strumento di assistenza linguistica, traduzione o sintesi vocale;
- mezzo per generare esempi, mappe concettuali o spiegazioni;
- ausilio per attività laboratoriali e interdisciplinari;
- risorsa inclusiva per alunni con DSA o bisogni educativi speciali.

Tutte le attività dovranno essere sotto la guida del docente e non potranno sostituire il processo di apprendimento personale dello studente.

12.3.3 Valutazione e autenticità

La valutazione dovrà sempre riflettere l'impegno, la comprensione e la capacità critica dell'alunno. Se l'alunno utilizza strumenti di IA per realizzare un elaborato, è necessario che dichiari l'uso effettuato (es. supporto linguistico, generazione di idee, rielaborazione del testo). L'uso non dichiarato o improprio dell'IA sarà considerato scorretto ai fini della valutazione.

12.3.4 Educazione civica e consapevolezza digitale

L'uso dell'IA sarà integrato nel curricolo di Educazione civica e nel curricolo Digitale, con percorsi che aiutino gli studenti a:

- comprendere come funziona un sistema di IA e quali limiti possiede;
- riconoscere fake news, manipolazioni digitali o contenuti generati artificialmente;
- riflettere sull'etica dell'informazione e della tecnologia;
- sviluppare un pensiero critico verso l'automazione e i suoi effetti sociali

12.3.5 Attività organizzativa e amministrativa

- Efficienza Amministrativa e Organizzativa: Sul fronte gestionale, l'IA è finalizzata alla semplificazione dei carichi burocratici e all'automazione di compiti ripetitivi, quali la redazione di bozze documentali, la classificazione degli atti e l'ottimizzazione degli orari. Questo permette di liberare risorse temporali da dedicare ad attività di maggior rilievo educativo e relazionale.
- Analisi dei Dati e Comunicazione: L'istituto sfrutta sistemi AI per il monitoraggio della frequenza e degli esiti scolastici, facilitando una pianificazione informata attraverso documenti strategici come il RAV e il PDM. Inoltre, l'IA potenzia l'accessibilità e la rapidità della comunicazione tra scuola e territorio.

12.3.6 Governance e sicurezza

- Ogni utilizzo delle applicazioni IA è progettato nel rispetto del GDPR, delle linee guida del Ministero dell'Istruzione e del Merito (MIM) e delle indicazioni del Garante Privacy. Viene garantita la tracciabilità delle operazioni e una costante supervisione umana, assicurando che il personale competente possa intervenire e correggere in ogni momento le proposte generate dai sistemi.

12.4 Coinvolgimento degli studenti e delle famiglie

Studenti e famiglie sono coinvolti secondo le seguenti modalità:

- Libere consultazioni sia durante i momenti didattici che attraverso le attività svolte nei consigli di classe e/o Istituto
- Incontri mirati con i Rappresentanti di studenti e delle famiglie sui rischi connessi all'uso dell'IA, in un'ottica di corresponsabilità educativa, anche in considerazione di possibili bias o discriminazioni
- Attività informative attraverso circolari, informative e newsletter sui siti internet istituzionali e tramite comunicazioni dirette
- Formazione degli studenti nelle attività didattiche curriculari ed extracurriculari, trasversale rispetto alle specifiche discipline, con particolare riguardo all'accrescimento della consapevolezza, al governo delle allucinazioni e dei bias dei sistemi AI, al rispetto della persona in tutte le sue declinazioni

Le comunicazioni, il materiale informativo e formativo, le circolari e ogni altro materiale tramesso o messo a disposizione degli studenti e delle famiglie, viene registrato e conservato per documentare le attività svolte in tal senso.

12.5 Coinvolgimento degli organi collegiali, dei docenti e del personale ATA

Il Collegio dei docenti delibera gli indirizzi pedagogici e didattici relativi all'uso dell'IA, nella progettazione curricolare ed extracurricolare e valuta gli esiti delle attività che coinvolgono le IA. I docenti, gli addetti amministrativi ed il personale tutto, nel rispetto dei singoli ruoli, viene coinvolto secondo le seguenti modalità:

- Momenti di confronto e dibattito nelle riunioni assembleari e negli incontri specifici dedicati
- Partecipazione a momenti formativi generali e specifici sia rispetto alle competenze digitali trasversali sia riguardo agli specifici strumenti IA utilizzati
- Distribuzione di materiale informativo
- Incremento della consapevolezza attraverso l'analisi di incidenti, bias rilevati, altre non conformità a rispetto ai risultati attesi

12.6 Valutazione e autenticità

La valutazione deve sempre riflettere l'impegno, la comprensione e la capacità critica dell'alunno. In caso di utilizzo di strumenti IA per un elaborato, l'alunno è tenuto a dichiarare l'uso effettuato (es. supporto linguistico, generazione di idee). L'uso non dichiarato o improprio dell'IA sarà considerato scorretto ai fini della valutazione.

13 Preparazione e risposta alle emergenze

L'uso dell'intelligenza artificiale può generare diverse situazioni di emergenza e rischi significativi. Questi scenari non riguardano solo malfunzionamenti tecnici, ma anche conseguenze etiche e di sicurezza, con potenziali impatti sulla vita umana, con particolare riferimento ad un settore sensibile quale la scuola.

13.1 Scenari di emergenza nell'uso delle IA

Le emergenze possono essere raggruppate nelle seguenti categorie principali:

- Malfunzionamenti e guasti tecnici:
  - Guasti hardware o software: Errori imprevisti nei sistemi fisici o nel codice dell'IA possono portare all'arresto improvviso di operazioni critiche.
  - Comportamenti imprevisti (emergenti): I sistemi di IA complessi possono sviluppare comportamenti non programmati o non previsti durante l'uso, che possono portare a decisioni errate o promuovere azioni pericolose da parte degli utilizzatori.

- Problemi di sicurezza e attacchi informatici:
  - Violazioni della sicurezza dei dati: I sistemi di intelligenza artificiale gestiscono spesso enormi quantità di dati sensibili. Una violazione può esporre informazioni private degli utilizzatori, dati riservati relativi alle persone e alle attività didattiche, dati personali afferenti alla sfera privata dei lavoratori o dati finanziari o relativi alle retribuzioni, con gravi conseguenze per la privacy e la sicurezza personale.
  - Attacchi malevoli: L'IA può essere sfruttata per lanciare attacchi informatici più sofisticati e su larga scala (es. malware/ransomware potenziati dall'IA), oppure gli stessi sistemi di IA possono essere presi di mira con attacchi di data poisoning o prompt injection per comprometterne il funzionamento. In questo tipo di attacco, gli aggressori inseriscono dati errati nel set di dati utilizzato per addestrare l'IA. Questi dati corrotti possono modificare le funzionalità dell'IA e creare scelte o previsioni errate. È quindi possibile aggiungere al set di dati nuovi punti dati errati o modificati, rendendo impossibile il corretto apprendimento del processo di IA. Sebbene l'impatto del avvelenamento dei dati possa sembrare sottile, può essere pericoloso e sabotare gradualmente le prestazioni del modello di un sistema di IA.
  - Data Breach e Privacy: La fuga di dati sensibili usati per l'addestramento o l'accesso non autorizzato a modelli che gestiscono dati personali
  - Inversione del modello: Qualsiasi attacco di inversione del modello cerca di recuperare i dati di addestramento utilizzati per creare un'IA. Gli aggressori possono estrarre informazioni sui dati di addestramento semplicemente interrogando ripetutamente il modello ed esaminandone i risultati. Ciò costituisce una grave minaccia alla privacy, soprattutto se l'IA è stata addestrata su informazioni private. L'inversione del modello può comportare la fuga di informazioni o di dati di specifici utenti individuali.
  - Attacco backdoor; questo attacco consiste nell'incorporare backdoor dannose nei modelli di IA durante la fase di addestramento. Tali backdoor vengono attivate da input particolari, che possono causare un comportamento non intenzionale del modello. Ad esempio, un sistema di riconoscimento delle immagini con backdoor potrebbe classificare le immagini in modo errato se al loro interno sono presenti determinati modelli. A volte

sono molto difficili da individuare poiché, nella maggior parte dei casi, il modello si comporta normalmente.
  - Ingegneria sociale potenziata dall'IA; in questo modo gli aggressori utilizzano l'IA per creare attacchi di ingegneria sociale altamente efficaci e personalizzati. I sistemi AI possono creare contenuti testuali, vocali o persino video realistici per convincere i bersagli.

- Conseguenze etiche e sociali:
  - Pregiudizi (bias) algoritmici e discriminazione: I modelli di IA sono spesso addestrati su dati che possono riflettere pregiudizi esistenti nella società. In situazioni critiche (es. nella valutazione dei lavori svolti dagli studenti, nella selezione del personale), ciò può portare a decisioni ingiuste o discriminatorie.
  - Perdita di controllo e dipendenza: Un'eccessiva dipendenza dall'IA per il pensiero critico e la risoluzione dei problemi potrebbe portare a una perdita di competenze umane fondamentali. In caso di fallimento dell'IA, gli operatori potrebbero non essere in grado di intervenire efficacemente.
  - Deepfake, Disinformazione e manipolazione: L'IA generativa può essere utilizzata per creare disinformazione realistica e su vasta scala, potenziando la manipolazione dell'opinione degli studenti e degli utilizzatori con particolare riferimento ai soggetti che hanno minor capacità di analisi critica.

- Emergenze in applicazioni specifiche:
  - Attività di laboratorio con indicazioni di formulazioni errate o indicazioni di sperimentazioni pericolose
  - Output errati nella gestione del personale con errori in assegnazione compiti e orari
  - Allucinazioni Critiche: l'AI può generare dati falsi ma estremamente convincenti, portando a risposte errate o fallimenti strutturali

- Altre conseguenze legali:
  - I sistemi di intelligenza artificiale generativa spesso utilizzano grandi quantità di dati, compreso materiale protetto da copyright, per addestrare i loro modelli. Ciò può portare alla riproduzione involontaria di contenuti protetti, violando potenzialmente i diritti di proprietà intellettuale. Inoltre, la generazione di nuovi contenuti che somigliano molto alle opere esistenti può sollevare controversie legali sulla proprietà e sull'originalità.

13.2 Prevenzione e analisi degli scenari di emergenza nell'uso delle IA

Il Gruppo di lavoro per l'IA monitora costantemente i sistemi implementati per prevenire l'insorgenza di tali situazioni emergenziali o correggere le deviazioni.

Inoltre consulta e approfondisce costantemente le linee guida sulla sicurezza, quali quelle presenti sul portale ufficiale dell'AI Act dell'Unione Europea o monitorando i report sulla sicurezza informatica del Computer Emergency Response Team (CERT-AGID) e dell'ACN Agenzia Nazionale per la Cybersicurezza.
Il Gruppo di lavoro per l'IA promuove le seguenti strategie di sicurezza per la prevenzione di incidenti e emergenze nell'uso dei sistemi IA:

1. Convalida dei dati
Le attività con i sistemi IA deve sempre implementare una convalida completa dei dati per identificare e filtrare i dati dannosi o corrotti.
I dati di input devono sempre essere anonimizzati o puliti da tutti i dati personali e da tutti i dati correlabili a dati personali, anche estrapolabili dall'incrocio di più dati, in modo che possano essere inseriti nel sistema di IA.
È necessario garantire frequenti controlli e l'integrità dei set di dati utilizzati per addestrare e testare i modelli di IA. Tali misure possono proteggere dagli attacchi di avvelenamento dei dati e ridurre al minimo il rischio di pregiudizi involontari nei sistemi di IA.

2. Migliorare la sicurezza dei modelli
Le organizzazioni dovrebbero utilizzare tecniche come l'anonimizzazione irreversibile dei dati di addestramento, pur mantenendone la funzionalità, in modo da consentire comunque prestazioni accurate del modello, ma rendendo più difficile per un aggressore estrarre informazioni su un singolo individuo. (ad esempio creando orari scolastici per "docente 1, docente 2…."

3. Controlli di accesso rigorosi
L'Istituto, attraverso il Gruppo di lavoro per l'IA e l'Animatore digitale, deve stabilire livelli di autenticazione e autorizzazione per ogni componente all'interno del sistema di IA, sia esso studente, insegnante, addetto amministrativo. Inoltre, devono essere abilitate l'autenticazione a più fattori per l'utilizzo del modello di IA e per l'accesso ai dati di addestramento.
Deve essere costantemente applicato il principio dei privilegi minimi in modo che gli utenti ottengano solo le autorizzazioni strettamente necessarie.

4. I dati di LOG degli accessi devono essere monitorati e conservati per un periodo congruo, almeno 6 mesi per gli Amministratori di sistema, il Gruppo di lavoro per l'IA e l'Animatore digitale, al fine di prevenire accessi ai settaggi e usi illeciti nei sistemi stessi.

5. Il Gruppo di lavoro per l'IA deve condurre regolarmente valutazioni di sicurezza dei sistemi di IA per determinare se esistono vulnerabilità. La sicurezza del sistema dovrebbe essere valutata utilizzando strumenti automatizzati oppure con test di penetrazione manuali. L'Animatore digitale deve mantenere aggiornati e patchati tutti i componenti deli sistemi di IA per proteggersi dalle vulnerabilità note.

13.3 Gestione delle emergenze

Il Gruppo di lavoro per l'IA e l'Animatore digitale devono essere periodicamente addestrati sugli scenari emergenziali e criticità elencate o emergenti e svolgere simulazioni e prove relativamente all'applicazione di quanto previsto nelle istruzioni/procedure stesse, coinvolgendo le eventuali parti interessate.

Nel caso in cui si verifichi il mancato rispetto di prescrizioni, anche legali, e/o difformità rispetto ai risultati attesi nell'uso delle IA, oppure si siano verificati incidenti o emergenze, il Responsabile del Gruppo di lavoro per l'IA ne ordina la sospensione dell'utilizzo fino alla risoluzione della criticità.

La **Pr 3 gestione incidenti e data breach** è periodicamente riesaminata (e, se necessario, aggiornata) sia dopo che si sono verificate eventuali situazioni di emergenza o incidenti, sia in sede di riesame da parte del Gruppo di lavoro per l'IA e Animatore digitale per valutare gli eventuali miglioramenti apportabili.
Tale procedura si applica anche in caso di incidenti informatici rilevanti o che possono incidere sul Perimetro di cybersicurezza nazionale come individuato dalla Direttiva NIS2 e per le evenienza di data breach come indicato dal GDPR.

Sia l'addestramento che le simulazioni e prove sono registrate come addestramenti nello specifico **modulo addestramento e prove di emergenza**

14 Valutazione delle prestazioni

14.1 Monitoraggio, misurazione, analisi e valutazione

Come riportato in Procedura **Pr_04 Gestione Non Conformità, Azioni Correttive, incidenti e miglioramento continuo**, L'Istituto descrive le modalità per attuare i processi di monitoraggio, misurazione, analisi e miglioramento necessarie a:

- assicurare la conformità del Sistema di gestione dell'Intelligenza Artificiale a quanto pianificato
- migliorare in modo continuo l'efficacia e l'efficienza del Sistema di Gestione dell'AI
- dimostrare la conformità alle prescrizioni legali

14.2 Sorveglianza e misurazione prestazioni relative all'uso delle AI

Il Gruppo di lavoro per l'IA e l'Animatore digitale, in collaborazione con il DPO quando individuato hanno il compito di monitorare e registrare:

- La rilevazione degli incidenti o emergenze nell'uso delle IA;
- I tempi di risoluzione degli incidenti o emergenze;
- Il difetti (Bug) rilevati nei sistemi IA utilizzati e/o sviluppati;
- Le segnalazioni, reclami o richieste di accesso privacy pertinenti la sicurezza delle IA;

Tali registrazioni sono mantenute nel **Registro Non conformità, Incidenti e Data breach**.

14.2.1Analisi e valutazione

L'Istituto gestisce i dati derivanti dalle attività di monitoraggio e registrazione incidenti, emergenze ed eventi per evidenziare l'efficienza e l'efficacia del Sistema di gestione dell'Intelligenza Artificiale e definire i relativi piani di miglioramento.
Il Responsabile del Gruppo di lavoro per l'IA ha il compito di raccogliere i dati e le registrazioni e mantenere aggiornato il **Registro Non conformità, Incidenti e Data breach**.

Il Responsabile del Gruppo di lavoro per l'IA, dopo avere raccolto le registrazioni e le informazioni relative alla sorveglianza, si accerta che le non conformità siano state risolte o gestite e relaziona la Dirigenza scolastica circa i risultati ottenuti.

I risultati delle misurazioni sono analizzati dal Consiglio di Istituto, al fine di individuare le necessarie azioni da intraprendere, nel caso le criticità siano recidive o non risolvibili direttamente dal Gruppo di lavoro per l'IA.

14.3 Audit interni

Il Responsabile del Gruppo di lavoro per l'IA, in collaborazione con l'Animatore digitale e il DPO pianifica audit periodici con i criteri e le modalità descritte nella procedura **Pr_04 Gestione Non Conformità, Azioni Correttive, incidenti e miglioramento continuo**, al fine di valutare e controllare che il Sistema di Gestione della IA:

- Sia conforme a quanto pianificato ed ai requisiti delle normative di riferimento
- Sia efficacemente attuato e mantenuto
- Sia efficace per il conseguimento degli indirizzi del Dirigente scolastico e del Consiglio di Istituto
- Fornisca informazioni per il riesame da parte del Consiglio di Istituto

Il Responsabile del Gruppo di lavoro per l'IA pianifica gli audit, ne organizza la conduzione, la gestione e la conservazione dei risultati derivati dagli audit stessi.

Il Gruppo di lavoro per l'IA deve adottare misure per la chiusura delle Non Conformità rilevate e identificare eventuali Azioni Correttive necessarie per l'eliminazione e/o riduzione delle loro cause.
Gli esiti delle azioni correttive approvate e realizzate, saranno controllati per verificarne e valutarne l'efficacia.

14.4 Riesame della Dirigenza

14.4.1Generalità

Il PIA ha durata triennale, in coerenza con il PTOF, ma deve essere verificato ed eventualmente aggiornato annualmente per adeguarsi:

- all'evoluzione normativa e tecnologica,
- all'introduzione di nuovi strumenti o pratiche,
- ai risultati emersi dal monitoraggio interno.

Il Sistema di gestione dell'Intelligenza Artificiale è quindi riesaminato dal Consiglio dell'Istituto in collaborazione il Gruppo di lavoro per l'IA almeno una volta l'anno.

14.5 Non conformità e azioni correttive

Le Azioni Correttive si basano sulla valutazione delle cause che stanno all'origine interna e/o esterna delle Non Conformità e sono finalizzate ad impedire il loro ripetersi.

Per determinare quali siano le Azioni Correttive da porre in atto, le fasi da seguire sono:

- identificare le cause delle Non Conformità, che l'analisi delle stesse ha evidenziato come importanti
- definire e valutare le azioni da promuovere
- programmare i tempi necessari per svolgere l'azione concordata
- eseguire l'Azione Correttiva
- verificare il buon esito e l'efficacia dell'azione

14.5.1Investigazione degli incidenti

Ogni incidente o situazione di emergenza sarà adeguatamente registrato ed analizzato al fine di identificarne le cause.
A tale scopo l'organizzazione ha implementato una procedura di investigazione degli incidenti **Pr_04 Gestione Non Conformità, Azioni Correttive, incidenti e miglioramento continuo**, al fine di registrare, investigare ed analizzare tempestivamente gli incidenti per:

- Determinare le eventuali carenze del SGIA ed i fattori che possono aver causato o contribuito alla causa dell'incidente
- Identificare la necessità di azioni correttive
- Identificare opportunità per il miglioramento
- Comunicare il risultato di tali investigazioni

15 Documenti collegati

Segue l'elenco dei documenti collegati che il Dirigente scolastico e il Gruppo di Lavoro, con la collaborazione del DPO, elaboreranno per la promozione dell'AI Literacy tra docenti, studenti e famiglie e una corretta attuazione dell'IA nella scuola:

- Regolamento d'Istituto per l'uso dell'IA
- Modulo Elenco documenti
- Registro delle Intelligenze artificiali - Elenco aggiornato delle piattaforme e strumenti autorizzati
- Registro trattamenti ai sensi Art. 30 GDPR
- Registro Non conformità, Incidenti e Data breach
- Modulo richiesta revisione
- DPIA
- FRIA
- Linea guida per studenti e docenti per l'Intelligenza artificiale Informativa sul trattamento dati
- Informativa famiglie
- Informativa interessati
- Informativa semplificata
- Decalogo
- Pr 1 Procedura gestione documenti
- Pr 2 Procedura valutazione del rischio
- Pr 3 gestione incidenti e data breach
- Pr 4 Gestione Non Conformità, Azioni Correttive, incidenti e miglioramento continuo
- Modulo addestramento e prove di emergenza
- Organigramma
- Funzionigramma
- Scheda analisi incidente/modulo azione correttiva
- Scheda per introduzione nuova AI
- Atto di nomina per il Referente per l'IA
- Atto di nomina per il Gruppo di lavoro per l'IA

Condiviso e approvato dal Collegio dei Docenti il 27 marzo 2026 e dal Consiglio di Istituto il 27 marzo 2026