



ISTITUTO OMNICOMPRESIVO
"Città Sant'Angelo"
CITTA' SANT'ANGELO - PE



PNRR Missione 4 Istruzione e Ricerca - Componente 1 – Potenziamento dell'offerta dei servizi di istruzione: dagli asili nido alle Università - Investimento 2.1: Didattica digitale integrata e formazione alla transizione digitale per il personale scolastico.

D.M. 66/2023 - Formazione del personale scolastico per la transizione digitale

Cybersicurezza ed utilizzo sicuro e consapevole del web (ID 362189)

Esperto: **Prof. Ugo Donatelli** – *Formatore AICA Scuola 4.0/DigCompEdu*
Tutor: **Prof.ssa Anna Onesti**

Elaborato finale corsisti: Regolamento sull'utilizzo dell'Intelligenza Artificiale



Regolamento sull'utilizzo dell'Intelligenza Artificiale nell'Istituto Omnicomprensivo Città Sant'Angelo



La Commissione europea ha riconosciuto il significativo potenziale dell'Intelligenza Artificiale (IA) per migliorare le nostre società, evidenziando come essa possa incrementare l'efficienza dei processi, stimolare l'innovazione e la ricerca, promuovere diritti fondamentali quali la libertà di espressione, l'accesso all'informazione e l'assistenza sanitaria, oltre a favorire importanti interessi pubblici come la sicurezza e la sanità pubblica. Tuttavia, la Commissione ha anche messo in guardia sui rischi derivanti dall'utilizzo dell'IA senza adeguate garanzie e controlli di qualità, sottolineando come ciò possa portare alla violazione dei diritti delle persone su larga scala, con difficoltà di prevenzione o rilevamento in assenza di trasparenza o consapevolezza del suo utilizzo. In linea con l'IA Act, pubblicato in Gazzetta nel 2024 e a regime nel 2026, che per la legislazione italiana prevede due articoli già in vigore da settembre 2024 (art. 2 e art. 5), e considerando le indicazioni della legge sul procedimento amministrativo e del codice dell'amministrazione digitale sull'utilizzo di strumenti informatici per l'efficienza della pubblica amministrazione, nonché le Linee Guida di AgID per l'adozione, l'acquisto e lo sviluppo di sistemi di IA nella Pubblica Amministrazione, l'Istituto Omnicomprensivo riconosce la necessità di regolamentare l'utilizzo dell'intelligenza artificiale, a partire da una Valutazione d'impatto della protezione dei dati (DPIA) nei vari contesti, con particolare attenzione alla presenza di minori. La cautela deve essere la parola chiave a tutti i livelli nell'utilizzo dell'IA nel contesto dell'istruzione.

Legenda degli Attori e Termini Tecnici

- **Sistema di IA:** sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali [i, 20].
- **Deployer:** persona fisica o giuridica (in questo contesto, la scuola o il docente che agisce sotto l'autorità della scuola) 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 [i, 21].
- **Fornitore:** persona fisica o giuridica che sviluppa un sistema di IA e lo immette sul mercato o lo mette in servizio sotto il proprio nome o marchio [i, 21].
- **Sistema di IA ad alto rischio:** sistema di IA classificato come tale ai sensi dell'art. 6 dell'AI ACT e dell'allegato III [i, 22]. In ambito scolastico rientrano in questa categoria i sistemi di IA utilizzati in particolare per:
 - Determinare l'accesso o l'ammissione agli istituti o ai programmi di istruzione e formazione professionale a tutti i livelli [i, 22].
 - Assegnare persone agli istituti o ai programmi di istruzione e formazione professionale a tutti i livelli [i, 22].
 - Valutare i risultati dell'apprendimento delle persone [i, 23].
 - Valutare il livello di istruzione adeguato per una persona e influenzare materialmente il livello di istruzione e formazione che le persone riceveranno o a cui potranno avere accesso [i, 23].
 - Monitorare e rilevare comportamenti vietati degli studenti durante le prove [i, 23].
- **Sistema di IA non ad alto rischio:** qualsiasi sistema di IA che non rientra nella definizione di sistema di IA ad alto rischio [i, 23].
- **Alfabetizzazione in materia di IA:** le competenze, le conoscenze e la comprensione che consentono ai *deployer* e alle persone interessate di procedere a una diffusione informata dei sistemi

di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare [i, 24].

- **Funzione dei log in ottica GDPR:** i log, che sono registrazioni cronologiche degli eventi che avvengono all'interno di un sistema informatico, assumono un'importanza cruciale per diversi aspetti legati al GDPR.

L'Istituto Omnicomprensivo definisce inoltre il termine di **apprendenti** inteso come personale docente e non docente, gli studenti e i genitori.

REGOLAMENTO

ARTICOLO 1: DEFINIZIONI, OBIETTIVI E ORIENTAMENTO STRATEGICO ALL'USO DELL'IA IN AMBIENTE SCOLASTICO

Definizioni

Si rimanda alle definizioni fornite nella sezione "Legenda degli attori e termini tecnici".

Obiettivi

L'Istituto Omnicomprensivo, attraverso l'integrazione dell'IA e del presente Regolamento nel Piano Triennale dell'Offerta Formativa (PTOF), si propone di:

- Migliorare l'efficienza delle operazioni amministrative.
- Supportare la gestione dei dati e la comunicazione con studenti e genitori.
- Automatizzare attività ripetitive (es. gestione delle email, programmazione degli appuntamenti).
- Analizzare i dati per migliorare i processi decisionali.
- Supportare la creazione di report e documenti.
- Garantire la protezione delle informazioni sensibili secondo le normative sulla privacy, utilizzando strumenti di IA che rispettino le linee guida sulla protezione dei dati.
- Offrire formazione al personale sull'uso degli strumenti di IA e creare un canale di supporto tecnico.
- Stabilire indicatori di performance per valutare l'efficacia dell'IA e raccogliere feedback per il miglioramento continuo.
- Utilizzare l'IA in modo etico, evitando discriminazioni e garantendo l'equità.
- Assumere la responsabilità per le decisioni prese con l'ausilio dell'IA.
- Sviluppare le competenze cognitive e non cognitive degli studenti, l'orientamento e la capacità di attivare le risorse per la loro autonomia, responsabilità e protagonismo.
- Valorizzare il personale scolastico, mettendolo nelle condizioni di fare autoformazione/ricerca affinché l'IA diventi strumento culturale.
- Promuovere un uso sicuro, responsabile e consapevole degli strumenti digitali e delle tecnologie legate all'IA tra personale, studenti e genitori.
- Sicurezza dei Dati: i log permettono di monitorare gli accessi ai dati personali, rilevare attività sospette o non autorizzate e tracciare potenziali violazioni di sicurezza (data breach). In caso di incidente, i log sono fondamentali per capire cosa è successo, quali dati sono stati compromessi e come intervenire.
- Responsabilità (Accountability): l'articolo 5(2) del GDPR introduce il principio di accountability, che richiede al titolare del trattamento di dimostrare la conformità al regolamento. I log rappresentano una prova concreta delle misure di sicurezza tecniche e organizzative adottate per proteggere i dati personali. Essi possono dimostrare chi ha fatto cosa, quando e perché, contribuendo a dimostrare la diligenza del titolare.
- Data Protection by Design e by Default: un'efficace gestione dei log supporta l'implementazione dei principi di "protezione dei dati fin dalla progettazione" e "protezione

dei dati per impostazione predefinita" (articolo 25 GDPR). Analizzando i log, è possibile identificare e correggere eventuali debolezze nei sistemi che potrebbero compromettere la protezione dei dati.

- Gestione degli Incidenti: in caso di *data breach* (articolo 33 GDPR), i log sono essenziali per ricostruire l'accaduto, valutare la portata della violazione e adempiere all'obbligo di notifica all'autorità di controllo e, in alcuni casi, agli interessati.
- Audit e Conformità: i log facilitano le attività di audit interni ed esterni, consentendo di verificare la conformità dei trattamenti di dati personali alle disposizioni del GDPR e alle policy aziendali.

Orientamento strategico

L'utilizzo dell'IA nell'Istituto Omnicomprensivo è orientato alle seguenti linee guida:

- Creatività digitale: supportare gli studenti nello sviluppo della scrittura creativa, offrire suggerimenti di revisione, personalizzare progetti, generare opere d'arte e musica, creare tutorial interattivi.
- Intelligenza emotiva: aiutare gli studenti a riconoscere le emozioni, sviluppare l'empatia e migliorare le abilità relazionali.
- Apprendimento personalizzato: adattare l'apprendimento alle esigenze specifiche, monitorare il progresso, supportare l'autovalutazione e migliorare la gestione del lavoro.
- Apprendimento delle lingue: migliorare la pronuncia, l'ascolto e la scrittura, effettuare traduzioni, simulare conversazioni e contesti culturali.
- Collaborazione interculturale, interreligiosa: agevolare la collaborazione in contesti internazionali e creare ambienti virtuali multilingue.
- Simulazioni educative: esplorare diverse discipline attraverso simulazioni realistiche e promuovere l'apprendimento basato su giochi.
- Etica dell'IA: esaminare le questioni etiche legate all'IA, sviluppare una comprensione critica delle implicazioni etiche e sensibilizzare alle sfide emergenti.
- Analisi dei dati: insegnare a raccogliere, elaborare e interpretare dati, creare modelli predittivi e identificare fonti attendibili.
- Programmazione e codifica: apprendere i fondamenti della programmazione, creare algoritmi, sviluppare progetti e il pensiero computazionale.
- Accoglienza ed inclusione: personalizzare l'apprendimento attraverso l'analisi del livello di competenza, l'adattamento dei contenuti, il feedback immediato e la variazione dei formati.
- Tutoraggio virtuale: fornire supporto personalizzato in qualsiasi momento, spiegare concetti difficili, generare esercizi su misura e suggerire risorse.
- Feedback dettagliato: analizzare gli elaborati, evidenziare punti di forza e debolezza, fornire spiegazioni e suggerimenti per il miglioramento.
- Supporto nella risoluzione di problemi: offrire assistenza immediata, spiegazioni dettagliate e suggerimenti per superare gli ostacoli.
- Apprendimento autodiretto: fornire risorse su argomenti di interesse personale e generare esercizi personalizzati per promuovere l'autonomia.
- Miglioramento dell'accessibilità: tradurre contenuti, fornire spiegazioni in diverse lingue, convertire testo in audio e adattare i materiali per studenti con diverse esigenze.
- Adattamento dinamico: regolare il livello di sfida e il supporto in base alle risposte e al comportamento di apprendimento degli studenti.

ARTICOLO 2: INTELLIGENZA ARTIFICIALE E FORMAZIONE OBBLIGATORIA

Cosa possono fare Docenti, Studenti, Genitori e Amministrazione Scolastica se adeguatamente formati:

- Docenti:

- Utilizzare strumenti di IA per preparare lezioni personalizzate, creare materiali didattici differenziati.
- Impiegare l'IA per fornire feedback dettagliato e supporto personalizzato agli studenti.
- Utilizzare l'IA come tutor virtuale per rispondere alle domande degli studenti e spiegare concetti.
- Integrare l'IA per simulazioni educative e attività di apprendimento interattive.
- Utilizzare l'IA per l'analisi dei dati relativi alla classe al fine di individuare aree di miglioramento e studenti a rischio.
- Promuovere l'alfabetizzazione in materia di IA tra gli studenti, sensibilizzandoli sui rischi e le opportunità.
- Supervisionare l'uso dell'IA da parte degli studenti in classe.
- Richiedere agli studenti di dichiarare esplicitamente l'uso dell'IA nei loro elaborati.
- Essere consapevoli della gamma di informazioni raccolte dagli strumenti di IA utilizzati.
- Monitorare l'utilizzo periodicamente conservando la documentazione dei processi.

- Studenti:

- Utilizzare l'IA come assistente virtuale per comprendere argomenti complessi e ottenere supporto per il brainstorming.
- Chiedere feedback sull'apprendimento e sul lavoro svolto.
- Utilizzare strumenti di IA approvati dall'istituto sotto la supervisione del docente.
- Citare sempre l'uso dell'IA nei propri elaborati.
- Essere trasparenti e divulgare le fonti del lavoro svolto con l'IA.
- Rivedere e verificare sempre le risposte fornite dall'IA.
- Modificare l'output dell'IA in modo che rifletta le proprie conoscenze.
- Monitorare l'utilizzo periodicamente conservando la documentazione dei processi.

- Genitori:

- Dotare i propri figli minorenni di dispositivi con accesso monitorato e controllato (parental control).
- Far partecipare i propri figli a corsi di formazione se previsti dal PTOF e regolamentati dall'Istituto ponendo i propri figli in situazioni di sicurezza e consapevolezza.
- Conoscere il Regolamento e partecipare ad eventi informativi e formativi.
- Firmare il Patto di Corresponsabilità, conoscere il Regolamento ed impegnarsi affinché il proprio figlio/a lo conosca nei dettagli.

- Amministrazione Scolastica:

- Utilizzare l'IA per migliorare l'efficienza delle operazioni amministrative, la gestione dei dati e la comunicazione.
- Automatizzare attività ripetitive e analizzare dati per migliorare i processi decisionali.
- Assicurare la protezione dei dati personali e la sicurezza informatica.
- Organizzare corsi di formazione sull'uso responsabile dell'IA per docenti, studenti e genitori.
- Fornire materiali informativi sull'IA e sensibilizzare sui rischi e le opportunità.
- Stabilire indicatori di performance per valutare l'efficacia dell'IA e raccogliere feedback.
- Assicurare che la scelta degli strumenti di IA sia coerente con il PTOF e non comporti costi aggiuntivi non approvati per studenti e famiglie.
- Definire modalità di utilizzo specifiche dell'IA per studenti con bisogni educativi speciali.
- Monitorare l'utilizzo periodicamente conservando la documentazione dei processi da parte di tutti gli apprendenti dell'Istituto.

- Gestire i log in conformità al GDPR. La gestione dei log in ottica GDPR richiede l'adozione di specifiche misure e principi:
 - *Minimizzazione dei dati*: i log devono contenere solo i dati strettamente necessari per le finalità previste (sicurezza, audit, gestione incidenti). È importante evitare la registrazione di dati personali non pertinenti o eccessivi. Ad esempio, se non necessario, si potrebbe evitare di registrare interi indirizzi IP o nomi utente completi.
 - *Integrità e immutabilità*: i log devono essere protetti da alterazioni o cancellazioni non autorizzate. Devono essere implementati meccanismi per garantirne l'integrità e la provenienza (ad esempio, timestamping sicuro, firma digitale).
 - *Conservazione limitata*: i log devono essere conservati per un periodo di tempo adeguato alle finalità per cui sono raccolti e in linea con le policy di retention aziendali, che devono essere conformi al principio di limitazione della conservazione (articolo 5(1)(e) GDPR). Non esiste un periodo di conservazione unico stabilito dal GDPR, ma è necessario definire periodi specifici in base alle esigenze e ai rischi. Il Garante per la Privacy italiano suggerisce un periodo minimo di conservazione di 60 giorni per alcuni tipi di log.
 - *Accesso ristretto*: l'accesso ai log contenenti dati personali deve essere limitato al personale specificamente autorizzato e per scopi legittimi (es. amministratori di sistema, responsabili della sicurezza). Ogni accesso dovrebbe essere tracciato.
 - *Sicurezza*: i log devono essere archiviati in modo sicuro per proteggerli da accessi non autorizzati, perdita o distruzione. Possono essere necessarie misure come la cifratura e controlli di accesso fisici e logici.
 - *Anonimizzazione e pseudonimizzazione*: ove possibile e appropriato, si dovrebbero considerare tecniche di anonimizzazione o pseudonimizzazione dei dati presenti nei log per ridurre i rischi per la privacy degli interessati.
 - *Policy di gestione dei log*: è fondamentale definire e implementare policy interne chiare e dettagliate per la raccolta, la conservazione, l'accesso, l'analisi e la cancellazione dei log, in conformità con i principi del GDPR.
 - *Trasparenza e informazione*: gli interessati devono essere informati (tramite l'informativa privacy) sul trattamento dei dati personali eventualmente presenti nei log e sulle finalità di tale trattamento.
 - *Audit log degli accessi*: è buona prassi tenere traccia degli accessi ai log stessi, per monitorare chi ha consultato le informazioni e quando.

Cosa è espressamente vietato a Docenti, Studenti, Genitori e Amministrazione Scolastica:

- Docenti:

- Utilizzare sistemi di IA vietati ai sensi dell'Articolo 5 dell'AI Act, come quelli che utilizzano tecniche subliminali manipolative, sfruttano vulnerabilità, effettuano scoring sociale, valutazioni del rischio predittive unicamente sulla profilazione, creano banche dati di riconoscimento facciale tramite scraping non mirato, o inferiscono emozioni sul luogo di lavoro e negli istituti di istruzione (salvo motivi medici o di sicurezza).
- Imporre costi aggiuntivi per l'uso di strumenti di IA senza procedure condivise.
- Delegare completamente all'IA la responsabilità delle valutazioni o delle decisioni didattiche.

- Studenti:

- Utilizzare l'IA senza il permesso dell'insegnante.
- Completare interamente verifiche o compiti a casa con l'IA senza un contributo originale.
- Non rivedere e verificare le risposte dell'IA, accettandole acriticamente.
- Non dichiarare l'uso dell'IA nei propri elaborati (plagio).
- Condividere le proprie credenziali di accesso agli strumenti di IA.
- Inserire dati personali sensibili negli strumenti di IA.
- Utilizzare strumenti di IA non approvati dall'istituto.

- Genitori:

- Dotare i propri figli minorenni di dispositivi con accesso libero alla rete.
- Non far partecipare i propri figli a corsi di formazione se previsti dal PTOF e regolamentati dall'Istituto ponendo i propri figli in situazioni di pregiudizio e di rischio.
- Non conoscere il Regolamento e assumere atteggiamenti di rifiuto non adeguatamente motivato.
- Non firmare il Patto di Corresponsabilità e il Regolamento per Presa Visione.

- Amministrazione Scolastica:

- Utilizzare sistemi di IA vietati ai sensi dell'Articolo 5 dell'AI Act.
- Immettere sul mercato, mettere in servizio o usare sistemi di IA ad alto rischio senza aver effettuato le necessarie valutazioni di conformità e adottato le misure di mitigazione del rischio previste dall'AI Act.
- Non garantire la formazione adeguata del personale sull'uso dell'IA.

ARTICOLO 3: RESPONSABILITÀ GENITORIALI SULL'USO IMPROPRIO DELL'IA

I genitori sono tenuti a vigilare sull'utilizzo degli strumenti di IA da parte dei propri figli al di fuori dell'ambiente scolastico. Devono firmare un'autorizzazione scritta per consentire l'uso degli strumenti di IA e per la privacy relativa alla protezione dei dati, dichiarando di essere informati sui rischi connessi e sulla informativa privacy. Qualora i prodotti generati dagli studenti al di fuori della supervisione scolastica risultino in violazione di norme legali o regolamentari, i genitori saranno considerati co-responsabili. La scuola si impegna a favorire il coinvolgimento dei genitori nell'educazione dei loro figli sull'utilizzo etico dell'IA attraverso incontri informativi, fornitura di materiali esplicativi ed esempi pratici. È importante sensibilizzare i genitori sull'educazione digitale, sull'importanza di proteggere le informazioni personali online, sull'uso di strumenti di controllo parentale e sulla partecipazione dei genitori a corsi di formazione dedicati, organizzati anche dalla scuola.

ARTICOLO 4: IMPEGNI PER IL PIANO DI FORMAZIONE ANNUALE

L'Istituto Omnicomprensivo riconosce che la possibilità di utilizzare e gestire l'IA è strettamente legata alla formazione del personale. L'uso improvvisato o superficiale dell'IA è vietato. Pertanto, l'Istituto organizzerà periodicamente corsi di formazione per docenti, studenti e genitori sull'uso responsabile dell'IA. La formazione è fondamentale per gestire i rischi, controllare il funzionamento degli strumenti di IA e avere l'ultima parola su ogni decisione. Il personale formato dovrà essere consapevole di cosa sta facendo, in un rapporto costante tra essere umano e macchina. L'alfabetizzazione in materia di IA è essenziale per consentire una diffusione informata e consapevole dei rischi e delle opportunità. L'autoformazione in Collegio, la condivisione delle scelte in Consiglio e la formazione nelle classi sono elementi chiave di questo processo. Pertanto nel Piano formazione del PTOF, i docenti e il Personale ATA parteciperanno a corsi di formazione annuale.

ARTICOLO 5: RISVOLTI ETICI E ATTENZIONE AL COMPORTAMENTO DEL PERSONALE

L'utilizzo dell'IA comporta importanti risvolti etici che devono essere attentamente considerati. È fondamentale analizzare e comprendere i potenziali rischi associati ai processi decisionali automatizzati, con particolare attenzione a elementi come equità, pregiudizio, discriminazione e responsabilità. La scuola si impegna a sviluppare una comprensione critica delle implicazioni etiche delle tecnologie intelligenti, affrontando temi come il bias algoritmico, la privacy e la responsabilità nell'uso dell'IA. Saranno promosse attività di generazione di scenari etici, analisi di casi studio e feedback etico personalizzato per sensibilizzare gli apprendenti alle sfide etiche emergenti legate all'automazione del lavoro, all'uso dei dati personali e alla discriminazione algoritmica. Ogni apprendente, in qualità di studente, deve essere consapevole dei limiti dell'IA, intesa come

impossibilità di una completa sostituzione dell'interazione umana e priorità di rivolgersi a un insegnante per aiuto. Ogni apprendente, in qualità di lavoratore della scuola, proprio per la natura complessa dell'IA, deve avere sempre chiara la responsabilità conseguente ad atti non coerenti con il Profilo professionale e con il Codice di comportamento dei dipendenti pubblici.

ARTICOLO 6: IA E AGENDA 2030

L'IA si basa su enormi quantità di dati e potenza di calcolo, risorse non sempre disponibili per tutte le istituzioni scolastiche. L'Istituto si impegna a utilizzare l'IA in modo consapevole, valutando l'efficienza e l'impatto ambientale degli strumenti adottati. L'automazione di attività amministrative ripetitive attraverso l'IA può contribuire a una maggiore efficienza e a un risparmio di risorse nel lungo termine. È importante che le scuole siano consapevoli della necessità di gestire l'innovazione e l'IA per non creare una "povertà di dati" e garantire pari opportunità digitali. Contestualmente occorre inserire l'IA all'interno della promozione della cultura dello sviluppo sostenibile.

ARTICOLO 7: IA E VALUTAZIONE

La valutazione di un test con l'IA è un processo che richiede la creazione di una chiave di correzione affidabile e la digitalizzazione delle risposte. L'IA può fornire un feedback coerente e uniforme, eliminando l'ambiguità nella valutazione e adattando le correzioni al livello di competenza degli studenti. Tuttavia, l'IA presenta alcune limitazioni nella correzione automatica a scuola, in quanto spesso non possiede il contesto completo, può non fornire feedback contestuale sulla coerenza concettuale o sulla qualità dell'argomentazione e può mancare di capacità di giudizio critico e valutazione qualitativa avanzata. La valutazione di risposte creative o originali rimane una sfida per l'IA. Pertanto, la correzione automatica da parte dell'IA richiede spesso una supervisione umana per garantire l'accuratezza e fornire un feedback equilibrato e personalizzato. L'IA può fornire un riscontro generale, segnalando errori grammaticali e suggerendo miglioramenti, ma non può sostituire completamente la valutazione umana per la complessità di alcuni compiti. In ambito scolastico, i sistemi di IA utilizzati per valutare i risultati dell'apprendimento delle persone rientrano nella categoria dei sistemi di IA ad alto rischio.

ARTICOLO 8: IA E INCLUSIONE

Gli strumenti di IA possono contribuire significativamente a creare un ambiente inclusivo a scuola, promuovendo l'uguaglianza delle opportunità di apprendimento per tutti gli studenti e lavoratori intesi come apprendenti, indipendentemente dalle loro abilità o dalle sfide che affrontano in relazione alla loro carriera scolastica. Possono essere utilizzati per tradurre contenuti, fornire spiegazioni in diverse lingue, convertire il testo in formato audio e adattare il contenuto alle esigenze specifiche degli studenti con diverse abilità, inclusi quelli con disabilità fisiche o cognitive. L'IA può offrire supporto personalizzato, assistenza multilingue, lettura assistita, traduzione istantanea e fornitura di risorse accessibili. Per gli studenti con disabilità motorie, l'interazione tramite tastiera o comando vocale può facilitare la partecipazione attiva. Durante periodi di istruzione a distanza, l'IA può svolgere un ruolo essenziale nell'offrire risorse educative. Per gli studenti con bisogni educativi speciali, l'uso dell'IA può essere personalizzato secondo il PDP/PEI, prevedendo modalità specifiche come sintesi vocale, supporto alla lettura, generazione di mappe concettuali interattive e creazione di esercizi personalizzati. L'uso dell'IA deve supportare, non sostituire, le strategie didattiche personalizzate. Scuole con studenti provenienti da diversi Paesi e culture possono impiegare strumenti di IA per tradurre il contenuto didattico e rendere l'apprendimento più accessibile.

ARTICOLO 9: IA E SANZIONI PER USO IMPROPRIO

Gli studenti che utilizzano in modo improprio gli strumenti di IA o generano contenuti in violazione del presente regolamento saranno soggetti a sanzioni disciplinari, definite in base alla gravità del comportamento. Le sanzioni saranno graduate e le violazioni ripetute comporteranno sanzioni

crescenti. Eventuali violazioni gravi, quali la diffusione non autorizzata di dati personali o la creazione di contenuti illegali, saranno segnalate alle autorità competenti. Anche i docenti e i genitori possono essere chiamati a rispondere di eventuali negligenze o mancata vigilanza. L'uso non autorizzato dell'IA da parte degli studenti comporta sanzioni disciplinari. Il plagio attraverso l'IA è considerato equivalente al plagio tradizionale. L'uso non autorizzato dell'IA da parte del personale scolastico può comportare danni di immagine all'istituzione e alla protezione dei dati promuovendo il rischio di data breach che comporta l'informativa al Garante entro 72 ore dalla violazione.

Si riporta di seguito l'elenco delle sanzioni degli studenti in base all'Articolo 5 dell'IA Act. Per il personale scolastico, invece, si fa esplicito riferimento al Codice del comportamento dei dipendenti pubblici e alle leggi connesse all'uso dei social.

Violazione dell'Articolo 5, lettera a) dell'IA Act (utilizzo di tecniche subliminali, manipolative o ingannevoli):

- *Prima violazione* (gravità lieve-media):

- Richiamo scritto da parte del docente o del docente coordinatore.
- Annotazione sul Registro di classe.
- Notifica ai genitori.
- Potenziale abbassamento del voto di comportamento.

- *Violazioni reiterate o caso singolo di gravità significativa:*

- Richiamo scritto da parte del Dirigente Scolastico.
- Sospensione dalle lezioni da 1 a 5 giorni deliberata dal Consiglio di Classe, previa istruttoria con audizione dello studente.
- Non partecipazione ai viaggi d'istruzione e/o alle visite guidate (a discrezione del Consiglio di Classe).
- Segnalazione al Dirigente Scolastico per ulteriori provvedimenti.
- Voto di comportamento negativo.
- Inserimento nel fascicolo dello studente.

Violazione dell'Articolo 5, lettera b) dell'IA Act (sfruttamento delle vulnerabilità di persone o gruppi):

- *Prima violazione* (gravità media):

- Richiamo scritto da parte del docente coordinatore o del Dirigente Scolastico.
- Annotazione sul Registro di classe.
- Notifica al Dirigente Scolastico ed ai genitori.
- Potenziale abbassamento del voto di comportamento.

- *Violazioni reiterate o caso singolo di gravità significativa* (es. danni significativi):

- Richiamo scritto da parte del Dirigente Scolastico.
- Sospensione dalle lezioni da 3 a 10 giorni deliberata dal Consiglio di Classe, previa istruttoria con audizione dello studente.
- Non partecipazione ai viaggi d'istruzione e/o alle visite guidate.
- Voto di comportamento negativo.
- Inserimento nel fascicolo dello studente.
- Segnalazione alle autorità competenti, se il comportamento configura bullismo o cyberbullismo.

Violazione dell'Articolo 5, lettera c) dell'IA Act (sistemi di IA per la valutazione o la classificazione sociale):

- *Utilizzo non autorizzato o consapevole di sistemi di social scoring* (gravità elevata):

- Richiamo scritto da parte del Dirigente Scolastico.
- Sospensione dalle lezioni da 5 a 15 giorni deliberata dal Consiglio di Classe, previa istruttoria con audizione dello studente.
- Non partecipazione ai viaggi d'istruzione e/o alle visite guidate.

- Voto di comportamento negativo.
- Inserimento nel fascicolo dello studente.
- Segnalazione alle autorità competenti, se il comportamento viola i diritti fondamentali e le normative sulla privacy.

Violazione dell'Articolo 5, lettera d) dell'IA Act (sistemi di IA per la valutazione del rischio di commissione di reati basata unicamente sulla profilazione):

- *Utilizzo non autorizzato o consapevole di tali sistemi* (gravità molto elevata):

- Richiamo scritto da parte del Dirigente Scolastico.
- Sospensione dalle lezioni da 10 a 15 giorni deliberata dal Consiglio di Classe, previa istruttoria con audizione dello studente.
- Potenziale allontanamento dalla comunità scolastica.
- Esclusione dallo scrutinio finale o dall'Esame di Stato (in base alla gravità e alle normative vigenti).
- Voto di comportamento negativo.
- Inserimento nel fascicolo dello studente.
- Notifica alle autorità scolastiche e giudiziarie.

Violazione dell'Articolo 5, lettera e) dell'IA Act (creazione o ampliamento di banche dati di riconoscimento facciale tramite scraping non mirato):

- *Raccolta e utilizzo non autorizzato di dati biometrici* (gravità elevata):

- Richiamo scritto da parte del Dirigente Scolastico.
- Sospensione dalle lezioni da 5 a 15 giorni deliberata dal Consiglio di Classe, previa istruttoria con audizione dello studente.
- Voto di comportamento negativo.
- Inserimento nel fascicolo dello studente.
- Segnalazione al DPO (Responsabile della Protezione dei Dati) della scuola.
- Notifica alle autorità competenti per violazione della normativa sulla privacy.

Violazione dell'Articolo 5, lettera f) dell'IA Act (inferire le emozioni nell'ambito del luogo di lavoro e degli istituti di istruzione):

- *Utilizzo non autorizzato di sistemi di inferenza emotiva* (gravità media):

- Richiamo scritto da parte del docente o del docente coordinatore.
- Annotazione sul Registro di classe.
- Notifica ai genitori.
- Potenziale abbassamento del voto di comportamento.

- *Violazioni reiterate o caso singolo di gravità significativa* (es. diffusione di dati sensibili):

- Richiamo scritto da parte del Dirigente Scolastico.
- Sospensione dalle lezioni da 1 a 5 giorni deliberata dal Consiglio di Classe, previa istruttoria con audizione dello studente.
- Voto di comportamento negativo.
- Inserimento nel fascicolo dello studente.
- Segnalazione al DPO della scuola.

È fondamentale sottolineare che la gravità della sanzione sarà valutata in base alla specifica situazione, all'intenzionalità dell'azione, al danno causato e all'eventuale reiterazione del comportamento. Inoltre, il coinvolgimento dei genitori è previsto in tutte le fasi del procedimento disciplinare. Le procedure di irrogazione delle sanzioni seguono quanto indicato negli elenchi precedenti, prevedendo generalmente: richiamo verbale, richiamo scritto, segnalazione, istruttoria del Consiglio di Classe con audizione dello studente e notifica alle famiglie e al Dirigente Scolastico. Nei casi più gravi, possono essere coinvolti l'Organo di Disciplina e le autorità competenti.

NORMATIVA GENERALE E DOCUMENTI DI RIFERIMENTO

- **Regolamento (UE) 2016/679 - GDPR (General Data Protection Regulation):** tutela dei dati personali.
- **Regolamento (UE) 2016/679 - GDPR artt. 5-25-30-32-33:** gestione dei log.
- **Codice in materia di protezione dei dati personali** - D.lgs. 196/2003, aggiornato dal **D.lgs. 101/2018**.
- **AGID (Agenzia per l'Italia Digitale)** - Strategia italiana per l'intelligenza artificiale 2024-2026.
- **AGID (Agenzia per l'Italia Digitale)** – Piano triennale per l'informatica nella Pubblica Amministrazione.
- **Legge n.71/2017** - Disposizioni a tutela dei minori per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo.
- **Legge n.241/1990** - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
- **Legge n.70/2024** - Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo.
- **Regolamento (UE) 2024/1689 (AI ACT).**
- **Legge n. 633/1941** - Legge sul diritto d'Autore.
- **Orientamenti etici per gli educatori sull'uso dell'IA** - Commissione Europea il 25 ottobre 2022.
- **Framework DigComp 2.2:** competenze digitali per cittadini europei, utile per progettare interventi educativi.
- **Linee guida Unesco IA.**
- **Linee guida sull'utilizzo dell'IA in ambito scolastico (Costruire il Futuro)** - Rete di scuole FVG.