ISTITUTO COMPRENSIVO STATALE DI LOZZO ATESTINO

REGOLAMENTO PER L'INTRODUZIONE E L'USO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

Governance, autorizzazione, impiego e controllo dei sistemi di IA

Versione 2.0	Revisione 10 agosto 2026	Prima adozione 13 febbraio 2026
Via G. Negri, 3 – 35034 Lozzo Atestino (PD)	Codice ministeriale PDIC85700D · C.F. 82005950280 · pdic85700d@istruzione.it	www.iclozzoatestino.edu.it

Principio guida L'IA supporta l'azione educativa e amministrativa, ma non sostituisce la responsabilità professionale, la relazione educativa, la valutazione umana né il potere decisionale degli organi competenti.

1. Oggetto, finalità e campo di applicazione

Il presente Regolamento disciplina la selezione, l'autorizzazione, l'acquisizione, la sperimentazione, l'uso, il monitoraggio e la dismissione dei sistemi di intelligenza artificiale impiegati dall'Istituto Comprensivo Statale di Lozzo Atestino.

Si applica al personale, agli alunni e alle alunne, ai collaboratori, ai fornitori e a ogni soggetto che utilizzi sistemi di IA per conto dell'Istituto o nell'ambito di attività scolastiche. Riguarda gli usi didattici, organizzativi, amministrativi, comunicativi, di orientamento, inclusione, ricerca e formazione.

- promuovere competenze di alfabetizzazione all'IA, pensiero critico e cittadinanza digitale;
- garantire centralità della persona, inclusione, accessibilità e pari opportunità;
- prevenire trattamenti illeciti di dati, discriminazioni, errori, dipendenza tecnologica e usi impropri;
- assicurare trasparenza, tracciabilità, sicurezza, controllo umano e responsabilità;
- integrare l'innovazione con PTOF, RAV, Piano di miglioramento, curricolo digitale e documenti di sicurezza dell'Istituto.

2. Quadro normativo e istituzionale

- Regolamento (UE) 2024/1689 (AI Act), nella versione vigente, incluse le modifiche introdotte dal Regolamento (UE) 2026/1744 e le relative scadenze applicabili;
- Regolamento (UE) 2016/679 (GDPR) e D.lgs. 30 giugno 2003, n. 196, come modificato dal D.lgs. 10 agosto 2018, n. 101;
- Legge 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale, con particolare riguardo alla tutela dei minori;
- Decreto ministeriale 9 agosto 2025, n. 166, e Linee guida per l'introduzione dell'intelligenza artificiale nelle istituzioni scolastiche;
- D.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), Legge 9 gennaio 2004, n. 4 e disciplina vigente in materia di sicurezza, accessibilità e amministrazione digitale;
- Legge 22 aprile 1941, n. 633 e normativa europea e nazionale vigente in materia di diritto d'autore e diritti connessi;

- Legge 29 maggio 2017, n. 71, come modificata dalla Legge 17 maggio 2024, n. 70, e disposizioni attuative in materia di bullismo e cyberbullismo;
- provvedimenti e materiali istituzionali del Garante per la protezione dei dati personali, incluso il vademecum aggiornato «La scuola a prova di privacy».

I richiami normativi si intendono effettuati ai testi vigenti. In caso di sopravvenienze legislative o di nuove indicazioni delle autorità competenti, prevalgono le disposizioni di rango superiore e il documento è aggiornato con la prima revisione utile.

3. Definizioni essenziali

Termine	Significato operativo
Sistema di IA	Sistema basato su macchina che, con differenti livelli di autonomia, produce previsioni, contenuti, raccomandazioni o decisioni a partire dagli input ricevuti.
IA generativa	Sistema che genera o modifica testi, immagini, audio, video, codice o altri contenuti.
Fornitore / deployer	Il fornitore sviluppa o immette sul mercato il sistema; l'Istituto, quando lo utilizza sotto la propria autorità, opera di regola come deployer.
Agente IA	Sistema capace di pianificare ed eseguire azioni o utilizzare strumenti esterni, anche su posta, documenti, archivi o applicazioni.
Controllo umano	Supervisione effettiva da parte di una persona competente, con possibilità di comprendere, correggere, arrestare o ignorare l'output.
Dati sintetici	Dati artificiali non riferibili a persone reali, utilizzati in via preferenziale per prove, esercitazioni e formazione.
Sistema ad alto rischio	Sistema ricadente nelle fattispecie individuate dall'AI Act, incluse determinate applicazioni in istruzione, accesso ai servizi e gestione del lavoro.

4. Principi di utilizzo

- Finalità educativa o istituzionale: ogni uso deve essere pertinente ai compiti dell'Istituto e proporzionato al risultato atteso.
- Centralità e autonomia della persona: l'IA non deve ridurre la libertà di giudizio, la dignità o lo sviluppo critico degli utenti.
- Controllo umano: nessun output produce automaticamente effetti su alunni, famiglie o personale.
- Protezione dei dati fin dalla progettazione e per impostazione predefinita: minimizzazione, limitazione delle finalità, sicurezza e tempi di conservazione definiti.
- Trasparenza e spiegabilità: utenti e interessati devono comprendere quando e per quale scopo è impiegata l'IA e a chi rivolgersi per chiarimenti o riesame.
- Equità, non discriminazione, inclusione e accessibilità: gli esiti sono controllati per bias e barriere, anche rispetto a disabilità, origine, genere, condizioni personali e socioeconomiche.
- Qualità e accuratezza: gli output sono verificati rispetto a fonti attendibili; errori e incertezze non sono occultati.
- Sicurezza e resilienza: accessi, integrazioni, log e fornitori sono gestiti secondo il livello di rischio.
- Sostenibilità: si privilegiano soluzioni adeguate alla finalità, evitando impieghi superflui o sproporzionati di risorse.
- Responsabilizzazione: decisioni, autorizzazioni, controlli e incidenti devono essere documentabili.

5. Condizioni per gli usi ammessi

Un sistema di IA può essere utilizzato per attività scolastiche soltanto se è presente nel Registro dei sistemi di IA autorizzati e se l'uso concreto rientra nelle finalità, negli utenti e nei dati indicati nel Registro.

Livello	Esempi	Condizioni minime
Ordinario	Ideazione, esercitazioni, spiegazioni, materiali su dati pubblici o sintetici, accessibilità, traduzione e revisione linguistica.	Autorizzazione e registrazione; verifica umana; nessun dato personale non necessario.
Con cautele rafforzate	Analisi di documenti interni, personalizzazione didattica, produzione pubblica, integrazioni o agenti IA, uso sistematico da parte di minori.	Valutazione preventiva documentata; coinvolgimento di RPD/DPO e responsabili tecnici quando pertinente; informazione, formazione e monitoraggio.
Alto impatto / potenzialmente alto rischio	Accesso o ammissione, valutazione che incide sul percorso, assegnazione di opportunità, gestione o selezione del personale, profilazione significativa.	Di regola non adottato. Eventuale uso soltanto se giuridicamente ammissibile, necessario, specificamente autorizzato e corredato dalle valutazioni previste dalla normativa.

L'autorizzazione riguarda sempre una combinazione determinata di sistema, finalità, utenti, categorie di dati e modalità operative. Una funzione nuova, un'integrazione diversa o una modifica sostanziale del fornitore richiedono un nuovo esame.

6. Pratiche vietate

Sono vietati, oltre ai casi previsti dalla legge:

- l'uso di sistemi non presenti nel Registro per trattare dati o svolgere attività istituzionali;
- l'inserimento in servizi non autorizzati di dati personali, categorie particolari di dati, credenziali, documenti riservati, informazioni su disabilità, salute, situazioni familiari, procedimenti disciplinari o valutazioni individuali;
- il riconoscimento delle emozioni nell'ambiente scolastico o lavorativo, salvo le ristrette eccezioni mediche o di sicurezza previste dalla legge e comunque senza preventiva autorizzazione formale;
- il punteggio sociale, la manipolazione subliminale o ingannevole e lo sfruttamento di vulnerabilità legate all'età, alla disabilità o alla condizione sociale;
- la categorizzazione biometrica diretta a inferire dati sensibili e la raccolta indiscriminata di immagini facciali;
- decisioni esclusivamente automatizzate su valutazione, ammissione, orientamento, disciplina, inclusione, assegnazione di benefici, selezione o gestione del personale;
- la generazione o diffusione di impersonificazioni, deepfake ingannevoli, contenuti sessualizzati, denigratori, discriminatori o utilizzati per bullismo e cyberbullismo;
- l'elusione delle misure di sicurezza, dei limiti di età, delle condizioni d'uso o dei controlli predisposti dall'Istituto;
- il collegamento di agenti IA a registro elettronico, SIDI, posta, archivi, gestionali, dispositivi o servizi cloud senza un progetto specificamente autorizzato;
- la pubblicazione o l'invio automatico di comunicazioni e documenti senza conferma umana competente.

7. Governance e responsabilità

Soggetto	Compiti principali
Dirigente scolastico	Assicura la governance; autorizza progetti e sistemi nei limiti delle competenze; dispone sospensioni; garantisce raccordo con organi collegiali, DSGA, RPD/DPO e sicurezza; riferisce periodicamente sull'attuazione.
Referente IA – Carlo Maron	Coordina istruttoria e mappatura; mantiene il Registro; supporta alfabetizzazione, sperimentazioni e monitoraggio; raccoglie segnalazioni; propone aggiornamenti. Non sostituisce le responsabilità del Titolare, del RPD/DPO o dei responsabili di procedimento.
DSGA e uffici	Curano gli aspetti amministrativi, contrattuali, documentali, contabili e di inventario; verificano che acquisti e affidamenti recepiscano i requisiti approvati.
RPD/DPO	Fornisce consulenza indipendente su protezione dati; supporta la valutazione dei rischi e la DPIA quando dovuta; coopera nella gestione delle violazioni di dati personali.
Team IA / innovazione / STEM	Supporta sperimentazione, formazione, condivisione di pratiche, accessibilità, verifica didattica e raccolta delle evidenze.
Personale	Usa soltanto sistemi autorizzati; rispetta finalità, istruzioni e riservatezza; verifica gli output; segnala errori e incidenti; mantiene la responsabilità professionale.
Studenti e famiglie	Rispettano la Policy studenti e le indicazioni dei docenti; proteggono dati e credenziali; dichiarano gli usi richiesti; segnalano contenuti o comportamenti dannosi.
Fornitori	Rispettano contratto, protezione dati, sicurezza, trasparenza, accessibilità, assistenza, cancellazione e audit; comunicano modifiche e incidenti senza ritardo.

8. Autorizzazione, Registro e ciclo di vita

Ogni proposta segue il seguente percorso, in misura proporzionata al rischio:

1. descrizione del bisogno, della finalità, degli utenti, dei dati, dell'alternativa non basata su IA e del beneficio atteso;
2. verifica preliminare di termini d'uso, età minima, sicurezza, accessibilità, ubicazione dei dati, conservazione, riuso per addestramento, subfornitori e trasferimenti;
3. classificazione del rischio e consultazione di DSGA, RPD/DPO, responsabili tecnici, organi collegiali o altri soggetti competenti quando necessario;
4. DPIA ai sensi dell'art. 35 GDPR soltanto quando il trattamento può presentare un rischio elevato; valutazione d'impatto sui diritti fondamentali quando e nei casi previsti dall'AI Act;
5. autorizzazione, registrazione, informazione agli utenti, configurazione sicura e formazione;
6. eventuale sperimentazione limitata, con criteri di successo e condizioni di arresto;
7. monitoraggio di accuratezza, bias, incidenti, reclami, efficacia didattica, costi e modifiche del servizio;
8. riesame almeno annuale e in occasione di modifiche sostanziali; sospensione o dismissione con esportazione e cancellazione dei dati.

Registro vincolante Il Registro dei sistemi di IA autorizzati è l'unica fonte istituzionale per conoscere strumenti, funzionalità, categorie di utenti e usi consentiti. L'assenza dal Registro equivale a mancata autorizzazione per l'uso scolastico.

9. Protezione dei dati personali e tutela dei minori

- Si usano dati personali soltanto quando indispensabili, su idonea base giuridica e con informativa adeguata; per prove e formazione si preferiscono dati sintetici o effettivamente anonimizzati.
- Non si inseriscono prompt, allegati o immagini eccedenti la finalità; la pseudonimizzazione riduce il rischio ma non trasforma i dati in dati anonimi.
- Gli account istituzionali sono personali; credenziali e codici di autenticazione non devono essere condivisi né inseriti nei prompt.
- I dati non possono essere riutilizzati dal fornitore per addestrare modelli o finalità proprie, salvo specifica valutazione, adeguata base giuridica e autorizzazione documentata.
- Per gli utenti con meno di quattordici anni, l'accesso a tecnologie di IA e i conseguenti trattamenti avvengono nel rispetto dell'art. 4 della Legge n. 132/2025 e con gli atti richiesti a chi esercita la responsabilità genitoriale. Tra quattordici e diciassette anni il minore può esprimere il consenso nei casi previsti, sulla base di informazioni chiare, semplici e accessibili.
- Le attività curricolari non devono imporre la creazione di account personali su servizi al consumo; l'Istituto predispone ambienti gestiti o un'alternativa didattica equivalente.
- Per alunni con disabilità, DSA o altri bisogni educativi, l'uso dell'IA è coerente con PEI, PDP o altra progettazione individualizzata, con particolare tutela dei dati sulla salute.

10. Acquisti, contratti e rapporti con i fornitori

Prima dell'acquisizione o dell'attivazione sono verificati almeno:

- ruolo privacy del fornitore e, quando ricorrono i presupposti, accordo ai sensi dell'art. 28 GDPR;
- finalità, dati trattati, ubicazione, trasferimenti, subfornitori, tempi di conservazione, cancellazione ed esportabilità;
- divieto o disattivazione del riuso dei dati e degli input per addestramento, salvo autorizzazione espressa;
- misure di sicurezza, gestione degli accessi, log, continuità del servizio, notifica degli incidenti e possibilità di audit;
- documentazione richiesta dall'AI Act, istruzioni d'uso, limiti noti, metriche, trasparenza e supervisione umana;
- accessibilità, tutela dei minori, condizioni di età, assistenza e diritto di recesso o dismissione;
- modifiche del modello o delle condizioni: il fornitore deve informare l'Istituto prima che incidano sull'autorizzazione.

11. Trasparenza, contenuti generati e proprietà intellettuale

- L'uso sostanziale dell'IA è dichiarato nei documenti, elaborati o comunicazioni quando richiesto dalla legge, dal docente, dalla procedura o dalla rilevanza del contenuto.
- I contenuti sintetici o manipolati, inclusi deepfake leciti, sono etichettati in modo chiaro; i testi pubblicati per informare il pubblico su materie di interesse pubblico sono sottoposti a revisione umana e, quando dovuto, recano l'indicazione dell'impiego di IA.
- La persona che approva o firma un contenuto ne verifica accuratezza, completezza, tono, riferimenti, assenza di dati indebiti e rispetto dei diritti altrui.
- Output, fonti e materiali di input sono utilizzati nel rispetto del diritto d'autore, delle licenze, dei diritti di immagine e delle regole di citazione; l'output di un sistema non è considerato automaticamente libero da diritti.

- Non si pubblicano prompt o log contenenti informazioni riservate; la trasparenza può essere assicurata mediante una descrizione sintetica e veritiera del contributo dell'IA.

12. Alfabetizzazione all'IA e formazione

L'Istituto assicura attività periodiche, differenziate per ruolo, su funzionamento e limiti dei sistemi, verifica degli output, protezione dei dati, sicurezza, diritto d'autore, inclusione, bias, trasparenza, uso didattico e gestione degli incidenti. Le attività essenziali sono documentate; per usi con cautele rafforzate è richiesta una formazione specifica prima dell'abilitazione.

Gli studenti sviluppano competenze progressive di comprensione, utilizzo critico, dichiarazione del contributo dell'IA e riconoscimento di contenuti sintetici o manipolati, in coerenza con il curricolo e l'età.

13. Monitoraggio, segnalazioni e incidenti

Errori gravi, output discriminatori o pericolosi, accessi indebiti, perdita di riservatezza, uso di sistemi non autorizzati, deepfake dannosi e altri incidenti devono essere segnalati senza ritardo al Dirigente scolastico, al Referente IA o all'indirizzo pdic85700d@istruzione.it.

- L'utente interrompe l'uso, evita ulteriori condivisioni e conserva soltanto le informazioni necessarie alla verifica, senza diffondere dati o contenuti dannosi.
- Il Dirigente attiva i soggetti competenti, incluso il RPD/DPO quando vi sono dati personali, valuta la sospensione del sistema e dispone le misure di contenimento.
- Le eventuali violazioni di dati personali sono gestite secondo la procedura data breach e i termini del GDPR; gli interessati sono informati quando previsto.
- Gli utenti possono chiedere spiegazione e riesame umano di un esito che li riguardi; reclami e richieste sono documentati e contribuiscono al monitoraggio.
- Almeno annualmente sono esaminati Registro, incidenti, reclami, formazione, benefici, criticità e necessità di revisione.

14. Approvazione, entrata in vigore e revisione

Il presente Regolamento è sottoposto agli organi collegiali competenti ed entra in vigore dalla data stabilita nell'atto di approvazione. È pubblicato sul sito istituzionale e richiamato nelle informative, nelle policy e nelle istruzioni operative pertinenti.

La revisione è almeno annuale e, in ogni caso, è effettuata quando intervengono modifiche normative, nuove Linee guida, incidenti significativi, cambiamenti dei fornitori o introduzione di usi ad alto impatto. Le Policy per il personale e per gli studenti costituiscono atti attuativi del presente Regolamento.

ALLEGATO A — Scheda preliminare di proposta e autorizzazione

Campo	Informazioni da compilare
Proponente e data	Nome, ruolo, unità/plesso, data della proposta
Sistema e fornitore	Denominazione, versione, URL, fornitore, funzioni richieste
Finalità e beneficio	Problema da risolvere, risultato atteso, coerenza con PTOF/PdM
Utenti e minori	Personale/alunni/famiglie; fasce d'età; modalità di accesso e supervisione
Dati e documenti	Dati pubblici, sintetici, interni, personali o particolari; allegati e output
Decisioni interessate	Effetti su valutazione, accesso, orientamento, disciplina, inclusione o lavoro
Integrazioni e agenti	Accesso a posta, cloud, registro, gestionali, API, pubblicazione o azioni automatiche
Fornitore e sicurezza	Conservazione, addestramento, subfornitori, trasferimenti, log, incidenti, cancellazione
Accessibilità e alternative	Misure inclusive; alternativa equivalente non basata su IA
Valutazioni richieste	☐ screening rischio ☐ RPD/DPO ☐ DPIA ☐ sicurezza ☐ impatto diritti fondamentali ☐ organi collegiali
Esito	☐ autorizzato ☐ autorizzato con condizioni ☐ sperimentazione ☐ non autorizzato
Condizioni e riesame	Istruzioni, formazione, indicatori, responsabile monitoraggio, data revisione

ALLEGATO B — Struttura minima del Registro dei sistemi di IA

Il Registro è aggiornato dal Referente IA e validato secondo le competenze interne. Per ciascun sistema sono riportati almeno i seguenti elementi.

ID	Sistema / fornitore	Finalità e utenti	Dati / integrazioni	Rischio e controlli	Stato / riesame

Campi ulteriori raccomandati: versione e funzioni abilitate; base giuridica; contratto/accordo privacy; sede dei dati; durata; età minima; formazione; referente operativo; incidenti; decisione di sospensione o dismissione.

ALLEGATO C — Scheda essenziale di segnalazione incidente

Campo	Informazioni
Segnalante e contatto	
Data, ora e sistema	
Descrizione dell'evento	
Persone e dati coinvolti	
Output o azioni prodotte	
Misure immediate adottate	
Diffusione o destinatari	
Allegati o evidenze disponibili	
Canale di segnalazione Dirigente scolastico, Referente IA Carlo Maron oppure pdic85700d@istruzione.it. Non inoltrare il contenuto dannoso a soggetti non coinvolti nella gestione.	

Fonti ufficiali principali

- MIM — Decreto ministeriale n. 166 del 9 agosto 2025
- EUR-Lex — Regolamento (UE) 2024/1689 sull'intelligenza artificiale
- EUR-Lex — Regolamento (UE) 2016/679 (GDPR)
- Normattiva — Legge 23 settembre 2025, n. 132
- Garante per la protezione dei dati personali — Scuola