



Ministero dell'istruzione e del merito
Istituto Comprensivo Statale "Don Milani"

Via Don Milani snc – 20085 LOCATE DI TRIULZI (MI) - Tel. 02 90780494
CM MIIC88500B - e-mail: MIIC88500B@istruzione.it - PEC: MIIC88500B@pec.istruzione.it
C.F. 97029000151 - IPA: istsc_miic88500B - CODICE UNIVOCO: UFG4BB
sito: <https://scuolalocate.edu.it>

REGOLAMENTO / POLICY D'ISTITUTO

SULL'USO DELL'INTELLIGENZA ARTIFICIALE (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 e da parte degli studenti, 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 per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche"* versione 1.0) e della Legge 23 settembre 2025, n. 132 - *"Disposizioni e deleghe al Governo in materia di intelligenza artificiale"* - 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/smartphone/tablet per il personale e PC/tablet per gli studenti, ai quali non è consentito in nessun caso l'uso dello smartphone) è permesso 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 sperimentazioni rivolte a personale e docenti, 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/smartphone/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 (Single Sign-On): 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 (Data Protection Impact Assessment): analisi prevista dall'art. 35 GDPR per trattamenti che possono comportare un rischio elevato per i diritti e le libertà delle persone. Letteralmente: valutazione d'impatto sulla protezione dei dati.

FRIA (Fundamental Rights Impact Assessment): 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. Letteralmente: valutazione d'impatto sui diritti fondamentali.

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 destinati a intere classi o gruppi di alunni con caratteristiche omogenee (omettendo qualsiasi riferimento a specifici alunni).
- f) Supporto alla definizione di 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 (relativi a condizioni di salute, disabilità, BES/DSA/PEI, relazioni riservate, procedimenti 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 1 alla DPIA (Google Workspace for Education, Microsoft app and services/Office 365, Canva for Education). Per ogni altro servizio, anche se presente nell'Allegato A al regolamento 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

Al momento la scuola non utilizza chatbot o assistenti IA. Qualora in futuro la scuola utilizzasse chatbot o assistenti IA rivolti a famiglie/studenti (es. sul sito), dovrà 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 conserverà 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) Gruppo di lavoro IA

L'Istituto ha costituito un gruppo di lavoro per l'intelligenza artificiale. Del gruppo di lavoro - che opera con la consulenza di un DPO e di un AI Compliance manager esterni - fanno parte

dirigente scolastico, DSGA, animatore digitale, un docente di scuola primaria e un docente di scuola secondaria di 1^a grado. Il Gruppo è incaricato di: supportare il DS nell'analisi del contesto e nella definizione della strategia di adozione dell'IA; redigere le policy interne per l'uso degli strumenti di IA in ambito didattico e amministrativo; predisporre linee guida, regolamenti, istruzioni operative e altri strumenti documentali; contribuire alla valutazione del livello di maturità digitale dell'istituto secondo lo schema AgID; collaborare con il DPO e l'AI Compliance Manager nella valutazione dei rischi (DPIA, ed eventuale FRIA); promuovere l'alfabetizzazione digitale e l'AI literacy di personale e studenti; monitorare l'introduzione graduale di strumenti IA attraverso progetti pilota; aggiornare periodicamente il DS sugli sviluppi normativi e tecnologici. Il coordinamento del gruppo è affidato al Dirigente scolastico che assume l'incarico di Referente per l'Intelligenza Artificiale. All'interno del gruppo, l'animatore digitale 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.

- 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 compila il form "Richiesta nuova app AI" alla pagina <https://www.easyteam.org/ai/richiesta-inserimento-nuova-ia-app/>. Prima di compilare il form, è consigliato il coinvolgimento dell'animatore digitale. 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 chiunque altro (compagni, docenti, personale della scuola, amici, conoscenti, familiari) o documenti della scuola. Le violazioni rientrano nelle regole di correttezza e valutazione dell'Istituto per le quali si rimanda al regolamento di valutazione e disciplina pubblicato all'indirizzo <https://scuolalocate.edu.it/la-scuola/le-carte/55-regolamenti>.

Il presente regolamento è stato approvato nel collegio docenti e consiglio d'istituto del 14 maggio 2026

ALLEGATO A - Applicazioni e software ammessi

Data ultimo aggiornamento: 21/04/2026

Elenco delle applicazioni autorizzate con indicazioni operative

Applicativo	AI presente di default	AI integrabile/attivabile	Motivazione	Condizioni d'uso
Adobe Acrobat Reader		X	Lettore PDF con funzioni IA disponibili (AI Assistant add-on); rischio se si analizzano/caricano documenti con dati personali.	Non usare AI Assistant su documenti con dati personali/sensibili; preferire uso locale/offline; disabilitare funzioni cloud non necessarie; usare account istituzionale; attenzione a condivisioni e sincronizzazioni automatiche.
Adobe Firefly	X		Generazione immagini/testi con IA; utile per materiali didattici; rischio se si caricano foto o dati identificativi.	Solo docenti (studenti solo se autorizzati dall'istituto); vietato caricare foto/volti di studenti; vietato inserire dati personali nei prompt; verificare licenze/diritti delle immagini.
Adobe Spark	X		Consentito solo Adobe Express for Education; Firefly IA gestibile/disattivabile da admin per K-12.	Solo Adobe Express for Education; Firefly/IA solo se autorizzata; niente dati personali nei prompt.
Algor Education (Algor)	X		Piattaforma per creare mappe/materiali da testo o file con AI; rischio se si caricano documenti contenenti dati personali.	Non caricare compiti, PDP/PEI o documenti con dati personali; usare solo contenuti didattici anonimi; revisione docente dei risultati; usare account istituzionale se previsto.
Autodesk		X	Consentito per CAD; funzioni AI/generative usabili solo con supervisione e dati non personali.	Solo licenze Education; funzioni AI/generative solo se autorizzate; vietati dati personali nei file.
Baamboozle			Piattaforma di giochi/quiz per la classe; utile per ripasso e dinamiche partecipative.	Raccomandato uso studenti senza account (solo partecipazione al gioco); docente con account; non usare nomi/cognomi degli studenti (solo nickname non identificativi); vietato inserire dati personali/sensibili in domande/risposte; non usare durante verifiche se non autorizzato.
Book creator	X		IA immagini opzionale; attivazione controllata dal docente; accesso con Adobe Education.	IA immagini opzionale; attivazione solo docente; vietato caricare volti o dati personali.
bSmart			Piattaforma per libri digitali e contenuti didattici; necessaria per testi adottati; attenzione a gestione account e dati di utilizzo.	Usare credenziali scolastiche; minimizzare dati nel profilo; verificare impostazioni privacy/cookie; evitare caricamenti di dati sensibili; uso verifiche/CBT secondo regolamento d'istituto.
Canva vers. for Education	X		Consentito solo con Canva for Education: controlli IA, DPA; contenuti studenti non usati per training.	Solo Canva for Education; IA Magic solo se autorizzata; vietati dati personali nei prompt.
Capcut	X		Generative AI e upload media; servizio consumer non controllabile centralmente.	Studenti 14+ ammessi solo previa autorizzazione dei genitori e supervisione docente; studenti <14 non ammesso (uso consentito solo al docente). In ogni caso: vietato caricare/elaborare foto/video/audio con volti, voci o nomi di studenti; usare solo contenuti stock/anonimi; esportazione e conservazione solo locale; niente pubblicazione su profili/servizi collegati.

ALLEGATO A - Applicazioni e software ammessi

Data ultimo aggiornamento: 21/04/2026

Elenco delle applicazioni autorizzate con indicazioni operative

Applicativo	AI presente di default	AI integrabile/attivabile	Motivazione	Condizioni d'uso
ChatGpt	X		Servizio LLM di tipo consumer. In versione gratuita non sono disponibili controlli centralizzati e configurazioni amministrative; la gestione dei dati e delle impostazioni dipende dall'utente, con maggiore rischio di inserimento improprio di informazioni e minore verificabilità della compliance. In caso di attivazione di versioni a pagamento/education con gestione istituzionale, il livello di controllo e governance è superiore e i rischi si riducono.	Ammesso solo per docenti come supporto alla preparazione didattica; vietato inserire dati personali o documenti scolastici. Non usare per valutazioni/compiti degli studenti; disattivare cronologia/condivisione se disponibili.
Claude (Anthropic)	X		LLM generativo: utile per supporto alla progettazione didattica e revisione testi; rischio alto se si inseriscono dati personali o materiali scolastici riservati.	Solo docenti; vietato inserire dati personali/sensibili o documenti interni (elenchi, PDP/PEI, valutazioni, verbali); non usare per valutazione o decisioni su studenti; disattivare/negare uso dei dati per addestramento dove disponibile; preferire piani Team/Enterprise con garanzie contrattuali e DPA.
code.org (ai disattivata)	X		Consentito per coding; AI Chat Lab/Tutor vietati salvo autorizzazione e policy dedicate.	Consentito con AI disattivata; attività guidate; vietato inserire dati personali nei progetti.
DeepL	X		Traduttore con IA; utile per traduzione/riscrittura di testi; rischio se si inseriscono dati personali o contenuti riservati.	Solo testi didattici; vietato inserire dati personali/sensibili; preferire account/licenza istituzionale (Pro se disponibile); non caricare verifiche o documenti con dati di studenti.
Duolingo (solo for Schools)	X		Piattaforma di apprendimento lingue; ammessa esclusivamente in configurazione "for Schools" per maggiore controllo didattico. Esclusa qualsiasi attivazione/uso di Duolingo Max (funzioni generative).	Solo utilizzo tramite classi "for Schools" con impostazioni privacy della classe; vietato inserire dati personali/sensibili in profilo o contenuti; evitare account personali studenti quando non necessari; nessun uso durante verifiche se non autorizzato dal docente.
Duolingo vers. for Schools	X		Consentito solo Duolingo for Schools; vietata versione Max con GPT-4/Roleplay.	Solo Duolingo for Schools; vietata versione Max/AI; uso con account classe.
Edpuzzle	X		Teacher Assist (IA) genera domande; vietato autograding per valutazioni ufficiali.	Teacher Assist solo docenti; revisionare domande; vietato uso per valutazioni automatiche ufficiali.

ALLEGATO A - Applicazioni e software ammessi

Data ultimo aggiornamento: 21/04/2026

Elenco delle applicazioni autorizzate con indicazioni operative

Applicativo	Al presente di default	Al integrabile/attivabile	Motivazione	Condizioni d'uso
ELi APPBook (Gruppo ELi)			Piattaforma per l'accesso ai libri digitali dei testi in adozione; necessaria per la fruizione di contenuti e risorse editoriali.	Usare solo per i testi in adozione; per studenti preferire accesso tramite codice (senza registrazione) dove previsto; minimizzare dati nel profilo; vietato inserire/caricare dati personali/sensibili (valutazioni, BES/DSA, elenchi); accessi con credenziali istituzionali per docenti; evitare condivisione pubblica di link/codici.
Evernote	X		Evernote AI opzionale; vietato inserire dati studenti o dati sensibili nei contenuti. App potenzialmente ad altro rischio, stando alla documentazione ritrovabile in data di formazione del presente documento/lista.	Ammesso solo per docenti per appunti organizzativi/didattici; vietato inserire dati di studenti o documenti con dati personali. Disattivare funzioni AI se non necessarie e usare solo account dedicato/istituzionale (non personale).
Genially	X		Funzioni IA per contenuti; prompt elaborati da modelli esterni; vietati dati personali.	IA solo se autorizzata; vietati dati personali nei prompt; output verificato dal docente.
Google Workspace for Education - Gemini - Notebook LM		X	Ambiente istituzionale gestibile; controlli admin; protezioni dati; uso conforme con policy e formazione.	Solo account istituzionali; Gemini solo se autorizzato; vietato in verifiche; no dati personali nei prompt.
Gynzy			Lavagna interattiva e strumenti per la didattica digitale; (al momento) non centrata su IA generativa; utile come "whiteboard" in classe.	Usare account istituzionali/classe; minimizzare dati profilo; non inserire dati personali/sensibili nelle attività; evitare materiali con nominativi/valutazioni; classi chiuse e link non pubblici; gestione credenziali e ruoli a cura della scuola.
HeyGen	X		Video/avatar con IA per creare contenuti didattici; rischio alto se si usano media identificativi.	Solo docenti; vietato caricare o generare contenuti con volti/voci di studenti o personale; usare solo materiali stock/anonimi; niente dati personali nei testi; niente pubblicazione esterna non autorizzata.
HUB Scuola		X	Ambiente digitale per libri e contenuti; include strumenti e Tutor AI; attenzione a dati inseriti e ai requisiti di età/registrazione indicati dal fornitore.	Usare account scolastico; AI solo su contenuti didattici; vietato inserire dati personali nei campi di testo/prompt; rispettare requisiti di età e modalità di accesso previste dall'informativa.
HUB Scuola		X	Ambiente digitale per libri e contenuti; include strumenti e Tutor AI; attenzione a dati inseriti e ai requisiti di età/registrazione indicati dal fornitore.	Usare account scolastico; AI solo su contenuti didattici; vietato inserire dati personali/sensibili nei campi di testo/prompt; per trattamenti ulteriori (es. marketing) valgono soglie/consenso: 14 anni o consenso genitoriale se minore; evitare condivisioni pubbliche e link aperti.
Kahoot	X		Consentito; usa generatore domande AI (GPT-4); vietato per valutazioni automatiche ufficiali.	Generatore AI solo docenti; revisionare quiz; vietato per valutazioni automatiche ufficiali.

ALLEGATO A - Applicazioni e software ammessi

Data ultimo aggiornamento: 21/04/2026

Elenco delle applicazioni autorizzate con indicazioni operative

Applicativo	Al presente di default	AI integrabile/ attivabile	Motivazione	Condizioni d'uso
LibreBooking			Sistema di prenotazione ambienti/risorse (aule, laboratori, attrezzature). Soluzione open-source tipicamente installata su server (self-hosted): utile per gestione organizzativa e tracciamento prenotazioni.	Preferire installazione su server della scuola o fornitore con DPA art. 28 GDPR; usare account istituzionali; minimizzare i dati (nome, email) ed evitare note con dati sensibili (es. motivazioni mediche); impostare visibilità "solo ciò che serve" e ruoli; definire tempi di conservazione e backup.
Liveworksheet	X		AI Chat Assistant solo docenti; vietato inserire dati studenti; uso account scuola.	AI Assistant solo docenti; vietato inserire dati studenti; usare account istituzionale.
MagicSchool.ai	X		Strumenti IA per docenti (lezioni, rubriche, feedback); utile ma rischioso se si inseriscono dati di studenti.	Solo docenti; vietato inserire dati personali/sensibili (nomi, valutazioni, PDP/PEI); usare esempi anonimi; non usare per valutazione automatica; esportare i materiali nei sistemi della scuola.
Minerva Education AI (minervaeducationai.it)	X		Assistente IA per attività didattiche e creazione materiali; utile ma piattaforma esterna (serve attenzione a dati e tracciamenti).	AmMESSO solo docenti; vietato inserire dati personali/sensibili o documenti interni; usare solo contenuti didattici anonimi; per adozione di istituto richiedere accordo/DPA e chiarimenti su conservazione dati e sub-fornitori.
Office 365 con/ senza Copilot	X		Microsoft 365: piattaforma istituzionale con controlli tenant. Microsoft 365 Copilot/Copilot Chat (work/education): impegni di privacy e compliance Microsoft 365; prompt/risposte e dati via Microsoft Graph non usati per addestrare i modelli di base; controlli e audit tramite Microsoft Purview.	Usare solo l'account istituzionale della scuola e accedere dalla versione "lavoro/scuola" (non con account personali). Non inserire mai nei prompt dati personali o sensibili (nomi studenti, valutazioni, PDP/PEI, ecc.). Non usare lo strumento durante verifiche o valutazioni. La scuola deve attivare regole che proteggono e gestiscono i dati (chi può vedere cosa, per quanto tempo si conservano e quando si eliminano).
Padlet	X		AI invia contenuti a terzi con diverse modalità. Non vietata ma applicazione con rischi nell'uso dei dati.	AmMESSO solo tramite account/ambiente istituzionale e bacheche private con moderazione docente; vietati dati personali, immagini o documenti di studenti. Funzioni IA disattivate/non usate e link non indicizzati (accesso solo a autorizzati).
Panquiz	X		IA genera domande; uso docente; vietato per valutazioni ufficiali automatizzate.	IA solo docenti; revisionare domande; vietato per valutazioni ufficiali automatizzate.

ALLEGATO A - Applicazioni e software ammessi

Data ultimo aggiornamento: 21/04/2026

Elenco delle applicazioni autorizzate con indicazioni operative

Applicativo	Al presente di default	Al integrabile/attivabile	Motivazione	Condizioni d'uso
Pear Deck			Strumento per lezioni interattive (Slides) con risposte studenti in tempo reale; tratta dati di utilizzo e potenzialmente dati identificativi se configurato con account.	Usare solo con account istituzionali; minimizzare dati profilo; evitare richieste di dati personali agli studenti nelle attività; preferire accesso tramite classe/codice senza raccolta extra; per adozione di istituto: formalizzare DPA/accordo privacy e verificare misure e conservazione dati.
Pearson (piattaforme/servizi digitali)			Piattaforme e contenuti digitali Pearson; gestione account studenti e dati di utilizzo; verificare limiti di età previsti dai servizi.	Usare email scolastiche; minimizzare dati nel profilo; rispettare i limiti di età e le condizioni del servizio (in alcune informative: non rivolto a studenti <14); evitare caricamenti di dati sensibili.
Planner 5D (Educational License – studenti ammessi con codice)	X		Uso didattico di modellazione 2D/3D con funzioni IA; ammesso per studenti solo tramite licenza Educational gestita dal docente/istituto e sotto supervisione.	Solo piano Educational; studenti solo con codice licenza (no account personali “liberi”); profili minimizzati (niente cognome/classe in chiaro); vietato caricare dati personali/sensibili e foto; disattivare/evitare community e condivisioni pubbliche; revoca licenze e cancellazione progetti a fine attività; DPA/accordo art. 28 GDPR con fornitore.
Powtoon		X	Funzionalità IA per creazione contenuti/video; rischio se si caricano dati/immagini di minori.	Usare preferibilmente con account docente; vietato caricare foto/video con volti o dati identificativi di studenti; niente dati personali nei prompt/script; esportare e conservare i file su archivi scolastici; verificare licenze e diritti d'autore.
QuestionWell	X		Generatore IA di domande/quiz/materiali; utile per preparare attività e verifiche.	Solo docenti; non inserire dati personali/sensibili nei prompt; non caricare verifiche con nomi studenti; usare contenuti didattici anonimi; gestire i materiali finali nei sistemi della scuola.
QuillBot		X	Assistente di scrittura/parafrasi con IA; utile per revisione e miglioramento testi; rischio privacy se si incollano testi con dati personali e rischio didattico (copia).	Vietato inserire dati personali/sensibili o testi che identificano studenti; vietato durante verifiche/interrogazioni salvo autorizzazione docente; usare solo per bozze anonime e revisione linguistica; per uso diffuso di istituto: valutare DPA e impostazioni di conservazione/telemetria.
Quizlet		X	Flashcard e studio; disponibili anche funzioni AI/assistite: utile per apprendimento, ma attenzione a dati inseriti e uso improprio durante valutazioni.	Preferire uso senza account per studenti o account istituzionali; vietato inserire dati personali/sensibili nei set o nei prompt; non pubblicare set con riferimenti identificativi; vietato durante verifiche/interrogazioni salvo autorizzazione docente; per studenti <14: se richiesta registrazione, gestire eventuale consenso genitoriale secondo policy di istituto.

ALLEGATO A - Applicazioni e software ammessi

Data ultimo aggiornamento: 21/04/2026

Elenco delle applicazioni autorizzate con indicazioni operative

Applicativo	Al presente di default	Al integrabile/attivabile	Motivazione	Condizioni d'uso
Reverso Context	X		Traduzione in contesto con tecniche NLP/IA; utile per lingua; rischio tracciamenti web e inserimento di dati personali nei testi.	Usare solo per frasi/testi didattici; vietato inserire dati personali/sensibili; evitare login con email personale degli studenti; attenzione a cookie e profilazione.
Sanoma (piattaforme/servizi digitali)			Piattaforme e contenuti digitali Sanoma; utili per fruizione di libri/risorse; attenzione a gestione account e tracciamenti.	Usare email scolastiche; minimizzare dati nel profilo; rispettare informativa e impostazioni privacy/cookie; evitare caricamenti di dati sensibili; uso secondo regolamento d'istituto.
SchoolAI	X		Piattaforma IA per scuola (tutor/attività/assistenti): utile per didattica guidata; rischio alto se usata con dati identificativi o senza governance su minori.	Preferire uso gestito dalla scuola (classi/utenze istituzionali); per studenti sotto 14: usare solo con condizioni della scuola e, se richiesto, consenso genitoriale; vietato inserire dati personali/sensibili; non usare per valutazione automatica; per adozione di istituto: DPA e verifica trasferimenti/garanzie.
Scratch	X		Face Sensing usa modello IA; vietare riprese volti; usare account scuola	Consentito; vietare Face Sensing con volti; usare account classe; supervisione docente.
SimpleMind			App per mappe mentali principalmente offline; utile per organizzazione e studio senza necessità di IA.	Evitare sincronizzazioni cloud se non necessarie; non inserire dati personali nei contenuti o allegati; usare dispositivi/account gestiti dalla scuola.
SketchUp (Trimble)		X	Software di modellazione 3D; può integrare estensioni/servizi con funzionalità IA (es. rendering/ottimizzazione/generazione contenuti); rischio se si usano servizi cloud o plugin terzi con caricamento di file/dati.	Usare licenze Education e, se disponibile, account istituzionale; vietato inserire dati personali o documenti scolastici nei modelli, nomi file o prompt; evitare upload su cloud (Trimble Connect o simili) di progetti con dati personali; estensioni IA/plugin terzi solo se autorizzati e valutati; conservazione/esportazione preferibilmente locale; logout e non salvare credenziali sui PC della scuola.
Sostituzioni Docenti			Gestionale per organizzare e pubblicare le sostituzioni: può trattare dati del personale (nominativi, orario, assenze/sostituzioni).	La privacy pubblicata appare generica e con riferimenti normativi datati, quindi serve governance contrattuale prima dell'uso. Accesso solo a personale autorizzato; schermate/monitor solo in aree riservate (non visibili a studenti/utenza esterna); minimizzare dati esposti (solo ciò che serve); credenziali istituzionali e log di accesso; utile accordo/DPA ex art. 28 GDPR e verifica di eventuali sub-fornitori/hosting e tempi di conservazione.
StoryboardThat		X	Include AI storyboard generator; vietati dati personali; output revisionato dal docente.	Al generator solo docente; vietati dati personali; output revisionato prima di condivisione.

ALLEGATO A - Applicazioni e software ammessi

Data ultimo aggiornamento: 21/04/2026

Elenco delle applicazioni autorizzate con indicazioni operative

Applicativo	AI presente di default	AI integrabile/attivabile	Motivazione	Condizioni d'uso
Thinglink	X		AI per immagini, tag, quiz; vietati dati personali; usare impostazioni privacy IA.	Funzioni AI solo se autorizzate; vietati dati personali; controllare impostazioni privacy e condivisione.
Veyon			Software per gestione aula informatica: consente monitoraggio e controllo dei PC degli studenti (schermi, blocco, demo, accesso remoto, trasferimento file). Ammesso solo per finalità didattiche e sicurezza della lezione.	Installazione solo su rete scolastica e solo PC d'aula; accesso consentito solo a docenti/personale autorizzato; vietato uso fuori dall'orario di lezione o su PC non didattici; disattivare/limitare funzioni non necessarie (es. file transfer, accesso remoto) se non indispensabili; niente registrazioni sistematiche; informativa interna agli studenti e aggiornamento registro trattamenti.
Wayground (ex Quizizz)		X	Piattaforma per quiz/compiti con generatori IA (domande, rubriche, lezioni). Utile didatticamente, ma richiede regole per evitare inserimento di dati personali nei prompt e per la gestione account studenti; dati ospitati extra-UE (USA).	Preferire partecipazione studenti "senza account" tramite codice attività; se account studenti: minimizzare dati (solo quanto necessario) e rispettare art. 8 GDPR (sotto 14 serve consenso del genitore); vietato inserire dati personali/sensibili nei prompt o nei contenuti caricati; per adozione di istituto: formalizzare accordo/DPA e verificare basi/garanzie trasferimento (SCC).
Wordwall	X		Usa AI content generator; docente revisiona; vietato inserire dati personali; no valutazioni automatiche.	AI generator solo docenti; revisionare attività; vietati dati personali; no valutazioni automatiche.
WPS Office (Kingsoft)		X	Suite office (documenti, fogli, presentazioni) con servizi cloud e funzioni AI attivabili (WPS AI): utile per attività didattiche, ma con rischio privacy se si usa cloud/AI su contenuti con dati personali.	Preferire uso locale/offline; se cloud: solo account istituzionale e sincronizzazione controllata; vietato inserire o caricare dati personali/sensibili (studenti, famiglie, BES/DSA, valutazioni) nei documenti o nei prompt; funzioni AI disattivate per gli studenti e comunque non utilizzabili da minori <16 senza autorizzazione genitoriale verificabile; evitare condivisioni pubbliche/link aperti; logout dai PC della scuola.
XMind		X	Software mappe mentali; include funzioni Xmind AI; utile per brainstorming e studio; rischio se si usano cloud/collaborazione con dati personali.	Preferire uso locale; se cloud/collab solo con account istituzionale; AI solo su contenuti didattici non personali; disattivare condivisioni pubbliche e link aperti.
Zanichelli		X	piattaforma editoriale; nessuna funzione IA dichiarata; usare account istituzionali e privacy policy.	Solo piattaforma editoriale; account istituzionali; nessuna IA dichiarata; minimizzare dati personali.

ALLEGATO A - Applicazioni e software ammessi

Data ultimo aggiornamento: 21/04/2026

Elenco delle applicazioni autorizzate con indicazioni operative

Applicativo	Al presente di default	Al integrabile/attivabile	Motivazione	Condizioni d'uso
Zoom		X	Piattaforma di videoconferenza con funzioni di IA attivabili (Zoom AI Companion: riassunti, smart recording, domande sulla riunione); ammessa per incontri con genitori e specialisti se governata dall'istituto.	Ammesso per colloqui/riunioni scuola-famiglia e con specialisti; preferire licenza d'istituto con accordo/DPA; AI Companion disattivato a livello account (meeting summary, smart recording, meeting questions); niente dati personali/sensibili condivisi o trascritti; link non pubblici, waiting room e passcode; registrazioni disattivate salvo necessità e informativa preventiva.



Ministero dell'istruzione e del merito
Istituto Comprensivo Statale "Don Milani"

Via Don Milani snc – 20085 LOCATE DI TRIULZI (MI) - Tel. 02 90780494
CM MIIC88500B - e-mail: MIIC88500B@istruzione.it - PEC: MIIC88500B@pec.istruzione.it
C.F. 97029000151 - IPA: istsc_miic88500B - CODICE UNIVOCO: UFG4BB
sito: <https://scuolalocate.edu.it>

ALLEGATO B

Mappa rapida dei documenti dell'Istituto

Documento	A cosa serve	Quando lo richiamo
Regolamento d'Istituto sull'uso dell'IA	Regole di comportamento e divieti/consensi.	Per definire cosa è consentito/vietato e le condizioni operative.
Allegato A – Inventario strumenti/app	Elenco strumenti: ammesso / con condizioni / non ammesso.	Per autorizzare o negare e comunicare condizioni.
Allegato B – Il presente documento Con istruzioni operative e formazione	Regole pratiche, esempi, procedure (account, incidenti).	Per standardizzare l'uso quotidiano e la formazione.
DPIA (<i>data protection impact assessment</i> - Valutazione d'impatto sulla protezione dei dati) AI	Valuta rischi privacy legati alle funzioni IA.	Quando si trattano dati di minori, dati particolari o su larga scala.
PUIA – Piano per l'utilizzo dell'intelligenza artificiale di istituto	Visione, governance e revisione annuale.	Per pianificare adozione, formazione e riesame.

Ruoli e responsabilità minime

- DS: decide adozione/abilitazione, approva condizioni d'uso, assicura trasparenza e supervisione umana.
- DSGA: presidia flussi amministrativi, istruzioni operative al personale e gestione documentale (output, accessi).
- Referente IA / Team per l'intelligenza artificiale: supporta screening casi d'uso, configurazioni e formazione di base, fa da tramite per richieste di ammissione di nuove app.
- DPO: supporta su impatti privacy e valutazioni (es. DPIA) quando pertinenti.

Per decisioni che incidono su studenti o personale (voti, sanzioni, ammissioni, assegnazioni), l'output IA non può essere usato "in automatico". Serve sempre controllo umano e motivazione.

Procedura per valutare uso Ai

1. Definire il caso d'uso
 - Chi usa (o dovrebbe usare) lo strumento?
 - Per quale attività concreta?
 - Quali dati potrebbero entrare/uscire?
 - Dove finiscono input/output?
 - Chi controlla e decide (supervisione)?
2. Verificare se lo strumento è già autorizzato.
 - Controllare Inventario (Allegato A).
 - Se non è presente: avviare la richiesta (Allegato B) e consentire solo prove con contenuti fittizi/anonimi.
3. Screening AI Act: è “alto rischio”?
 - Alto rischio quando l'IA incide su valutazioni, ammissioni/assegnazioni o *proctoring* (sorveglianza automatizzata durante lo svolgimento di test).
 - Di norma NON alto rischio: bozze, traduzioni, sintesi, esercizi generici (sempre con verifica umana).
4. Se è alto rischio: presìdi rafforzati (e FRIA - *Fundamental Rights Impact Assessment* ovvero valutazione dell'impatto su diritti fondamentali).
 - Documentazione e istruzioni del fornitore; definizione di supervisione umana reale; tracciabilità minima e gestione incidenti.
 - Valuta FRIA prima del primo utilizzo (Sezione 5).
5. Trasparenza verso utenti (AI Act art. 50).
 - Se un utente interagisce con un assistente IA: deve saperlo (salvo sia ovvio).
 - Per contenuti pubblicati generati/manipolati con IA: regole interne di disclosure e revisione umana.
6. AI literacy (AI Act art. 4).
 - Briefing minimo per il personale coinvolto (rischi, divieti, fact-checking, dati).
7. Formalizzare e comunicare.
 - Aggiornare Inventario (Allegato A) con condizioni.
 - Accessi: preferire tenant istituzionale (per esempio, l'account collegato al dominio di istituto); SSO (ad esempio: accedere con Google) solo per servizi autorizzati; niente account personali per attività d'Istituto.

FRIA: che cos'è e quando serve

FRIA significa Valutazione d'Impatto sui Diritti Fondamentali. Descrive come un sistema di IA può incidere sui diritti delle persone (es. non discriminazione, tutela dei minori, trasparenza) e le misure per prevenire o ridurre i rischi.

Nota pratica: con gli usi previsti in Istituto (IA come supporto a bozze, sintesi, idee e materiali), la FRIA di norma non è necessaria. Diventa necessaria prima del primo utilizzo se la scuola impiega un sistema di IA ad Alto Rischio in ambito istruzione (es. ammissioni/assegnazioni, valutazioni degli esiti che incidono sul percorso, *proctoring*).

Quando è richiesta: prima del primo utilizzo di un sistema di IA ad alto rischio da parte di un soggetto pubblico (come una scuola), secondo AI Act art. 27.

Quando non è richiesta: se lo strumento non ricade nell'alto rischio (es. supporto generico a bozze/sintesi) o se non è usato per decisioni/valutazioni/monitoraggi su persone. In tali casi può essere comunque una buona pratica nei casi borderline.

Esempi rapidi

Esempio A – Bozza di comunicazione

Uso di uno strumento di intelligenza artificiale (es. Google Gemini o Microsoft Copilot) per rendere più chiaro un testo generico.

- Autorizzabile se: strumento autorizzato; **nessun dato personale**; output trattato come bozza.

Esempio B – Correzione/valutazione automatizzata

Software che propone un punteggio o suggerisce un voto.

- Trattare come caso ad attenzione elevata: possibile alto rischio (screening AI Act), di norma vietato da questo Istituto, salvo casi particolari da valutare/normare.

1) Regole pratiche

Testo	
NON inserire mai dati personali di studenti/minori, famiglie o personale nei prompt.	GDPR Art. 5 – Minimizzazione: puoi trattare solo i dati strettamente necessari per lo scopo; quindi niente nomi, cognomi, dettagli identificativi nei prompt se non indispensabili. GDPR Art. 25 – Privacy by design/by default: la scuola deve impostare strumenti e processi in modo che, di default, si usino meno dati possibile e si evitino divulgazioni non necessarie.
NON inserire mai dati sensibili (salute, BES/DSA/PEI, disciplinare, relazioni).	GDPR Art. 9 – Dati particolari: i dati su salute, bisogni educativi, provvedimenti disciplinari ecc. hanno tutele rafforzate e regole più stringenti; in pratica vanno evitati nei prompt e trattati solo con basi giuridiche e garanzie specifiche.
Se devi lavorare con dati o documenti della scuola, <u>usa solo strumenti approvati</u> (Allegato A).	GDPR Art. 28 – Responsabili e contratto: se un fornitore tratta dati per conto della scuola, serve un accordo (DPA) che definisca istruzioni, misure di sicurezza e sub-fornitori. GDPR Art. 32 – Sicurezza: impone misure adeguate (es. controllo accessi, cifratura, log, gestione incidenti). GDPR Art. 44–49 – Trasferimenti extra SEE: se i dati possono uscire dallo Spazio Economico Europeo, servono garanzie specifiche (es. clausole contrattuali standard) e valutazioni del rischio.
Usa l’IA per bozze e supporto; la responsabilità del risultato finale è tua.	GDPR Art. 5 – Accountability: la scuola (e chi opera per essa) deve poter dimostrare di aver rispettato il GDPR; non basta “averci provato”. AI Act art. 14 – Supervisione umana: i sistemi rilevanti (in particolare quelli ad alto rischio) devono essere usati con controllo umano reale: niente “pilota automatico” sulle decisioni.
Verifica sempre: fonti, date, riferimenti normativi, numeri, nomi, istruzioni operative.	GDPR Art. 5 – Esattezza: i dati devono essere corretti e aggiornati; se usi output con errori (nomi, date, numeri) rischi trattamenti inesatti e decisioni sbagliate. AI Act art. 13 – Trasparenza: richiede che l’utente abbia informazioni utili per capire limiti e uso corretto del sistema; in pratica: devi interpretare criticamente l’output e non fidarti alla cieca.

Se hai dubbi, usa una forma anonima o chiedi indicazioni (DSGA/DPO/Referente IA).	GDPR Art. 24 – Responsabilità del titolare: la scuola deve organizzare regole e controlli per garantire conformità; chiedere indicazioni interne fa parte di questo presidio. GDPR Art. 39 – Compiti del DPO: il DPO informa e fornisce consulenza su GDPR, controlla l’osservanza e supporta nelle valutazioni; quindi è il canale corretto in caso di incertezza. Ai Act – Art. 4: impone a chi usa un sistema di IA nell’organizzazione, quindi anche una scuola, di adottare misure per garantire un livello adeguato di competenza sull’IA
Dichiara quando un contenuto è stato creato o rielaborato con IA (materiali didattici, comunicazioni, immagini, audio/video). Se usi un chatbot con studenti, rendi chiaro che stanno interagendo con un sistema di IA quando non è ovvio.	Ai Act – Art. 50: La trasparenza riduce inganni/ambiguità e rende l’uso dell’IA “tracciabile” e comprensibile per studenti e famiglie (accountability e correttezza dei comportamenti).
Mai decisioni importanti “solo IA”: non usare output IA per valutazioni, voti, sanzioni o decisioni che incidono significativamente sullo studente senza un controllo umano reale e motivato.	GDPR Art. 22 - Protegge studenti e famiglie da decisioni opache o errate; impone che le scelte che incidono in modo significativo non siano lasciate a processi automatizzati senza intervento umano. Ai Act art. 14: Stabilisce che sistemi Ai devono essere progettati per garantire che possano essere supervisionati da persone durante l’utilizzo.
Se per errore inserisci o condividi dati personali in uno strumento IA non autorizzato (o noti accessi anomali), segnala subito a DSGA/DPO/dirigente come possibile data breach.	GDPR Artt. 33,34 – si impone al titolare di notificare la violazione di dati personali al Garante il prima possibile e impone di informare anche gli interessati quando la violazione può comportare un rischio elevato per i loro diritti e le loro libertà.

Come anonimizzare correttamente e login

Sostituisci sempre i riferimenti identificativi con etichette generiche. Quando fai login in una app esterna non inclusa tra i servizi autorizzati **non accedere tramite SSO** (ad esempio: alla richiesta “accedi tramite Google” non accettare, ma crea un nuovo account anche con mail istituzionale, ma con nuova password).

Esempi
NO “Mario Rossi (classe 2B) ha DSA e necessita di...” → SI “Studente [S1] (classe [2B]) necessita di misure...”
NO “La madre di Giulia Bianchi ha chiesto...” → SI “Un genitore ha richiesto...”
NO “Invio verbale CdC del 12/11” → SI “Riassumi questa decisione (testo senza nomi e dettagli identificativi)...”
NO Login su app terza con “Accedi con Google/Microsoft” (SSO) → SI Registrazione/login con email come username e creazione di una password nuova e dedicata per quel servizio (non riutilizzata)

Gestione degli account e degli accessi

La seguente sezione disciplina le modalità obbligatorie di accesso ai servizi digitali per tutelare la privacy degli studenti.

A) PIATTAFORME ISTITUZIONALI ("I BIG")

- Strumenti: Google Workspace for Education, Microsoft 365, Canva for Education.
- Procedura: Gli utenti della scuola accedono autonomamente utilizzando le proprie credenziali istituzionali personali (es. nome.cognome@scuolalocate.edul.it).
- Motivazione: Con questi fornitori la Scuola ha sottoscritto un contratto specifico (DPA) che garantisce la protezione dei dati e impedisce la profilazione commerciale.

B) TUTTE LE ALTRE APPLICAZIONI (APP TERZE)

- Strumenti: Solo a titolo di esempio, Kahoot, Duolingo, Scratch, Padlet, Edpuzzle, Panquiz e qualsiasi altro software didattico online.
- Divieto: È VIETATO chiedere agli studenti di registrarsi autonomamente (**Sign Up**) a questi servizi, né utilizzando l'email istituzionale né quella personale, salvo diversa indicazione.
- Procedure obbligatorie (Alternative):
 1. Modalità "Account Classe" (Consigliata): Il docente crea e gestisce una classe virtuale dal proprio pannello di controllo, generando per gli studenti utenze anonime o pseudonimizzate (senza uso di email).
 2. Accesso via Codice/PIN: Lo studente partecipa all'attività inserendo un codice di gioco o cliccando su un link temporaneo fornito dal docente, senza effettuare alcuna registrazione o login.

Checklist prima di usare un LLM (o un servizio di intelligenza artificiale)

Domanda
a) Sto inserendo dati personali o sensibili?
b) Sto usando un account/strumento approvato dall'Istituto?
c) L'obiettivo è una bozza generica o una decisione su persone?
d) Posso ottenere lo stesso risultato senza incollare contenuti riservati?
e) Ho previsto una revisione/approvazione (se comunicazione ufficiale)?

Come richiedere la valutazione di una nuova app/servizio con IA

Se desideri utilizzare una app o un software che include funzioni di IA (anche "*dietro le quinte*"), prima verifica se è già presente nell'Inventario (Allegato A del Regolamento). Se non è presente, segui questi passaggi essenziali:

Compila il modulo interno "Richiesta valutazione app" su www.easyteam.org . Una volta compilato il modulo, si valuterà, in accordo con il Referente dell'Istituto e con gli organismi preposti al controllo, l'ammissione della app indicate/proposta nella lista dei software consentiti.
Attendi l'esito della valutazione (Ammesso / Non ammesso) e consulta le eventuali condizioni operative pubblicate nell'Inventario (Allegato A).
Fino alla decisione, l'uso è consentito solo nell'ambito di sperimentazioni formalmente autorizzate ed esclusivamente con contenuti fittizi o anonimizzati, senza documenti riservati della scuola.

Verifica qualità e responsabilità

Non dare per vere le risposte: l'IA può sbagliare (date, norme, citazioni, numeri).
Per documenti ufficiali: controllo umano +, se necessario, verifica con fonti istituzionali.
Non utilizzare output IA per valutazioni, diagnosi o decisioni su singoli studenti.

Conservazione e archiviazione dell'output

Salva solo l'output necessario nei sistemi documentali della scuola (es. Drive/SharePoint) secondo le regole interne.
Evita di archiviare log/chat non necessari; se lo strumento salva cronologia, attenersi alle impostazioni approvate.
Etichetta i documenti: bozza / revisione / app

Cosa fare in caso di errore (es. dato personale nel prompt)

Interrompi l'attività e non riutilizzare la conversazione.
Avvisa subito DS/DSGA e DPO secondo canale interno (email/ticket/telefono).
Indica: strumento usato, data/ora, tipo di dato inserito, eventuale output generato, azioni già fatte.
Segui le istruzioni ricevute (contenimento, eventuale richiesta log, comunicazioni).

Esempi pratici (casi tipici) e cosa fare

Gli esempi di seguito aiutano a riconoscere situazioni rischiose (specie quando un servizio può usare i contenuti per finalità proprie, es. addestramento/training) e indicano le azioni corrette.

Esempio A – Docente incolla un PEI/PDP o una relazione nominativa in un'IA “gratuita/consumer”

Rischio	Cosa fare
a) Rischio: dati particolari (salute/BES/DSA/PEI) e dati di minori inseriti in un servizio non governato dall'Istituto; possibile conservazione della chat e/o riuso per finalità del fornitore.	b) Cosa fare subito: a) interrompere l'attività e non proseguire nella stessa conversazione; b) non copiare ulteriormente dati nel servizio; c) segnalare immediatamente a DS/DSGA e DPO, indicando strumento, data/ora e tipo di dato; d) seguire le istruzioni di contenimento (es. chiusura sessione, raccolta evidenze). c) Cosa fare per lavorare correttamente: usare solo strumenti autorizzati e, comunque, operare sempre su contenuti anonimizzati (es. “Studente SI”) e senza dati particolari.

Esempio B – Strumento di “correzione/scrittura” che dichiara di usare i testi per migliorare il servizio/modello

Rischio	Cosa fare
a) Rischio: i temi/elaborati o documenti di lavoro possono essere riutilizzati dal fornitore (finalità proprie). In questo caso lo strumento non è idoneo per dati della scuola.	b) Cosa fare: a) non utilizzare lo strumento con elaborati reali o documenti scolastici; b) richiedere/valutare una versione istituzionale che preveda controllo amministrativo, opzioni di esclusione dal training e accordi adeguati; c) in assenza di tali garanzie, consentire solo uso con testi generici o completamente anonimi.

Esempio C – Attività didattica che richiede l’accesso a YouTube/Maps/Search con account personale

Rischio	Cosa fare
a) Rischio: tracciamento e raccolta dati in ambito “consumer”, mancanza di governance dell’Istituto.	b) Cosa fare: a) evitare di richiedere/condizionare l’attività al login con account personale; b) preferire fruizione senza account (quando possibile) e con impostazioni che minimizzino la personalizzazione; c) prevedere alternative equivalenti per chi non intende usare servizi consumer.

Esempio D – Piattaforma che propone “analytics/benchmark” e chiede di riutilizzare dati (anche aggregati) per proprie analisi

Rischio	Cosa fare
a) Rischio: comunicazione di dati a un soggetto che può agire come titolare (o contitolare) per finalità proprie; possibili ulteriori valutazioni (base giuridica, trasparenza, trasferimenti, rischio).	b) Cosa fare: a) non attivare/aderire senza valutazione preliminare (Sez. 6) e senza autorizzazione; b) chiedere chiarimenti sul ruolo del fornitore e sulle finalità; se non è “per conto” della scuola, lo strumento è in genere non ammesso per dati di studenti; c) se l’uso è ritenuto necessario, attivare le tutele contrattuali e informative appropriate e documentare le valutazioni.

Regola pratica: se un servizio dichiara (nei termini o nelle impostazioni) che i contenuti inseriti possono essere conservati e/o usati per training o altre finalità proprie, non deve essere utilizzato con dati o documenti della scuola; è ammesso solo con contenuti anonimi o con una versione istituzionale autorizzata dall’Istituto.

Uso di dispositivi personali (BYOD): condizioni minime

Condizione	Indicazione operativa
Account istituzionale	Accedere allo strumento esclusivamente con account/canali autorizzati dall'Istituto.
Dispositivo protetto e aggiornato	Sistema operativo e applicazioni aggiornati; protezioni attive (es. blocco schermo, forte raccomandazione antivirus/EDR se previsto).
Divieto di salvataggio locale di contenuti riservati	Evitare di scaricare/salvare su dispositivo personale documenti/output con informazioni riservate o non pubbliche.
Divieto di inserire dati personali nei prompt	Non inserire nei prompt dati personali, dati sensibili o documenti contenenti tali informazioni.

In mancanza anche di una sola condizione, l'uso BYOD per attività con IA non è autorizzato.

Credenziali e informazioni di sicurezza: mai nei prompt

Divieto assoluto di inserire nei prompt o caricare su piattaforme IA:

Esempi (non esaustivi)
Password, PIN, codici di recupero, token, chiavi API.
Credenziali di accesso a servizi scolastici o di terzi (registro, piattaforme, servizi cloud).
Link riservati (es. URL con parametri di accesso o condivisioni non pubbliche).
Dettagli tecnici o procedure di sicurezza che possano compromettere sistemi o infrastrutture.
Qualsiasi informazione che consenta a terzi di autenticarsi o ottenere accesso non autorizzato.

Trasparenza verso famiglie/studenti: chatbot e canali esterni

In caso di utilizzo di chatbot o assistenti IA su sito web, canali di comunicazione, sportelli digitali o altri contesti rivolti a utenti esterni, applicare almeno le seguenti misure:

Requisito	Operatività minima
Avviso di uso IA	Informare in modo chiaro che l'utente sta interagendo con un sistema di IA.
Canale umano alternativo	Indicare e mantenere disponibile un canale di contatto umano (email/telefono/sportello).
Divieto dati sensibili	Inserire messaggi che invitano a non comunicare dati sensibili; evitare campi che inducano l'inserimento di tali dati.
Escalation/istradamento	Prevedere il passaggio a operatore in caso di richieste non gestibili, ambigue o di particolare delicatezza.
Revisione periodica	Rivedere periodicamente risposte/FAQ e aggiornare in base a errori riscontrati e cambiamenti del servizio.

Misure minime di sicurezza per il personale (uso quotidiano)

Misura	Esempio/nota
Autenticazione forte (se disponibile)	Abilitare MFA/2FA (autenticazione a due fattori) sugli account utilizzati.
Blocco schermo	Bloccare il dispositivo quando non presidiato (automatico e manuale).
Aggiornamenti	Mantenere aggiornati sistema operativo, browser e applicazioni.
Protezione endpoint	Forte raccomandazione antivirus/EDR secondo le dotazioni e indicazioni dell'Istituto.
Gestione file	Evitare copie locali non necessarie; usare canali/archivi istituzionali secondo indicazioni.

Equità, non discriminazione e accessibilità: regole operative essenziali

Regola	Indicazione
Controllo <i>bias</i> e linguaggio	Verificare che l'output non introduca stereotipi, discriminazioni o formulazioni inadeguate.
Alternativa equivalente	Prevedere sempre un'alternativa equivalente non basata su strumenti consumer/IA, quando necessario per inclusione e accessibilità.

Riesame e aggiornamenti: quando segnalare e attivare la valutazione

Segnalare al referente interno/Dirigenza la necessità di aggiornare inventario/valutazioni/istruzioni operative quando si verifica almeno una delle seguenti condizioni:

Casi tipici
Introduzione di un nuovo strumento o nuova funzionalità IA per attività didattiche o amministrative.
Modifica dei Termini di Servizio, impostazioni di privacy, modalità di conservazione dei dati o uso per training.
Episodi/incidenti (anche potenziali) legati a data breach, inserimento accidentale di dati personali o output anomali.
Cambiamenti organizzativi o procedurali che impattano ruoli, responsabilità o flussi di approvazione.