Ministero dell'Istruzione e del Merito

Ufficio Scolastico Regionale per il Lazio

"ISTITUTO COMPRENSIVO 2 - via BARBARANELLI"

Via F. Barbaranelli, 3/3-a - 00053 CIVITAVECCHIA (RM) Tel. 0766.472023

Cod.Fisc. 91038390588 - Cod.Mecc. RMIC8GN009 – www.iccivitavecchia2.edu.it

E-mail: rmic8gn009@istruzione.it – Pec: rmic8gn009@pec.istruzione.it

REGOLAMENTO SULL'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

Il presente regolamento disciplina l'uso dell'Intelligenza Artificiale (IA) all'interno dell'istituzione scolastica, garantendo un utilizzo etico, sicuro e conforme alle normative vigenti. L'uso degli strumenti di IA da parte dei docenti deve rispettare le normative vigenti e le disposizioni della scuola per la protezione dei dati personali. La responsabilità del contenuto dei documenti prodotti con tale strumento resta in capo alla persona fisica che l'ha utilizzato per crearli. L'uso degli strumenti di IA deve tenere conto dei limiti contrattuali relativi all'età degli studenti, stabiliti dai fornitori di IA e dalle norme vigenti. La scelta degli strumenti di IA deve essere coerente con le previsioni del PTOF in merito all'adozione di materiali didattici e non deve comportare costi aggiuntivi per gli studenti e le famiglie, salvo che non siano approvati secondo procedure condivise.

DEFINIZIONI

Per una comprensione condivisa dei termini utilizzati nel presente documento:

- **Intelligenza Artificiale (IA)**: insieme di tecnologie e algoritmi che consentono a sistemi informatici di svolgere compiti che normalmente richiederebbero l'intervento umano, come

analizzare dati, generare testo, riconoscere immagini, o fornire suggerimenti. Nel contesto scolastico, possono trovare applicazione principalmente l'IA generativa e l'IA predittiva.

- **IA Generativa**: sistemi di IA in grado di generare nuovi contenuti (testo, immagini, codice, ecc.) sulla base di prompt forniti dall'utente. Esempi: ChatGPT (Open AI), Google Gemini, MS Copilot, Claude (Anthropic), Grok, Deep Seek, NotebookLM, ecc..

- **Strumenti di IA**: software, piattaforme e applicazioni basate su modelli di IA, incluse le tecnologie di apprendimento automatico (machine learning), i modelli linguistici (Large Language Models, LLM) e i sistemi di generazione di contenuti multimediali.

- **Deployer**: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.

- **Dati personali**: Qualsiasi informazione relativa a una persona identificata o identificabile (nome, cognome, numero di telefono, indirizzo email, account digitali, dati contabili, assenze, permessi, retribuzioni, risultati scolastici, esigenze educative speciali, immagini sotto forma di fotografie e filmati video, registrazioni vocali, ecc.). Nel contesto della scuola, i dati personali richiedono protezione particolare perché spesso riguardano minori.

- **Dati appartenenti alle particolari categorie**: dati personali di cui all'articolo 9, paragrafo 1, del Regolamento (UE) 2016/679 riguardanti: le origini, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, lo stato di salute, la vita sessuale o l'orientamento sessuale di una persona, cui si aggiungono i dati genetici e i dati biometrici.

- **Anonimizzazione**: processo di trasformazione irreversibile dei dati personali in dati anonimi, rendendo impossibile la re-identificazione dell'individuo, anche attraverso mezzi legali e tecnologicamente ragionevoli, per cui i dati anonimi non sono più soggetti al GDPR e possono essere trattati liberamente, a differenza della pseudonimizzazione.

- **Pseudonimizzazione:** trattamento di dati personali in modo che i dati personali non possano essere più attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuibili a una persona fisica identificata o identificabile. La pseudonimizzazione è un processo reversibile e comporta la conservazione separata delle chiavi di re-identificazione. Esempio: sostituire il nome reale con un nome fittizio in un testo dove non è possibile risalire all'identità vera.

- **Bias (distorsione)**: errori sistematici negli algoritmi di IA che portano a risultati discriminatori o ingiusti. Esempio: un'IA addestrata con dati storici distorti potrebbe perpetuare discriminazioni basate su genere o provenienza geografica.

- **Prompt**: l'input testuale che un utente fornisce a un sistema di IA generativa per ottenere una risposta.

- **Chatbot:** Software che simula ed elabora le conversazioni umane, consentendo agli utenti di interagire con i dispositivi digitali

- **Dati di addestramento:** i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere;

- **Privacy by design**: Principio secondo cui la protezione dei dati deve essere considerata fin dalla fase di progettazione di un sistema, non aggiunta dopo.

- **GDPR (General Data Protection Regulation)**: Regolamento europeo sulla protezione dei dati personali che stabilisce come i dati devono essere trattati, con particolare attenzione ai dati dei minori.

AMBITO DI APPLICAZIONE

Il regolamento si applica a tutto il personale docente e non docente, agli studenti e alle famiglie, nell'ambito delle attività didattiche e amministrative della scuola.

PROTEZIONE DEI DATI PERSONALI

Prima di introdurre qualunque nuovo strumento di IA, la Scuola verificherà:

— la conformità al GDPR;

— la sede dei server e le garanzie di protezione dei dati;

— la specificità d'uso per la Scuola e l'istruzione (preferenza per licenze Education);

— l'assenza di funzioni di profilazione o pubblicità o di altre funzioni ultronee eccessive e non pertinenti con i compiti istituzionali di istruzione e di formazione prorie dell'Istituzione scolastica.

Nessun docente dovrà inserire su strumenti di IA dati personali, relazioni riservate, PEI, PDP o, in generale, dati personali appartenenti alle particolari categorie (ex sensibili) di cui all'art.9 del GDPR.

Il personale scolastico non docente non dovrà inserire su strumenti di IA dati personali, atti amministrativi riservati o, in generale, dati personali appartenenti alle particolari categorie (ex sensibili) di cui all'art.9 del GDPR.

STRUMENTI AUTORIZZATI E MODALITÀ D'USO

La scuola manterrà un elenco aggiornato delle piattaforme e applicazioni IA autorizzate. Ogni nuovo strumento sarà valutato in base a tre criteri: 1. Utilità didattica; 2. Sicurezza e conformità alla normativa privacy; 3. Facilità d'uso e accessibilità.

INDIVIDUAZIONE DEI SISTEMI DI IA NON AMMESSI

L'AI Act impone agli utilizzatori (Scuole) di valutare il rischio connesso all'uso dei sistemi di IA, adottando misure proporzionate al livello di rischio. La Scuola ha valutato di escludere preferenzialmente (o estrema limitazione) anche i sistemi ad Alto rischio, in considerazione della vulnerabilità dei soggetti coinvolti.

1. **Sistemi a Rischio Inaccettabile (VIETATI)**

In ottemperanza all'AI Act (Art. 5), l'Istituzione vieta categoricamente l'uso di sistemi che costituiscono una chiara minaccia ai diritti fondamentali. Divieto assoluto, quindi, di utilizzare sistemi di riconoscimento biometrico emotivo negli ambienti educativi e lavorativi, sistemi di social scoring (attribuzione di punteggi di affidabilità basati sul comportamento sociale/scolastico) ed, in generale, sistemi che impiegano tecniche subliminali o manipolative.

2. **Sistemi ad Alto Rischio (OBBLIGHI STRINGENTI E LIMITAZIONI)**

La Scuola adotta una politica di tolleranza zero o estrema limitazione per i sistemi di IA classificati come Alto Rischio dall'AI Act, data la vulnerabilità dei soggetti (minori) e la centralità dei diritti fondamentali nell'ambito educativo. I sistemi di IA considerati ad Alto Rischio sono quelli che influenzano significativamente la vita e la carriera educativa degli studenti, come definiti dall'AI Act (es. sistemi per l'ammissione, la valutazione predittiva con conseguenze dirette, il monitoraggio dei comportamenti durante le prove).

Pertanto l'Istituzione Scolastica esclude preferenzialmente l'adozione di sistemi di IA ad Alto Rischio. L'eventuale adozione sarà valutata solo in casi di comprovata necessità e beneficio non ottenibile con soluzioni a rischio inferiore, mentre esclude in modo assoluto:

- i sistemi di IA impiegati per prendere decisioni finali o sommative relative alla promozione, non ammissione o assegnazione di voti finali degli studenti. L'IA può fungere solo da strumento di supporto e analisi per il docente.
- sistemi di IA che generano profilazioni comportamentali o cognitive invasive degli studenti per scopi diversi dal supporto immediato all'apprendimento individualizzato, e che potrebbero portare a stigmatizzazione o discriminazione

UTILIZZO DELLA IA DA PARTE DEI DOCENTI

I docenti possono utilizzare strumenti di IA per i seguenti fini:

- Supporto per la preparazione delle lezioni e materiali didattici integrativi (es. riassunti, schemi, quiz, dispense ed esercizi);
- personalizzare percorsi di apprendimento in base alle esigenze degli alunni, creare esercizi e attività di verifica;
- Pianificazione pedagogica e progettazione didattica a livello di gruppo-classe
- Supporto alla correzione di elaborati, senza mai sostituire la valutazione del docente
- Automazione di compiti amministrativi che non richiedono trattamento di dati personali oltretutto di particolari categorie
- sviluppare rubriche di valutazione e criteri di feedback;
- effettuare ricerche e analisi di dati per migliorare le proprie pratiche didattiche

Ai docenti non è consentito l'utilizzo dell'IA al fine di automatizzare interamente le correzioni delle verifiche senza supervisione umana e che:

- non tiene conto dei limiti contrattuali relativi all'età degli studenti, stabiliti dai fornitori di IA e dalle norme vigenti
- comporta costi aggiuntivi per gli studenti e le famiglie, salvo approvazione secondo procedure condivise

È responsabilità del docente verificare sempre l'accuratezza, la pertinenza e l'affidabilità dei risultati generati dall'IA prima di utilizzarla in classe o condividerla con gli alunni.

I docenti sono incoraggiati a introdurre gli alunni ai concetti base dell'IA, alle sue potenzialità e ai suoi limiti, promuovendo un approccio critico e consapevole. L'utilizzo di IA non deve compromettere l'originalità dei lavori degli alunni né violare i diritti di proprietà intellettuale. I docenti devono educare gli alunni alla citazione appropriata delle fonti, inclusi i contributi derivanti dall'IA.

A scopo esemplificativo nella tabella seguente vengono descritte sinteticamente le principali operazioni da evitare in modo assoluto e le operazioni più comuni che i docenti sono autorizzati a svolgere attraverso i sistemi di IA generativa:

COSA SI PUOI FARE (SÌ ☑)	**COSA NON SI DEVE FARE (NO ✖)**
Generazione di bozze per piani di lezione, unità didattiche, presentazioni e materiali didattici personalizzati	Inserire dati ex sensibili o di particolari categorie degli studenti (salute, valutazioni psicologiche) in strumenti IA
Creazione automatica di test ed esercizi personalizzati su specifici argomenti	Inserire dati personali degli studenti (nomi, voti, elaborati, valutazioni) in strumenti IA
Redazione di email, bozze di relazioni, o riassunti di riunioni	Inserire relazioni riservate, PEI, PDP
Supporto organizzativo nella gestione di materiali o nella pianificazione delle attività didattiche	Utilizzare sistemi di IA per classificare gli studenti o determinarne l'accesso a specifici percorsi formativi
Utilizzo di strumenti IA per generare griglie di valutazione	Utilizzare strumenti di IA per correzioni automatizzate senza supervisione

Guidare gli studenti nell'attività di ricerca su temi di studio in attività di gruppo	Non utilizzare il proprio account scolastico per applicazioni di IA non autorizzate dalla Scuola

UTILIZZO DELLA IA DA PARTE DEGLI STUDENTI

In attesa di un quadro normativo e di indirizzi operativi più definiti a livello nazionale ed europeo, e in considerazione delle specifiche esigenze didattiche, formative ed etiche, la Scuola adotta un principio di cautela riguardo l'uso dell'Intelligenza Artificiale (IA) da parte degli studenti: in particolare l'utilizzo di strumenti e applicazioni basate sull'IA generativa (come chatbot, text-to-image, o software di riassunto/creazione automatica di contenuti) è vietato agli studenti durante le attività didattiche, le verifiche e per la produzione di compiti o elaborati da presentare a scuola. Tale divieto è motivato dalla necessità di:

- garantire l'autenticità e l'originalità del lavoro degli studenti, tutelando la valutazione del percorso di apprendimento;
- prevenire il rischio di plagio e di mancato sviluppo delle competenze critiche e di scrittura autonoma;
- tutelare la riservatezza dei dati personali e scolastici.

Gli studenti possono utilizzare strumenti di IA per i seguenti fini:

- Chiedere approfondimenti e spiegazioni su argomenti di studio
- Generare esercizi e quiz per auto-verificarsi
- Farsi aiutare nel metodo di studio (creare mappe concettuali, schemi, riassunti)
- Esercitarsi nel problem-solving ricevendo feedback immediato
- Imparare a usare l'IA in modo consapevole e critico

Agli studenti non è consentito:

- Copiare integralmente risposte generate da IA per compiti e verifiche
- Immettere dati personali propri o di compagni in sistemi IA (es. cognomi, indirizzi, informazioni familiari)

- Usare servizi IA non approvati dalla scuola con l'account scolastico
- Usare servizi di IA per evitare il ragionamento e lo studio personale

Gli studenti si dovranno attenere scrupolosamente alle seguenti disposizioni:

- Lo studente deve verificare sempre le risposte consultando il docente o fonti affidabili
- L'IA è uno strumento per imparare meglio, non per non studiare
- Se il docente chiede di non usare IA per un compito specifico, rispettare questa indicazione

Limitazioni di età per l'uso dell'IA

- L'accesso agli strumenti di IA deve rispettare le limitazioni di età imposte dai fornitori dei servizi di IA e dalle linee guida ministeriali
- Gli strumenti di IA devono essere dotati di sistemi di "age gate" così da escludere dal servizio gli under 13 e i minorenni che non abbiano avuto il consenso dei genitori (Provv. Garante per la protezione dei dati n.114/2023 e n.755/2024)

Plagio, originalità e dichiarazione d'uso dell'IA

- Gli studenti devono dichiarare esplicitamente se e come hanno utilizzato strumenti di IA nei propri lavori scolastici
- L'uso dell'IA senza dichiarazione è considerato plagio e può comportare provvedimenti disciplinari
- I docenti devono fornire criteri chiari per distinguere un uso legittimo da un uso scorretto dell'IA

Responsabilità degli studenti e delle famiglie

- Gli studenti sono responsabili di qualsiasi contenuto prodotto con strumenti di IA
- I genitori sono responsabili per l'uso dell'IA da parte dei figli al di fuori dell'ambito scolastico e devono essere coinvolti nella formazione sull'uso consapevole dell'IA

A scopo esemplificativo nella tabella seguente vengono descritte sinteticamente le principali operazioni da evitare in modo assoluto e le operazioni più comuni che sono consentite agli studenti nell'impiego di strumenti di IA:

COSA SI PUOI FARE (SÌ ☑)	COSA NON SI DEVE FARE (NO ✖)
Generare riassunti, schemi, mappe concettuali o chiedere spiegazioni semplificate di argomenti difficili (verificando sempre le fonti)	Incollare nomi, cognomi o codici fiscali ed altri dati personali propri o di compagni (es. cognomi, indirizzi, informazioni familiari)
Creare quiz, test di autovalutazione o simulare interrogazioni per prepararsi alle verifiche	Generare automaticamente compiti, tesine o svolgere esercizi che dovrebbero attestare le competenze personali dello studente
Generare contenuti come presentazioni a scopo didattico	Utilizzare il proprio account scolastico per applicazioni di IA non autorizzate dalla Scuola

UTILIZZO DELLA IA PER IL PERSONALE ATA E PER ATTI ISTITUZIONALI

L'uso di strumenti di IA per attività istituzionali e di produzione di atti e documenti deve rispettare le norme in vigore e le disposizioni della scuola per la protezione dei dati, a tutela della sicurezza dei dati e della struttura informatica. La responsabilità del contenuto dei documenti prodotti con l'utilizzo di strumenti di IA resta in capo alla persona fisica che ha utilizzato l'IA per crearli. Il personale ATA è tenuto a garantire la massima riservatezza e sicurezza dei dati trattati tramite strumenti di IA, attenendosi scrupolosamente alle normative sulla privacy (GDPR) e alle politiche interne dell'Istituto. Non devono essere utilizzati strumenti di IA non autorizzati o non conformi ed in tali strumenti non devono essere inseriti dati personali, soprattutto se appartenenti a particolari categorie (ex sensibili).

Attività suggerite:

- Automazione di compiti ripetitivi: gestione calendari, organizzazione documenti e altre attività amministrative di routine.
- Analisi di dati: elaborazione di statistiche su presenze, efficienza energetica e altri aspetti della gestione scolastica.
- Redazione di bozze: preparazione di comunicazioni interne o circolari da verificare e finalizzare.

- Gestione documentale: organizzazione, archiviazione e recupero efficiente dei documenti scolastici.

Il risultato generato dall'IA deve essere sempre verificato e validato dal personale ATA prima della sua diffusione o utilizzo ufficiale.

Attività consentite

In particolare al personale amministrativo è consentito utilizzare strumenti di IA per i seguenti fini:

- Supporto alla produzione di atti e documenti o parte di essi, nel rispetto delle norme vigenti e delle disposizioni scolastiche in materia di privacy, sicurezza ed, in particolar modo, nel rispetto delle misure di sicurezza tecniche ed organizzative che scaturiscono dalla valutazione dei rischi connessi all'utilizzo dei particolari sistemi

- Migliorare i processi organizzativi

L'IA non può essere impiegata per decisioni automatizzate che abbiano conseguenze dirette sugli alunni o sul personale, senza supervisione umana.

La responsabilità del contenuto dei documenti prodotti con l'IA rimane sempre in capo alla persona.

La responsabilità delle decisioni resta in capo alle persone fisiche anche quando si siano avvalse del supporto dell'IA.

DIVIETI ASSOLUTI

Le seguenti operazioni sono vietate per tutto il personale:

- Immissione di dati appartenenti a categorie particolari (ex sensibili). I dati particolari includono: informazioni su disabilità, disturbi dell'apprendimento, origini etniche, condizioni di salute, situazioni familiari, dati biometrici, dati sulle convinzioni religiose o filosofiche, opinioni politiche, l'appartenenza sindacale, vita sessuale o orientamento sessuale.

- Profilazione automatica di studenti attraverso sistemi IA che potrebbero portare a discriminazione o alla creazione di "profili di rischio" basati su caratteristiche personali

- Sentiment analysis (analisi del sentimento) su testi riguardanti studenti, anche anonimizzati, senza valutazione etica preventiva (vietato dalla normativa UE sull'IA)

- È vietato l'uso dell'IA per la sorveglianza degli studenti o per la raccolta di dati sensibili senza autorizzazione

A scopo esemplificativo nella tabella seguente vengono descritte sinteticamente le principali operazioni da evitare in modo assoluto e le operazioni più comuni che il personale è autorizzato a svolgere attraverso i sistemi di IA, in particolare quella generativa:

COSA SI PUOI FARE (SÌ ☑)	**COSA NON SI DEVE FARE (NO ✖)**
Chiedere una bozza di lettera per convocare una riunione generica	Incollare nomi, cognomi o codici fiscali di dipendenti o fornitori nei prompt
Creare bozze di circolari, note, verbali, email formali e avvisi per il personale e le famiglie	Utilizzare l'IA per elaborare o riassumere documenti interni, documenti riservati o informazioni non ancora pubbliche, caricandoli su piattaforme esterne
Far riassumere una normativa ministeriale o una circolare	Caricare verbali di procedimenti disciplinari o note di demerito
Tradurre comunicazioni standard per le famiglie (es. istruzioni iscrizioni)	Inserire dati bancari (IBAN) o dettagli relativi a pagamenti/stipendi
Creare materiali di supporto organizzativo (es. moduli e tabelle orarie)	Inserire dati relativi a situazioni familiari o che descrivono particolari situazioni a Scuola che hanno coinvolto l'interessato
Usufruire del supporto alla stesura di documenti per bandi, gare, acquisti	Inserire dati personali di qualunque soggetto con cui la Scuola entra in relazione per adempiere gli obblighi legali e per perseguire interessi pubblici

Ottimizzare testi per il sito web della scuola	Caricare file PDF contenenti tabelle con dati identificativi

PRIVACY E SICUREZZA DATI

La protezione dei dati personali rappresenta una priorità assoluta nell'utilizzo dell'Intelligenza Artificiale in ambito scolastico.

Ogni utilizzo di strumenti di IA deve essere pienamente conforme al Regolamento Generale sulla Protezione dei Dati (GDPR - Reg. UE 2016/679) e alla normativa nazionale vigente. È vietato inserire dati personali, di particolari categorie o relativi a vicende giudiziarie degli alunni, del personale o di terzi in strumenti di IA, che dovranno essere preventivamente autorizzati dall'Istituto e sottoposti ad una valutazione d'impatto sulla protezione dei dati (DPIA), se necessario. L'Istituto privilegerà l'adozione di strumenti di IA che garantiscano elevati standard di sicurezza, protezione dei dati e conformità alle normative sulla privacy, possibilmente con server localizzati all'interno dell'UE. Non dovranno essere inseriti dati personali di terzi in strumenti di IA approvati dall'Istituto scolastico e, a tale scopo, qualunque informazione personale riferita a persona fisica dovrà essere omessa ed i dati identificativi dovranno essere resi anonimi, per minimizzare i rischi legati alla protezione dei dati.

Misure di sicurezza obbligatorie per la protezione dei dati personali ad opera degli utenti e degli amministratori

- Utilizzare le versioni "Enterprise" o "Team" delle AI che offrono garanzie contrattuali sul fatto che i dati non verranno utilizzati per l'addestramento del modello. Ad es. Gemini for Education e NotebookLM sono assistenti AI con protezione dei dati di livello enterprise . ciò significa che quando utilizzano i loro account Workspace for Education, gli utenti dispongono di una protezione dei dati di livello enterprise.
- ANONIMIZZAZIONE Rimozione o mascheratura delle informazioni personali quando non necessarie in modo da rendere anonime le raccolte di informazioni nei prompt e nei contenuti trasmessi al fine di ottenere prompt di risposta pertinenti alle richieste. Ad esempio sostituire i dati anagrafici con un segnaposto (es. "Dipendente A", "Fornitore X", "Società Alfa", "Alunno_01"), eliminazione di ogni riferimento a date di nascita o situazioni familiari

specifiche ed utilizzo della forma [OMISSIS]" per evitare di fornire ulteriori informazioni personali.

- CIFRATURA DEI DATI E DEI DOCUMENTI Soluzioni atte a rendere incomprensibili i dati acceduti all'interno dei contenuti creati e trasmessi, tranne ai soli autorizzati che possiedono la chiave di decifratura – Ciò può essere fatto ad esempio sceglindo applicazioni che utilizzano la crittografia end-to-end per proteggere le informazioni trasmesse.

- PSEUDONIMIZZAZIONE dei dati personali prima di inserirli in sistemi di IA: sostituzione dei nomi reali con codici.

- MINIMIZAZIONE DEI DATI: Inserire solo le informazioni strettamente necessarie per l'attività richiesta. Evitare di incollare documenti competi nella loro versione originale, interi contratti o database.

- UTILIZZO DI PASSWORD FORTI (mediante sistemi di password manager professionali) e attivazione dell'autenticazione a due fattori su tutti gli account e gli strumenti di IA utilizzati. Implementare strumenti di verifica automatica degli accessi che avvisano quando qualcuno accede al sistema da dispositivi o luoghi non autorizzati.

- LIMITAZIONE DEGLI ACCESSI attraverso l'attivazione di permessi specifici nelle impostazioni di privacy in modo da consentire solo determinate attività di trattamento ai soggetti con cui si condivide un documento.

- MONITORAGGIO DELLE AUTORIZZAZIONI CONCESSE ALLE APPLICAZIONI DI AI SUI DISPOSITIVI UTILIZZATI e controlli granulari che permettono di vedere esattamente quali dati sono stati condivisi e con chi.

- CONTROLLI PERIODICI e accurati finalizzati alla verifica preliminare delle impostazioni di privacy e di sicurezza delle Applicazioni di IA: in particolare va verificato che sia stata disattivata qualunque funzionalità di condivisione esterna.

- VERIFICA della disabilitazione della funzione di addestramento del modello. Questa opzione impedisce che le conversazioni dell'utente vengano usate per migliorare l'IA.

- VERIFICA DELLE POLICY DEL FORNITORE: Controllare se l'azienda di intelligenza artificiale (fornitore del servzio di IA) garantisce la residenza dei dati nell'UE e non trasferisce dati extra-UE.

- VERIFICA DEI TEMPI DI CONSERVAZIONE Verificare tramite gli amministratori delle piattaforme di IA che i dati personali nei prompt e nelle risposte siano mantenuti solo per il periodo strettamente necessario agli scopi di lavoro o di studio controllando costantemente tra le impostazioni della piattaforma di IA che sia sempre attiva la funzione di non conservazione dei dati derivanti dalle interazioni al termine di ciascuna sessione e che sia sempre possibile per l'utente eliminare manualmente i contenuti all'interno delle Applicazioni.

- MONITORAGGIO ED AGGIORNAMENTO Monitoragio continuo e update dei sistemi di IA al Mantenere sempre aggiornati sistemi operativi, browser e applicazioni per correggere le vulnerabilità note.
- CONTROLLO ACCESSI ACCOUNT Controllare regolarmente l'attività degli account e dei sistemi per identificare tempestivamente eventuali anomalie o attività sospette.

- BACKUP DEI DATI per garantire integrità e sicurezza - avere a disposizione una copia dei dati, conservata in un luogo sicuro è ciò che permette in caso di attacco informatico (associato anche all'utilizzo di strumenti di IA che quindi fanno aumentare il cyber risk) di non cedere ai ricatti e ripristinare il proprio sistema piuttosto celermente.

- SICUREZZA DELLE POSTAZIONI Mettere in sicurezza le postazioni di lavoro, attraverso logout automatici, update degli OS e dei software di protezione antivirus e antimalware e limitare a priori gli utilizzi degli strumenti di lavoro per fini personali.

- SICUREZZA DEI DISPOSITIVI Mettere in sicurezza i dispositivi in dotazione per l'attività lavorativa, soprattutto quelli mobili, per cui va posta cautela nell'impostazione delle misure di sincronizzazione, incoraggiando tecniche di codifica per file o cartelle specifiche, accessibili quindi mediante procedure di autenticazione definite o attivabili in caso di furto e/o perdita del bene di proprietà della Scuola.

- SISTEMI DI RILEVAZIONE ANOMALIE Configurazione di alert automatici per monitorare l'uso anomalo dell'IA a Scuola: picchi improvvisi di utilizzo, accessi fuori orario, condivisione di file di grandi dimensioni.

IPOTESI DI SPERIMENTAZIONE E PROSPETTIVE FUTURE

Riconoscendo il potenziale dell'IA come strumento didattico innovativo e la necessità di preparare gli studenti a un mondo sempre più tecnologico, la scuola intende adottare un approccio progressivo e controllato:

Avvio Sperimentale: a partire dal prossimo Anno Scolastico è ipotizzata l'attivazione di una fase di sperimentazione didattica controllata e limitata all'uso di strumenti di IA.

Obiettivi della Sperimentazione:

- Valutare l'efficacia didattica e l'impatto etico dell'IA in contesti educativi specifici.
- Sviluppare modelli di IA Literacy (alfabetizzazione sull'IA) per insegnare agli studenti il funzionamento, i limiti, i rischi e l'uso responsabile di tali tecnologie.
- Definire le Linee Guida Interne per un uso sicuro, etico e conforme alla normativa, in particolare riguardo alla data protection (GDPR) e al rispetto del diritto d'autore.

Condizioni: L'eventuale uso futuro sarà sempre subordinato a:

- Valutazione preliminare delle necessità e dei bisogni specifici nei vari ambiti di utilizzo (didattica e amministrazione);
- Scelta del fornitore del servizio di IA adeguato, sulla base dell'affidabilità e della capacità di garantire la conformità alla normativa privacy vigente (in particolar modo Regolamento UE 2016/679 o GDPR e Codice Privacy D.lgs.196/03 novellato dal D.lgs.101/18);
- Predilizione di strumenti approvati dal Ministero dell'Istruzione o integrati in Google Workspace for Education, che offrono garanzie specifiche per il contesto scolastico e rispettano gli standard di protezione dei minori;
- Coinvolgimento del DS, del team digitale, del DPO e dei referenti per l'IA indivviduati tra i docenti ed il personale amministrativo, in un apposito Gruppo di lavoro per l'IA, ai fini della valutazione della conformità dell'applicazione di IA ai principi del PTOF ed alla normativa vigente in materia (privacy, sicurezza, etica, utilità pedagogica) e per la sua approvazione ed autorizzazione;
- Valutazione d'impatto sulla protezione dei dati personali (DPIA ai sensi dell'art.35 del GDPR) e, per i sistemi ad alto rischio, anche l'esecuzione della FRIA (art.27 del AI Act);
- Approvazione ed autorizzare degli strumenti di IA da parte del Consiglio di Istituto;
- Diffusione di informazioni chiare e trasparenti sulle attività previste (ogni sistema di AI adottato deve essere comprensibile nei suoi processi decisionali) ed in particolare sui trattamenti di dati personali ad esse connessi agli interessati;
- Adozione delle misure di mitigazione dei rischi per la protezione dei dati personali;
- Istruzioni e linee guida operative per l'uso corretto degli strumenti di IA soprattutto in relazione ai relativi trattamenti di dati personali per la tutela dei diritti dei soggetti interessati;

- ❖ Progettazione e programmazione della formazione continua - Per garantire un uso consapevole dell'AI, è essenziale investire nella formazione di docenti, studenti e personale amministrativo;
- ❖ Sensibilizzazione di studenti e famiglie per l'uso consapevole degli strumenti di IA autorizzati.
- ❖ Supervisione umana - Ogni decisione che riguarda studenti e processi didattici deve restare sotto il controllo umano. L'IA può automatizzare operazioni ripetitive, ma non deve mai sostituire la valutazione del docente.

CONCLUSIONI

Il presente Regolamento sarà oggetto di revisione periodica da parte del Dirigente Scolastico, in collaborazione con il Collegio Docenti e il Consiglio d'Istituto, per adattarsi all'evoluzione tecnologica, normativa e alle esigenze della comunità scolastica.

RIFERIMENTI NORMATIVI E QUADRO ETICO

Il Regolamento in oggetto si basa sui principi e sulle direttive nazionali ed europee in materia di IA ed è stato elaborato in conformità alle seguenti norme, regolamenti e linee guida:

- Linee Guida del Ministero dell'Istruzione e del Merito per l'introduzione dell'Intelligenza Artificiale nelle istituzioni scolastiche (DM 166/2025).
- Regolamento (UE) 2024/1689 (AI Act), in particolare per quanto concerne gli obblighi per i Deployer (utilizzatori) di sistemi di IA: la scuola è consapevole del Regolamento sull'Intelligenza Artificiale (c.d. AI Act) approvato dall'Unione Europea, il quale mira a garantire che l'IA sia sicura, trasparente, etica, non discriminatoria e rispettosa dei diritti fondamentali. L'attuale cautela si allinea all'approccio europeo basato sul rischio, ponendo l'attenzione sugli impatti etici e sociali degli strumenti di IA.
- Regolamento (UE) 2016/679 (GDPR), Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
- Codice in materia di protezione dei dati personali (D.lgs.196/03 e s.m. e i. novellato dal D.lgs.101/18) e Normativa Italiana (Provvedimenti e Linee guida del Garante e Leggi e decreti legislativi con riflessi in materia di protezione dei dati personali): si tiene conto delle indicazioni del Garante per la Protezione dei Dati Personali relative alla necessità di garantire

la piena trasparenza nell'utilizzo di sistemi di IA e di tutelare i minori, in particolare per quanto concerne l'accesso e l'uso dei dati.

- Linee guida generali (incluse linee guida, raccomandazioni e buone pratiche) per chiarire la legge e promuovere una comprensione comune delle normative UE sulla protezione dei dati.
- Deontologia Professionale Docente: i docenti sono tenuti al rispetto dei principi di correttezza e diligenza, monitorando l'uso etico e responsabile di ogni tecnologia, come previsto dal Codice di Comportamento dei dipendenti pubblici e dalle direttive ministeriali sull'educazione civica digitale.