Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO STATALE "*VIA DEI SALICI*"
Via A. Robino 25/A – 20025 Legnano
Tel: 0331 541316
Cod.mec.MIIC85500G – C.F- 84003710153
e-mail: miic85500g@istruzione.it
e-mail: miic85500g@pec.istruzione.it

Allegato B - Mappa rapida dei documenti dell'Istituto

Documento	A cosa serve	Quando lo richiamo
Regolamento/Policy 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, Istruzioni operative e formazione	Regole pratiche, esempi, procedure (account, incidenti).	Per standardizzare l'uso quotidiano e la formazione.
DPIA AI (se applicabile)	Valuta rischi privacy legati alle funzioni IA.	Quando si trattano dati di minori, dati particolari o su larga scala.
PUIA	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 digitale:** 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 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 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.
- Di norma NON alto rischio: bozze, traduzioni, sintesi, esercizi generici (sempre con verifica umana).

4. Se è alto rischio: presìdi rafforzati (e FRIA).

- 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-check, dati).

7. Formalizzare e comunicare.

- Aggiornare Inventario (Allegato A) con condizioni.
- Accessi: preferire tenant istituzionale; 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 un LLM 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, usa solo strumenti approvati (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,	**Ai Act – Art. 50:** La trasparenza riduce inganni/ambiguità e rende l'uso dell'IA "tracciabile" e comprensibile per studenti e

audio/video). Se usi un chatbot con studenti, rendi chiaro che stanno interagendo con un sistema di IA quando non è ovvio.	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 secondo la procedura interna (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 possible e impone di informare anche gli interessati quando la violazione puo 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 un'app esterna non inclusa tra i servizi autorizzati non accedere tramite SSO (ad esempio: alla richiesta "accedi tramite google" non accettare, ma creare nuovo account anche con mail istituzionale, ma con nuova password).

Esempi
❌ "Mario Rossi (classe 2B) ha DSA e necessita di…" → ✅ "Studente [S1] (classe [2B]) necessita di misure…"
❌ "La madre di Giulia Bianchi ha chiesto…" → ✅ "Un genitore ha richiesto…"
❌ "Invio verbale CdC del 12/11" → ✅ "Riassumi questa decisione (testo senza nomi e dettagli identificativi)…"
❌ Login su app terza con "Accedi con Google/Microsoft" (SSO) → ✅ 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 studenti accedono autonomamente utilizzando le proprie **credenziali istituzionali personali** (es. *nome.cognome@scuola.edu.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

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 un'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 i referenti IA 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 S1") 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 minimizzano la personalizzazione; c) prevedere alternative equivalenti per chi non intende usare servizi consumer.

Esempio D – Piattaforma che propone "analytics/benchmark" e chiede di riusare 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.

INTEGRAZIONI PER COERENZA CON REGOLAMENTO D'ISTITUTO (AI)

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 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 bias 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.