

REGOLAMENTO / POLICY D'ISTITUTO SULL'USO DELL'INTELLIGENZA ARTIFICIALE (IA)

Regolamento / Policy d'Istituto sull'uso dell'IA

1) Scopo e ambito di applicazione

La presente Policy disciplina l'uso di strumenti di Intelligenza Artificiale (IA) – inclusi i modelli generativi testuali e multimodali (LLM) e gli strumenti per la generazione e modifica di immagini e video (es. text-to-image / text-to-video), come ChatGPT, Gemini, Copilot e strumenti analoghi – da parte del personale dell'Istituto per attività didattiche, amministrative e di comunicazione istituzionale, nel rispetto della normativa vigente (in particolare GDPR e normativa nazionale privacy) e delle disposizioni dell'Unione europea in materia di IA (Reg. UE 2024/1689 – AI Act), tenendo conto delle indicazioni ministeriali applicabili e operando in coerenza con il PTOF e con il Patto educativo di corresponsabilità, ove pertinenti. La presente Policy è adottata nel rispetto del GDPR e della normativa nazionale privacy, del Regolamento (UE) 2024/1689 (AI Act) e, ove applicabile e per quanto pertinente, delle indicazioni ministeriali in materia di IA nelle istituzioni scolastiche adottate con DM MIM n. 166 del 9 agosto 2025 (Linee guida allegate) e della Legge 23 settembre 2025, n. 132, ferma restando l'applicazione prioritaria e diretta della normativa europea.

Nota: la citazione di nomi commerciali (es. ChatGPT, Gemini, Copilot, Canva, ecc..) è a scopo puramente descrittivo e non implica autorizzazione; fanno fede l'Inventario d'Istituto (Allegato A) e le condizioni d'uso ivi indicate.

A) Si applica a: Dirigente scolastico, DSGA, personale di segreteria, docenti, studenti, ATA, collaboratori, consulenti/fornitori che operano per conto della scuola.

Si applica su: dispositivi e account istituzionali.

B) Dispositivo personale: l'uso di strumenti di IA per attività dell'Istituto su dispositivo personale (PC/telefono/tablet) è consentito solo per i servizi autorizzati dall'Istituto e secondo le relative condizioni d'uso. Per servizi esterni non autorizzati è vietato l'accesso tramite SSO ("Accedi con Google/Microsoft" o equivalenti) e l'uso dell'account di dominio; in mancanza di tali condizioni, l'uso su dispositivo personale non è autorizzato.

Nella fase iniziale per la redazione del presente Regolamento, l'Istituto ha avviato una ricognizione degli strumenti e delle app a disposizione, senza coinvolgimento degli studenti, ponendo priorità su strumenti governabili tramite account istituzionali (es. Microsoft 365 Copilot e Canva for Education). Il Regolamento si applica al personale e, per quanto di competenza, anche agli studenti. L'introduzione di nuovi strumenti o nuove funzionalità AI, e qualsiasi modifica delle condizioni d'uso per studenti o personale, richiede valutazione preliminare, aggiornamento dell'Inventario (Allegato A) ed eventuali comunicazioni interne. L'eventuale uso di funzionalità di Intelligenza Artificiale su strumenti istituzionali autorizzati è ammesso quando il trattamento dei dati personali è necessario per finalità didattiche e organizzative dell'Istituto (art. 6(1)(e) e/o 6(1)(c) GDPR). Il consenso è richiesto solo per attività facoltative e separatamente.

2) Definizioni

Strumento IA/LLM: sistema che genera testi, immagini, codice o risposte automatiche a partire da un'istruzione dell'utente.

Prompt: la richiesta/istruzione inserita dall'utente per ottenere un output dal sistema IA.

Output: testo/immagine/documento prodotto dall'IA.

Dati personali: informazioni riferite a persona identificata o identificabile (es. nome studente, email, telefono, codice fiscale).

Dati particolari (sensibili): categorie speciali di dati (es. salute, disabilità, BES/DSA/PEI, situazioni familiari delicate) e, ove applicabile, dati giudiziari/disciplinari.

Dati riservati dell'Istituto: informazioni e documenti non destinati alla pubblicazione (es. verbali, registri, documenti interni, credenziali, procedure interne), anche quando non contengono dati personali.

Account istituzionale: credenziali rilasciate e gestite dalla scuola (es. Google Workspace/Microsoft 365) soggette a policy, controlli e revoca da parte dell'Istituto.

Account personale: credenziali private dell'utente, non gestite dall'Istituto.

Dispositivo personale: uso di un dispositivo personale (PC/telefono/tablet) per attività dell'Istituto.

Anonimizzazione: trasformazione dei dati che rende la persona non identificabile in modo ragionevole (irreversibile).

Pseudonimizzazione: sostituzione degli identificativi con codici/etichette (es. "Studente S1"), con possibilità di re-identificazione tramite informazioni aggiuntive conservate separatamente.

Cronologia/Log/Telemetria: registrazioni conservate dallo strumento (es. cronologia chat, accessi, metadati tecnici) che possono incidere su riservatezza e conservazione.

Addestramento/Training: processo con cui un modello IA viene (ri)allenato; alcuni servizi, a seconda dei termini contrattuali/impostazioni, possono usare contenuti inseriti dagli utenti per migliorare il modello.

Allucinazioni: risposte dell'IA plausibili ma errate o inventate (es. riferimenti normativi inesistenti, dati o citazioni non verificabili).

Supervisione umana: controllo e validazione da parte di una persona competente prima dell'uso dell'output (specialmente per comunicazioni ufficiali o contenuti che incidono su persone).

Decisione automatizzata: decisione assunta tramite processi automatizzati (anche con IA) che produce effetti giuridici o incide in modo analogo significativamente su una persona.

SSO: sistema di accesso che consente di entrare in un servizio usando le stesse credenziali di un altro account (es. "Accedi con Google/Microsoft"), senza creare una password separata.

DPA (Data Processing Agreement): accordo/atto con cui il fornitore è designato Responsabile del trattamento e si disciplinano istruzioni, misure di sicurezza, sub-responsabili e trasferimenti.

DPIA (Valutazione d'impatto sulla protezione dei dati): analisi prevista dall'art. 35 GDPR per trattamenti che possono comportare un rischio elevato per i diritti e le libertà delle persone.

FRIA (Valutazione d'impatto sui diritti fondamentali): analisi degli impatti dell'uso dell'IA sui diritti fondamentali e delle misure di mitigazione, ove applicabile o ritenuta opportuna in base al caso d'uso.

Servizio "consumer" e servizio "istituzionale/tenant": per "consumer" si intende un servizio usato con account personali e governance limitata; per "istituzionale/tenant" un servizio configurato e governabile dall'Istituto (es. criteri di accesso, impostazioni, audit), in genere preferibile.

3) Principi generali

a) Uso responsabile e tracciabile: l'IA è un supporto, non sostituisce le responsabilità umane.

b) Minimizzazione: usare il minimo di informazioni possibile (preferibilmente nessun dato personale).

c) Supervisione umana obbligatoria: ogni output va verificato prima dell'uso, soprattutto se comunicazione ufficiale.

d) Riservatezza e sicurezza: proteggere dati e credenziali; vietata la condivisione non autorizzata.

e) Equità e non discriminazione: l'IA può riflettere bias o produrre contenuti distorti; il personale deve evitare usi che possano generare disparità di trattamento o discriminazioni, adottando controlli e correzioni, soprattutto quando l'output incide su persone.

f) Accessibilità e inclusione: quando l'IA è impiegata per supportare la didattica o la comunicazione, l'Istituto promuove soluzioni accessibili e inclusive, evitando che l'uso degli strumenti crei barriere o esclusioni e garantendo alternative equivalenti quando necessario.

4) Usi consentiti (solo alcuni esempi)

- a) Bozze di testi generici (circolari, avvisi, comunicazioni) senza dati personali.
- b) Riformulazione/semplificazione linguistica di testi già pubblici o generici.
- c) Traduzioni e revisione di stile di testi non contenenti dati personali.
- d) Creazione di checklist, template, FAQ, procedure operative interne in forma anonima.
- e) Supporto alla preparazione di materiali didattici generali (non personalizzati su singoli studenti).
- f) Supporto a formule e automazioni di base per fogli di calcolo (Excel/Sheets) utilizzando dati fittizi o anonimizzati.
- g) Creazione di tabelle e pianificazioni generiche (calendari, cronoprogrammi, liste di controllo) senza dati personali.
- h) Sintesi e riorganizzazione di contenuti pubblici (es. note e documenti istituzionali), senza incollare documenti riservati.
- i) Creazione di modelli e testi standard (es. modulistica, comunicazioni tipo) come bozza da revisionare, senza dati personali.
- j) Produzione di schemi, mappe concettuali, scalette e bozza di slide generiche, senza dati personali.
- k) Generazione di immagini/illustrazioni e materiali grafici (es. locandine, copertine, icone, infografiche) senza dati personali e senza riferimenti a persone identificabili (es. volti, nomi, classi).

NB: Ogni nuovo strumento è utilizzabile solo dopo inserimento nel documento Inventario.

5) Usi vietati (divieti operativi)

- a) Inserire nei prompt dati personali identificativi di studenti/minori, famiglie o personale (nomi, email, numeri, CF, indirizzi), salvo casi eccezionali autorizzati e con strumenti approvati.

- b) Inserire dati particolari/sensibili (salute, disabilità, BES/DSA/PEI, relazioni riservate, provvedimenti disciplinari nominativi).
- c) Usare l'IA per valutazioni/decisioni automatiche su studenti (ammissioni, assegnazioni, classificazioni, scoring) o sul personale, senza specifica istruttoria, valutazione del rischio e autorizzazione formale.
- d) Usare sistemi di IA che analizzano/emulano/interpretano emozioni o stati psicologici di studenti/persone in ambito scolastico, salvo casi previsti dalla legge e formalmente autorizzati.
- e) Caricare su strumenti IA file interi o parziali (verbali, registri, PEI/PDP, fascicoli) anche se “solo per riassumere” o “analizzare”.

Resta inoltre vietato inserire nei prompt o trasmettere tramite strumenti IA credenziali, password, codici di accesso, token, link riservati, informazioni di sicurezza o dettagli che possano compromettere i sistemi dell'Istituto; tali informazioni non devono mai essere riportate né in chiaro né in forma parzialmente mascherata.

6) Login a software, siti e app di terzi

L'uso di credenziali istituzionali dell'Istituto (account di dominio) e dell'autenticazione SSO (“Accedi con Google/Microsoft” o equivalenti) è consentito esclusivamente per i servizi indicati nella DPIA e nell'Allegato A alla DPA (Google Workspace for Education, Microsoft app and services/Office 365, Canva for Education). Per ogni altro servizio, anche se presente nell'Allegato A applicazioni e software (catalogo), è vietato usare SSO e qualunque accesso con account di dominio. L'eventuale registrazione con email istituzionale come semplice username è consentita solo senza SSO, con password dedicata diversa, e senza inserire dati personali né caricare materiali scolastici.

7) Regole su account, strumenti e acquisizione (procurement)

Sono ammessi esclusivamente gli strumenti indicati nell'Inventario d'Istituto (Allegato A), utilizzati con account istituzionali o con modalità espressamente autorizzate. Qualsiasi nuova adozione, estensione d'uso o attivazione di funzionalità basate su IA/LLM (anche quando l'IA è integrata “dietro le quinte” in un'app o tramite servizi terzi/API) è consentita solo dopo una valutazione preliminare di privacy e sicurezza e il conseguente aggiornamento dell'Inventario, che per ciascuno strumento indica l'esito (Ammesso, Ammesso con condizioni, Non ammesso) e le condizioni operative.

Le modalità operative e i passaggi rapidi per richiedere la valutazione di nuovi strumenti o funzionalità (anche con IA integrata) sono descritti nell'Allegato B. Il DPO è coinvolto per il parere sugli aspetti di protezione dei dati e per supportare l'eventuale DPIA; la decisione finale di adozione e le disposizioni organizzative conseguenti competono al Titolare, nella persona del Dirigente scolastico. In sede di istruttoria, l'Istituto verifica almeno il ruolo del fornitore (processor/controller), l'esistenza e adeguatezza degli accordi contrattuali applicabili (inclusa la DPA quando il fornitore tratta dati per conto della scuola), l'eventuale catena di sub-fornitori e i trasferimenti di dati, nonché le misure di sicurezza e le impostazioni governabili dal tenant (controlli amministrativi, autenticazione, log e tempi di conservazione, opzioni di esclusione dal training ove disponibili), assicurando coerenza con le finalità istituzionali e con i principi di minimizzazione.

Gli strumenti "in valutazione" possono essere utilizzati esclusivamente nell'ambito di sperimentazioni formalmente autorizzate dall'Istituto, con condizioni di prova documentate e senza inserimento di dati personali o documenti riservati. È vietato usare account personali per attività lavorative con dati della scuola.

Il personale è tenuto a rispettare le misure minime di sicurezza su credenziali e dispositivi (autenticazione forte ove disponibile, blocco schermo, aggiornamenti, antivirus/EDR – un "antivirus avanzato" che rileva comportamenti sospetti e aiuta a bloccarli sui dispositivi) e ad attenersi alle istruzioni operative e al piano di formazione adottati dall'Istituto (Allegato B).

8) Trasparenza verso utenti esterni (se applicabile)

Qualora la scuola utilizzi chatbot o assistenti IA rivolti a famiglie/studenti (es. sul sito), deve garantire adeguata trasparenza: indicare chiaramente che l'utente interagisce con un sistema IA, fornire canale alternativo umano e assicurare che l'assistente non richieda/gestisca dati sensibili.

In ogni caso, i contenuti destinati alla pubblicazione o a comunicazioni istituzionali che siano redatti con supporto di strumenti IA devono essere sottoposti a revisione umana prima dell'uso, con verifica di accuratezza e coerenza con le fonti ufficiali; quando opportuno, l'Istituto conserva traccia del processo di revisione e qualifica l'output come bozza fino alla validazione finale, evitando che l'automazione sostituisca le responsabilità e le verifiche proprie delle funzioni istituzionali.

9) Gestione incidenti (data breach / uso improprio)

- a) Se viene inserito per errore un dato personale o un documento riservato in un LLM, informare immediatamente il Dirigente/DSGA e il DPO secondo la procedura di segnalazione interna.
- b) Non cancellare prove/log se richiesti per l'analisi, limitare la diffusione e seguire le indicazioni ricevute.
- c) Qualsiasi sospetto di accesso non autorizzato o fuga di dati va segnalato subito.

10) Entrata in vigore, controlli e aggiornamenti

La Policy entra in vigore dalla data di pubblicazione. È soggetta a riesame almeno annuale o in occasione di introduzione di nuovi strumenti o funzionalità, incidenti di sicurezza, aggiornamenti normativi e indicazioni istituzionali rilevanti; in tali casi l'Istituto aggiorna anche l'Inventario (Allegato A) e comunica tempestivamente al personale eventuali nuove condizioni o divieti.

11) Divieti di utilizzo

È vietato utilizzare per finalità istituzionali applicazioni, piattaforme o funzionalità (anche integrate "dietro le quinte") non presenti nell'Inventario d'Istituto (Allegato A). Qualsiasi nuova app o nuova funzione basata su IA/LLM può essere utilizzata solo dopo richiesta formale compilando il Modulo predisposto dall'Istituto.

12) Referente Ai / Team Ai di Istituto

L'Istituto individua un Referente IA (oppure un Team Ai con un Referente Ai al suo interno) con funzioni di supporto organizzativo e operativo per l'uso conforme degli strumenti di IA. Il Referente Ai coordina le procedure per l'aggiornamento dell'elenco delle applicazioni ammesse e delle relative condizioni d'uso, supporta docenti e personale nella richiesta/valutazione di nuove app e promuove indicazioni formative di base. Collabora con Dirigente, DSGA, DPO ed eventuale Consulente Ai esterno per gli aspetti di privacy, sicurezza e gestione delle segnalazioni/criticità.

- 12.1 Richiesta ammissione nuove app/software

La richiesta per ammettere nuove app o software all'interno dell'Allegato A al presente Regolamento, può essere presentata da docenti, staff, referenti di progetto, funzioni strumentali e personale amministrativo, per esigenze didattiche o organizzative motivate. Il

richiedente contatta il Referente (o altro personale con simili funzioni) o il Team Ai interno all'Istituto il quale, una volta ottenuta la richiesta, compila il form "Richiesta nuova app Ai" alla pagina www.easyteam.org/ai/form_nuova_app. Prima di compilare il form, l'eventuale coinvolgimento del Referente Ai / animatore digitale è consigliato. In caso di ammissione, il richiedente verrà avvisato (e con esso il Referente Ai dell'Istituto) del responso e, se positivo, contestualmente verrà aggiornato l'Allegato A.

13) Studenti e Intelligenza artificiale

È consentito usare l'IA solo per supporto (es. idee, scalette, revisione linguistica) e non per consegnare come proprio un elaborato generato integralmente. È obbligatorio dichiarare quando e come l'IA è stata usata (strumento e tipo di aiuto, anche per i compiti da casa) e conservare, se richiesto, i passaggi principali. È vietato inserire nei prompt dati personali propri o di terzi (compagni, docenti, famiglia) o documenti della scuola. Le violazioni rientrano nelle regole di correttezza e valutazione dell'Istituto (integrità del lavoro e responsabilità individuale).