Atto di Indirizzo del Dirigente scolastico:

Intelligenza Artificiale nelle Istituzioni Scolastiche

Sintesi della Trasformazione Digitale

Contesto Normativo e Quadro Giuridico

L'introduzione dell'intelligenza artificiale nelle scuole italiane non rappresenta più una scelta opzionale, ma un obbligo giuridico vincolante. Il quadro normativo si articola su tre livelli complementari[1]:

- **Regolamento (UE) 2024/1689 (AI Act)**: Entrato in vigore ad agosto 2024, stabilisce i requisiti per sistemi IA ad alto rischio, con applicazione completa entro il 2 agosto 2026[2].
- **Legge Nazionale IA (L. 132/2025)**: Entrata in vigore il 10 ottobre 2025, introduce disposizioni nazionali per l'uso responsabile dell'IA nella Pubblica Amministrazione, incluse le scuole.
- **Linee Guida MIM (9 agosto 2025)**: Pubblicate sulla Piattaforma Unica, forniscono indicazioni operative specifiche per l'uso consapevole, etico e sicuro dell'IA in ambito scolastico, in conformità con la normativa europea.
- **Regolamento (UE) 2016/679 (GDPR)**: Continua a disciplinare la protezione dei dati personali, con tutela rafforzata per minori considerati soggetti vulnerabili.

L'articolo 4 dell'AI Act, entrato in vigore il 2 febbraio 2025, impone obbligatoriamente la formazione di tutto il personale che utilizzi sistemi di IA (AI Literacy).

Privacy, GDPR e Protezione dei Minori

Un aspetto cruciale della trasformazione è la protezione della privacy degli studenti, riconosciuti dal GDPR come categoria vulnerabile meritevole di tutela rafforzata[3].

Base giuridica e consenso genitori: Contrariamente a una percezione diffusa, **non è necessario acquisire il consenso dei genitori** per l'uso didattico di strumenti di IA. La base giuridica è il **pubblico interesse** (articolo 6, paragrafo 1, lettera e del GDPR), in quanto l'attività didattica costituisce finalità istituzionale della scuola. Richiedere il consenso significherebbe subordinare l'esercizio di una funzione pubblica alla volontà dei singoli, snaturando il carattere istituzionale dell'attività scolastica[4].

Minimizzazione dei dati: Le scuole devono applicare rigorosamente il principio di minimizzazione, trattando solo i dati strettamente necessari alle finalità didattiche e formative. Ove possibile, privilegiare utilizzi anonimi o con dati di dominio pubblico, evitando l'identificazione degli studenti. Per la prima fase di adozione (2025-26), si raccomanda di limitarsi esclusivamente a **casi d'uso a rischio nullo**, ossia applicazioni che non comportano trattamento di dati personali[5].

Diritti e responsabilità: Gli studenti mantengono pienamente i diritti di accesso, rettificazione e cancellazione dei propri dati, con responsabilità della scuola di garantire l'esercizio effettivo di tali diritti. La scuola rimane titolare del trattamento e responsabile della conformità GDPR anche quando ricorre a fornitori cloud terzi.

Certificazione ACN e Sicurezza Informatica

Un elemento distintivo della governance dell'IA a scuola è la necessità di distinguere tra attività amministrativo-organizzative e attività didattiche pure, poiché i requisiti applicabili non sono identici[6].

Attività amministrativo-organizzative: Per tutte le applicazioni di IA destinate a supportare le funzioni gestionali della scuola (es. documentazione, comunicazioni istituzionali, analisi dati organizzativi), è **obbligatoria la certificazione ACN (Agenzia per la Cybersicurezza Nazionale)**. Questa certificazione, prevista dal Codice dell'Amministrazione Digitale (D.Lgs. 82/2005), attesta che il servizio rispetta gli standard minimi di sicurezza, affidabilità e localizzazione dei dati richiesti alle pubbliche amministrazioni. In particolare, garantisce che **i dati siano localizzati all'interno del territorio dell'Unione Europea**, evitando trasferimenti verso Paesi terzi privi di adeguate tutele.

Attività didattiche pure: Per le attività strettamente educative, è possibile una **maggiore flessibilità**, pur nel rigoroso rispetto del GDPR e dell'AI Act. Strumenti didattici quali Canva, Kahoot! e SketchUp, pur non disponendo di certificazione ACN autonoma, possono essere utilizzati nella didattica a condizione che sia completata una **DPIA (Data Privacy Impact Assessment)** specifica, valutando il rischio residuo come accettabile.

Strumenti integrati nelle piattaforme cloud: **Gemini** (integrato in Google Workspace for Education) e **Copilot** (integrato in Microsoft 365 Education) rappresentano il modello ottimale iniziale, poiché basati su infrastrutture cloud già qualificate ACN. Questi strumenti offrono garanzie contrattuali elevate, data residency in UE e assicurano che i dati non siano utilizzati per l'addestramento di modelli IA esterni.

Strumenti vietati: ChatGPT non certificato (utilizzabile solo tramite Azure OpenAI Service qualificato ACN), NotebookLM come applicazione standalone, e qualunque strumento "consumer" gratuito non certificato.

Valutazione dei Rischi: DPIA e Classificazione

La valutazione del rischio è il fulcro della governance dell'IA a scuola, determinando quali usi siano ammissibili e quale livello di documentazione sia richiesto[7].

Sistemi a rischio inaccettabile: Vietati in qualunque contesto (es. riconoscimento biometrico per scopi di controllo, valutazione automatizzata senza intervento umano che impatti diritti).

Sistemi ad alto rischio: Inizialmente vietati. Ammissibili solo dopo governance consolidata, formazione completata, DPIA e FRIA redatte, con decisione esplicita del Dirigente.

Sistemi a rischio limitato: Ammissibili dopo DPIA specifica e approvazione DPO.

Sistemi a rischio nullo/minimo: Ammissibili in Fase 1 (2025-26) senza formalità di DPIA, essendo privi di trattamento di dati personali o con dati anonimizzati.

DPIA (Data Privacy Impact Assessment): Obbligatoria per trattamenti ad alto rischio, quando decisa l'adozione di sistemi che comportino elaborazione di dati personali con impatti significativi su privacy e libertà. La DPIA, strumento previsto dal GDPR, identifica rischi, misure di mitigazione e valuta se il rischio residuo scenda sotto la soglia di accettabilità. Per i casi d'uso iniziali a rischio nullo, la DPIA non è richiesta.

Fasi di Adozione Graduale e Prudenziale

La scuola deve introdurre l'IA secondo un approccio **progressivo e controllato**, non generalizzato:

Fase 1 (2025-26): Casi d'uso a rischio nullo

- Generazione di materiali didattici generici (es. schede, guide, presentazioni senza dati personali)
- Supporto amministrativo a elaborazione documenti non sensibili
- Uso mediato e supervisionato dagli insegnanti (non autonomo degli studenti)
- Formazione staff su AI literacy
- Definizione di governance e policy
- Sperimentazione controllata con monitoraggio continuo

Fase 2 (2026+): Casi d'uso a rischio limitato

- Possibile solo dopo completamento governance, policy, formazione
- Con DPIA specifica e approvazione DPO
- Monitoraggio intensificato
- Eventuale uso mediato con studenti

Fase 3 (2026+): Casi d'uso ad alto rischio

- Possibile solo con DPIA e FRIA complete
- Decisione esplicita del Dirigente
- Revisione frequente
- Informazione trasparente a famiglie e studenti

Governance: Struttura e Responsabilità

Una governance efficace richiede il coinvolgimento strutturato di molteplici soggetti, superando la tradizionale divisione tra ambito didattico e amministrativo[8].

Dirigente Scolastico: Responsabile strategico dell'introduzione dell'IA. Redige un atto di indirizzo che definisce finalità e priorità del Piano IA, che deve essere integrato nel PTOF. Rimane titolare del trattamento dati e autorità decisionale su ogni caso d'uso di rischio elevato.

Referente per l'Innovazione e l'IA: Figura interna (docente nominato) che coordina le operazioni quotidiane, traduce le politiche in azioni concrete, gestisce il calendario formativo, monitora rischi operativi. Diverso dal consulente esterno.

Gruppo di Lavoro Multidisciplinare: Composto da 5-7 membri: 3-4 docenti (rappresentanti discipline artistiche, digitali, supporto BES), DSGA, personale tecnico ATA, DPO. Valuta rischi specifici, approva casi d'uso, redige policy e regolamenti, monitora adozione. Riporta trimestralmente al Collegio dei Docenti.

Collegio dei Docenti: Delibera su policy, strategie e Piano IA, approva delibere di governance, riceve report di monitoraggio.

DPO (Data Protection Officer - Responsabile della Protezione dei Dati): Valuta conformità GDPR, redige DPIA quando necessario, identifica rischi privacy, supporta decision-making su usi ad alto rischio. Per scuole in contratto con Vargiu Scuola Srl, il DPO esterno supporta questa funzione.

Consiglio di Istituto: Approva l'integrazione del Piano IA nel PTOF, riceve rendiconti annuali di conformità.

Strumenti Autorizzati: White List Iniziale

Per garantire conformità e sicurezza nella prima fase, la scuola adotta una **white list ristretta** di strumenti pre-valutati[9]:

Strumento	Certificazione ACN	Uso Amministrativo	Uso Didattico	Condizioni
Gemini (Google Workspace)	Sì (tramite Workspace)	Sì, condizionato	Sì, conforme	Solo Workspace Education con data residency UE
Copilot (Microsoft 365)	Sì (tramite M365)	Sì, condizionato	Sì, conforme	Solo M365 Education con configurazione ACN
Canva for Education	No	No	Sì, con DPIA	Trasferimento dati extra-UE - richiede DPIA specifica
Kahoot!	No	No	Sì, con DPIA	Trattamento risposte/IP - richiede DPIA e informativa
SketchUp for Schools	No	No	Sì, con DPIA	Integrato Google Workspace - rischio inferiore
GeoGebra	No	No	Sì	Modelli matematici - rischio minimo
ChatGPT diretto	No	No	No	**Vietato - non certificato**
NotebookLM	No	**Vietato**	No (solo con cautela)	**Consumer app - non idonea**

Piano d'Istituto per l'IA

Le Linee Guida MIM prescrivono che ogni scuola rediga un **Piano d'Istituto per l'Intelligenza Artificiale**, integrato nel PTOF, quale strumento di governance, programmazione e monitoraggio[10].

Il Piano deve contenere:

1. **Visione pedagogica e principi etici**: L'IA come strumento di personalizzazione, inclusione e sviluppo del pensiero critico, mantenendo la centralità del docente e il rispetto dei diritti umani.
2. **Obiettivi operativi misurabili** in tre aree:
    - Didattica: personalizzazione percorsi, tutoraggio intelligente, inclusione, valutazione formativa
    - Amministrazione: automazione processi, analisi predittiva dispersione, gestione documentale
    - Competenze digitali: AI literacy per staff e studenti in linea con DigComp 3.0
3. **Descrizione della governance**: Ruoli, responsabilità, struttura del gruppo di lavoro, modalità di decision-making.
4. **Analisi dei rischi e conformità**: Classificazione sistemi IA, DPIA quando richieste, valutazione FRIA, misure di mitigazione, conformità GDPR/AI Act.
5. **Risorse, formazione, partenariati**: Budget allocato, piani formativi AI literacy obbligatori (Art. 4 AI Act), collaborazioni con università e reti di scuole.
6. **Indicatori di monitoraggio (KPI)**: Numero casi d'uso adottati, tasso formazione completata, incidenti privacy rilevati, feedback comunità educante.
7. **Coinvolgimento comunità educante**: Assemblee, questionari, forum per raccogliere proposte, prevenire criticità, costruire consapevolezza etica.

Formazione (AI Literacy) - Obbligo Normativo

L'articolo 4 dell'AI Act, in vigore dal 2 febbraio 2025, **impone obbligatoriamente la formazione** di tutti coloro che forniscono o utilizzano sistemi di IA[11].

Per le scuole, ciò significa formazione strutturata per:

- **Dirigente e figure apicali**: Governance IA, responsabilità legale, AI Act, rischi etici
- **Docenti**: Funzionamento dell'IA, pedagogia con IA, riconoscimento bias, etica digitale, privacy
- **Personale ATA**: Automazione processi, sicurezza informatica, conformità normativa
- **Studenti** (secondaria): Uso consapevole IA, riconoscimento manipolazione algoritmica, etica digitale

Modalità: Almeno 20 ore per staff, formazione qualificata preferibilmente in linea con framework **DigComp 2.2** (in uso fino fine 2025) e **DigComp 3.0** (atteso da Commissione Europea entro dicembre 2025), che integra competenze di AI literacy.

Certificazione: Possibile certificazione formale tramite enti accreditati (es. Skill On Line) per attestare acquisizione competenze DigComp.

Azioni Immediate del Dirigente

Nella prima fase, prima ancora che il gruppo di lavoro definisca policy complete, il Dirigente deve adottare misure preventive[12]:

1. **Atto di Indirizzo** (novembre-dicembre 2025): Definisce finalità, priorità e strategia per il Piano IA integrato nel PTOF, autorizza costituzione gruppo di lavoro.

2. **Circolare Restrittiva** (dicembre 2025): Proibisce l'uso autonomo di strumenti IA non autorizzati, vietando qualunque applicazione che comporti trattamento di dati personali fino a completa definizione delle policy.

3. **Costituzione Gruppo di Lavoro** (dicembre 2025): Nomina referente interno, convoca gruppo multidisciplinare, avvia ciclo riunioni per analisi rischi e definizione policy.

4. **Adozione White List Iniziale** (gennaio 2026): Approva strumenti autorizzati (Google Workspace, Microsoft 365 con restrizioni, strumenti didattici certificati con DPIA).

5. **Pianificazione Formazione** (gennaio-febbraio 2026): Avvia moduli AI literacy per staff, coordina con fornitori (es. Skill On Line) per certificazioni.

6. **Coinvolgimento Comunità** (gennaio-marzo 2026): Assemblee con docenti e famiglie, informativa su IA e privacy, raccolta feedback.

Cosa Vietare Rigorosamente

Per tutela della comunità educante, alcune pratiche rimangono **categoricamente vietate**[13]:

- ChatGPT non certificato (usare solo via Azure OpenAI Service ACN-qualificato)
- NotebookLM come applicazione standalone per usi amministrativi
- Qualunque strumento gratuito "consumer" non certificato
- Riconoscimento biometrico (viso, impronta) per controllo o valutazione
- Valutazione automatizzata di elaborati studenteschi senza intervento umano
- Accesso autonomo di studenti a strumenti IA non supervisionati (Fase 1)
- Trasferimento di dati personali verso Paesi terzi senza garanzie contrattuali
- Profilazione di studenti per previsioni di comportamento
- Utilizzo di modelli IA addestrati su dati rubati o non consensuali

Timeline e Scadenze Critiche

Periodo	Azione	Responsabile
Novembre-Dicembre 2025	Atto di indirizzo, circolare restrittiva, costituzione gruppo lavoro	Dirigente
Gennaio-Febbraio 2026	Formazione AI literacy staff (20 ore min.), approvazione white list	Gruppo di lavoro
Febbraio 2, 2026	Scadenza Art. 4 AI Act - formazione obbligatoria attiva	Staff
Marzo-Aprile 2026	Redazione Policy e Regolamento IA, DPIA completate	Gruppo di lavoro + DPO

Aprile-Maggio 2026	Sperimentazione casi d'uso rischio nullo, monitoraggio	Docenti
Giugno 2026	Primo report monitoraggio al Collegio, adeguamenti	Referente IA
Agosto 2, 2026	Scadenza applicazione completa AI Act - controlli iniziano	Tutte le scuole
Settembre 2026	Valutazione Fase 1, pianificazione Fase 2	Dirigente + Gruppo

Riferimenti Normativi

[1] Regolamento (UE) 2024/1689 (AI Act); Legge 132/2025; Linee Guida MIM 9 agosto 2025; https://www.mim.gov.it/documents/20182/0/MIM_Linee+guida+IA+nella+Scuola_09_08_2025-signed.pdf

[2] AI Act Art. 85, compliance timeline; European Commission (2024)

[3] Regolamento (UE) 2016/679 (GDPR), artt. 4, 8, 14, 35 su minori e categoria vulnerabile

[4] GDPR Art. 6(1)(e) - Public interest base per scuole; Vargiu Scuola DPO nota 111/25

[5] GDPR principio di minimizzazione (Art. 5); AI Act rischio-based approach; MIM Linee Guida 2025

[6] Codice dell'Amministrazione Digitale (D.Lgs. 82/2005); Decreto ACN cybersicurezza; Vargiu Scuola DPO nota 110/25

[7] GDPR Art. 35 (DPIA); AI Act Arts. 6-52 (classificazione rischio); Vargiu Scuola DPO nota 110/25

[8] MIM Linee Guida IA 2025; Vargiu Scuola DPO nota 104/25 (Governance)

[9] Vargiu Scuola DPO nota 110/25 (tabella strumenti e certificazione ACN)

[10] MIM Linee Guida IA 2025; PTOF integrazione Piano IA

[11] AI Act Art. 4 (in vigore 2 febbraio 2025); MIM Linee Guida su AI Literacy

[12] Vargiu Scuola DPO note 104/25, 108/25 (azioni immediate Dirigente)

[13] AI Act Art. 5 (vietati), Art. 6 (alto rischio); GDPR Art. 12-22 (diritti); Vargiu Scuola DPO note 110/25, 111/25