ISTITUTO COMPRENSIVO STATALE "SILVIO PELLICO"
20004 ARLUNO (MI) – Piazza Europa, 9
Codice Meccanografico MIIC860003 *Cod. Fiscale* 93527540152
Tel.029017001 - Fax 02 90376792
Sito Web: www.icspellico.edu.it - *E-mail*:MIIC860003@istruzione.it;
Posta certificata: MIIC860003@pec.istruzione.it

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. Ai sensi dell'AI Act, i sistemi di intelligenza artificiale possono presentare un livello di rischio inaccettabile, elevato, limitato o minimo. I sistemi a rischio inaccettabile sono vietati; quelli ad alto rischio sono ammessi solo nel rispetto di obblighi stringenti di conformità, controllo e tutela dei diritti. I sistemi a rischio limitato richiedono principalmente misure di trasparenza verso gli utenti, mentre quelli a rischio minimo sono generalmente utilizzabili nel rispetto delle regole interne dell'Istituto, della normativa vigente e dei principi di correttezza, sicurezza e protezione dei dati.

> ***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, assistente tecnico, 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 o applicazioni o software non autorizzati è vietato l'accesso tramite SSO ("Sistema che permette di accedere direttamente con Google o equivalenti) e l'uso

ISTITUTO COMPRENSIVO S.PELLICO - C.F. 93527540152 C.M. MIIC860003 - A3C0BBE - ISTITUTO COMPRENSIVO SILVIO PELLICO ARLUNO
Prot. 0006734/U del 12/11/2026 20:07:17 - Norme e disposizioni attuative

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 (ad esempio per il testing di applicazioni non ancora in elenco).

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

L'impiego dell'intelligenza artificiale nell'Istituto deve avvenire nel rispetto di finalità educative, inclusive e di sviluppo della persona, quale strumento di supporto alla personalizzazione degli apprendimenti, alla valorizzazione delle inclinazioni individuali, al sostegno delle fragilità cognitive e di apprendimento e alla promozione della cittadinanza digitale. L'IA non costituisce una persona né una fonte autonoma e autorevole di conoscenza: i suoi contenuti devono essere sempre verificati criticamente, corredati ove possibile da fonti e bibliografia, e non devono sostituire il giudizio umano, la relazione educativa, lo studio autonomo e la progressiva acquisizione delle competenze. L'Istituto promuove pertanto un uso consapevole, proporzionato e responsabile di tali strumenti, tenendo conto anche del loro impatto ambientale e del rischio di dipendenza o di impoverimento delle capacità cognitive nel lungo periodo.

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

b) Minimizzazione: usare il minimo di informazioni possibile (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).

l) Supporto alla didattica laboratoriale interattiva anche con quiz e giochi.

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'accesso con le credenziali dell'Istituto (account di dominio) e con sistemi di autenticazione SSO, quali "Accedi con Google", "Accedi con Microsoft" o equivalenti, è consentito esclusivamente per i servizi espressamente indicati nella DPIA e nel relativo Allegato 1: Google Workspace for Education, Microsoft app and services / Office 365 e Canva for Education.

Per qualunque altro servizio, anche se incluso nell'Allegato A delle applicazioni e dei software autorizzati, occorre attendere la preventiva autorizzazione dell'amministratore della piattaforma, inteso come il soggetto incaricato dall'Istituto della gestione tecnica degli account, delle autorizzazioni di accesso e delle configurazioni di sicurezza dei servizi digitali.

L'eventuale registrazione con email istituzionale come semplice nome utente è consentita solo alle seguenti condizioni:

a- senza utilizzare il login SSO;

b- con una password dedicata, diversa da quella istituzionale;

c- senza inserire dati personali;

d- senza caricare materiali scolastici.

L'utente, docente o altro dipendente dell'Istituto, è tenuto a utilizzare il proprio account istituzionale esclusivamente su dispositivi assegnati o comunque nella propria esclusiva disponibilità, non condivisi con terzi e adeguatamente protetti.

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

Sono ammessi esclusivamente gli strumenti indicati nell'Inventario d'Istituto (Allegato A), preferibilmente utilizzati con account istituzionali o con modalità espressamente autorizzate. È ammesso l'uso di account personali su dispositivi dell'Istituto esclusivamente per attività di supporto generico (es. idee, bozze, riformulazioni) con contenuti anonimi e non riconducibili alla scuola o a persone fisiche, nel rispetto dei divieti di cui alla sezione "Usi vietati". *Resta preferibile, ove disponibile*, l'uso di versioni/tenant istituzionali con controllo amministrativo. 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) Uso improprio e misure correttive e disciplinari

L’utilizzo di sistemi di intelligenza artificiale in difformità dalle disposizioni del presente Regolamento, delle istruzioni impartite dall’Istituto, delle misure di sicurezza adottate e, ove applicabile, della Valutazione d’Impatto sulla Protezione dei Dati (DPIA), costituisce uso improprio. In tali casi l’Istituto adotta misure correttive e, ove ne ricorrano i presupposti, attiva i procedimenti disciplinari previsti dalla normativa vigente, dal Regolamento di disciplina d’Istituto, dal Patto educativo di corresponsabilità e dalle disposizioni applicabili al personale scolastico. Le misure sono determinate secondo criteri di proporzionalità, gradualità, responsabilità e finalità educativa, tenendo conto della gravità del comportamento, dell’intenzionalità, della reiterazione, della natura dei dati eventualmente coinvolti, del danno o del rischio arrecato a studenti, famiglie, personale o terzi, nonché dell’eventuale omessa vigilanza o mancata supervisione umana. Per gli studenti possono essere adottati, in relazione alla gravità del fatto, provvedimenti quali richiamo, annotazione disciplinare, annullamento della prova o valutazione negativa nei casi consentiti, nonché ulteriori misure previste dal Regolamento di disciplina; per il personale restano ferme le responsabilità disciplinari, organizzative, amministrative e, ove ne ricorrano i presupposti, civili, penali e in materia di protezione dei dati personali. Resta in ogni caso fermo che l’utilizzo dell’intelligenza artificiale non esonera l’autore dell’attività dalla piena responsabilità del contenuto prodotto, delle decisioni assunte e degli effetti che ne derivano.

- 9.1 Gestione incidenti

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 periodico 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, rivolgendomi al Team Referente.

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, direttamente al Team Referente (o all'animatore digitale o ad incaricato dal Team). L'incaricato del Team Referente, in accordo con i consulenti nominati (esterni o interni) valuterà l'ammissibilità della/e app proposta/a. In caso di ammissione verrà aggiornato l'Allegato A e inviato all'Istituto, in particolare all'incaricato del Team, il quale consegnerà il documento aggiornato per la conservazione.

13) Studenti, famiglie 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). Gli studenti possono utilizzare strumenti di intelligenza artificiale esclusivamente per finalità didattiche, sotto la guida del docente e nel rispetto del presente Regolamento, della normativa vigente, della tutela della privacy, della sicurezza dei dati e del sistema informatico dell'Istituto, anche quando l'utilizzo avvenga al di fuori dei plessi scolastici. L'uso dell'IA deve avere finalità di supporto all'apprendimento, alla comprensione, al brainstorming, al miglioramento del lavoro svolto e allo sviluppo del pensiero critico, della curiosità e della capacità di verificare l'affidabilità delle fonti; resta invece vietato utilizzarla in modo fraudolento, per aggirare i processi di valutazione, per

automatizzare integralmente compiti, elaborati o verifiche senza espressa autorizzazione del docente, nonché per presentare come interamente originali contenuti generati con il suo ausilio. Lo studente è tenuto a verificare criticamente gli output ricevuti, a rispettare il diritto d'autore e le norme sulla proprietà intellettuale, a dichiarare in modo trasparente l'eventuale contributo significativo dell'IA nei propri elaborati, a formulare richieste chiare e pertinenti secondo le indicazioni dei docenti e a segnalare tempestivamente eventuali risposte errate, incoerenti o fuorvianti. L'uso diretto degli strumenti di IA da parte degli studenti deve inoltre avvenire nel rispetto dei limiti di età previsti dai fornitori e dalla normativa vigente; gli studenti non possono utilizzare tali strumenti né cedere propri dati personali senza l'autorizzazione di chi esercita la responsabilità genitoriale e, per gli studenti minorenni, l'utilizzo è subordinato alla preventiva autorizzazione o liberatoria dei genitori o tutori. I genitori o tutori esercitano un ruolo di supervisione sull'uso degli strumenti di IA da parte dei minori al di fuori dell'ambito scolastico e sono invitati a partecipare alle iniziative formative promosse dall'Istituto; tali impegni si raccordano con il Patto educativo di corresponsabilità e concorrono allo sviluppo delle competenze di cittadinanza digitale.



Firmato digitalmente da:
La Dirigente Scolastica
Prof.ssa Alessandra Sebastiani