

PRIVACY SCUOLA 2026

REGOLAMENTO DI ISTITUTO PER L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

Governance, didattica, amministrazione, privacy, sicurezza e supervisione umana

Istituto: Istituto d'Istruzione Superiore Secondaria Statale "Eugenio Pantaleo" - Codice meccanografico: NAIS12800T -
Sede: Via Cimaglia, 96 - 80059 Torre del Greco (NA) - Dirigente: Giuseppe Mingione - Data: 25/09/2026

Premessa

L'Intelligenza Artificiale può migliorare insegnamento, apprendimento, inclusione, accessibilità, organizzazione e servizi amministrativi, ma richiede una governance preventiva, responsabilità umana effettiva e controlli proporzionati ai rischi. Il presente Regolamento disciplina l'uso dei sistemi di IA nell'Istituto, compresa l'IA generativa, e si coordina con i documenti del Kit Base relativi a personale, studenti, fornitori, sicurezza, data breach, diritti degli interessati e valutazione dei rischi.

L'Istituto opera, quando utilizza sistemi di IA sotto la propria autorità, quale deployer ai sensi del Regolamento (UE) 2024/1689, ferme le diverse qualificazioni che possono derivare dal singolo caso concreto. L'IA è sempre strumento di supporto: non sostituisce l'autonomia professionale, pedagogica, amministrativa o decisionale dei soggetti competenti.

Riferimenti normativi e istituzionali essenziali

- Regolamento (UE) 2024/1689 (AI Act), secondo il calendario di applicazione e le disposizioni di volta in volta pertinenti;
- Regolamento (UE) 2016/679 (GDPR) e d.lgs. 196/2003, come modificato dal d.lgs. 101/2018;
- Legge 23 settembre 2025, n. 132, per le disposizioni applicabili all'istruzione e alla pubblica amministrazione;
- Linee guida MIM per l'introduzione dell'Intelligenza Artificiale nelle istituzioni scolastiche, allegate al D.M. n. 166 del 9 agosto 2025;
- Codice dell'Amministrazione Digitale, normativa scolastica, disciplina sulla sicurezza informatica, tutela dei minori, diritto d'autore e ulteriori norme applicabili al caso concreto.

Art. 1 - Oggetto e finalità

- promuovere un uso antropocentrico, sicuro, affidabile, etico, trasparente e responsabile dell'IA;
- favorire innovazione, qualità didattica, inclusione e semplificazione amministrativa senza delegare alla tecnologia responsabilità proprie delle persone;
- proteggere dignità, autonomia, diritti fondamentali e pari opportunità, con particolare attenzione ai minori e ai soggetti vulnerabili;
- stabilire un unico processo di autorizzazione, inventario, monitoraggio, sospensione e riesame dei sistemi IA;
- definire regole chiare per personale, studenti, fornitori, strumenti, dati, contenuti e incidenti.

Art. 2 - Ambito di applicazione

Il Regolamento si applica al Dirigente scolastico, DSGA, personale docente e ATA, studenti, esperti, collaboratori, tirocinanti, consulenti, fornitori e ad ogni soggetto che utilizzi IA per attività riconducibili all'Istituto. Si applica a sistemi istituzionali, servizi cloud, chatbot, copilot, agenti, modelli generativi, plugin, estensioni, API e funzioni IA incorporate in software già in uso.

L'uso personale e privato estraneo all'attività scolastica resta fuori dal presente Regolamento, ma non può essere confuso con attività istituzionali né comportare l'inserimento di dati, documenti o contenuti dell'Istituto in strumenti non autorizzati.

Art. 3 - Definizioni essenziali

Termine	Definizione
Sistema di IA	Sistema basato su macchina che, per obiettivi espliciti o impliciti, produce previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.
IA generativa	Sistema capace di generare testi, immagini, audio, video, codice o altri contenuti a partire da istruzioni o dati di ingresso.
Deployer	Soggetto che utilizza un sistema di IA sotto la propria autorità, salvo gli usi personali non professionali previsti dalla normativa.
Caso d'uso	Finalità concreta per cui un sistema IA viene impiegato, con utenti, dati, output e impatti definiti.
Referente IA	Funzione organizzativa eventualmente individuata tramite PS26-GOV-09 per coordinare la governance IA, senza poteri decisionali autonomi.
PUIA	Piano e Strategia di Istituto per l'adozione dell'IA di cui a PS26-IA-02, se formalmente adottato.

Art. 4 - Principi generali

- centralità della persona e supervisione umana effettiva;

- finalità istituzionale chiara, necessità e proporzionalità;
- protezione dei dati, minimizzazione e privacy by design/by default;
- accuratezza, qualità, verifica delle fonti e contestualizzazione degli output;
- equità, non discriminazione e prevenzione dei bias;
- sicurezza, resilienza, controllo degli accessi e tracciabilità proporzionata;
- trasparenza verso gli interessati e comprensibilità delle regole d'uso;
- responsabilità: chi utilizza l'IA resta responsabile del risultato finale che adotta, comunica, valuta o firma.

Art. 5 - Governance dell'IA e ruolo dell'Istituto quale deployer

Il Dirigente scolastico esercita la governance complessiva dell'uso istituzionale dell'IA. L'Istituto adotta un approccio per casi d'uso: non è sufficiente che uno strumento sia tecnicamente disponibile; deve essere autorizzato per la finalità concreta e per le categorie di dati effettivamente trattate.

La governance si fonda almeno su valutazione preventiva, inventario dei sistemi IA, gestione delle autorizzazioni, formazione, supervisione umana, monitoraggio, gestione incidenti e riesame periodico. Se individuato, il Referente IA coordina i flussi previsti da PS26-GOV-09. Il DPO/RPD è coinvolto tempestivamente per i profili di protezione dati, senza assumere compiti decisionali o tecnici propri del Titolare, del DSGA o delle funzioni ICT.

Art. 6 - Ecosistema digitale autorizzato e inventario degli strumenti IA

- per attività istituzionali si utilizzano prioritariamente strumenti compresi nell'ecosistema digitale autorizzato e, ove disponibili, account istituzionali gestiti centralmente;
- l'Istituto mantiene aggiornato PS26-GEN-06 con sistemi, finalità, utenti, stato di autorizzazione, fornitore, principali dati trattati e data di riesame;
- è vietato utilizzare account personali per trattare dati o documenti dell'Istituto quando il servizio non è stato espressamente autorizzato per tale finalità;
- non è ammessa l'attivazione autonoma di plugin, agenti, estensioni o connettori che accedano a Drive, posta elettronica, registro elettronico, archivi, rete o altri sistemi istituzionali;
- il Dirigente può sospendere o limitare uno strumento o una funzione IA in caso di rischio, modifica contrattuale, vulnerabilità, non conformità o perdita delle condizioni di autorizzazione.

Art. 7 - Procedura preventiva per nuovi sistemi e nuovi casi d'uso

1. Definire bisogno, finalità, utenti, dati, output, integrazioni e impatti previsti.
2. Effettuare test iniziali con dati fittizi, sintetici o adeguatamente anonimizzati, salvo autorizzazione espressa per dati reali.

3. Compilare PS26-GEN-03 prima dell'attivazione stabile o dell'uso con dati reali/account istituzionali.
4. Verificare fornitore, DPA/ruoli privacy, subfornitori, trasferimenti, tempi di conservazione, sicurezza, uso dei dati per training e condizioni contrattuali.
5. Aggiornare PS26-GEN-06.
6. Se emergono indicatori di rischio elevato, utilizzare PS26-RSK-02 e, quando necessario, avviare DPIA e ulteriori valutazioni richieste dalla normativa.
7. Richiedere il parere del DPO/RPD tramite PS26-GOV-03/04 quando il caso presenta profili privacy rilevanti.
8. Formalizzare la decisione del Dirigente/Titolare con condizioni, utenti autorizzati, limiti, formazione e data di riesame.

Art. 8 - Ruoli e responsabilità

Soggetto	Responsabilità essenziali
Dirigente scolastico / Titolare	Indirizzo, autorizzazione, accountability, sospensione, decisioni finali e adozione delle misure organizzative.
DSGA	Coordinamento degli impieghi amministrativi e organizzativi nei limiti delle proprie competenze.
Referente IA, se individuato	Coordinamento dei casi d'uso, supporto a GEN-03/GEN-06/PUIA, formazione e monitoraggio; nessun potere autorizzativo autonomo.
RPD/DPO	Informazione, consulenza e sorveglianza sui profili privacy; pareri su rischi, DPIA, minori e trattamenti rilevanti. Non è approvatore operativo.
Amministratore di sistema / ICT / RTD	Configurazione tecnica, accessi, integrazioni, logging, sicurezza e supporto tecnico secondo le competenze e istruzioni ricevute.
Docenti	Responsabilità pedagogica, definizione delle consegne, verifica degli output, supervisione degli studenti e valutazione umana.

Soggetto	Responsabilità essenziali
Personale ATA	Uso solo per compiti autorizzati, controllo degli output e rispetto delle regole su dati e documenti.
Studenti	Uso secondo consegne, integrità didattica, protezione dei dati e rispetto delle regole di istituto.
Fornitori	Adempimenti contrattuali e normativi, sicurezza, trasparenza e garanzie coerenti con il ruolo effettivo.

Art. 9 - Alfabetizzazione e formazione in materia di IA

L'Istituto adotta misure per assicurare, in misura adeguata ai ruoli, alle conoscenze e al contesto d'uso, un livello sufficiente di alfabetizzazione IA del personale e delle persone che operano sui sistemi per suo conto. La formazione comprende funzionamento e limiti, allucinazioni, bias, privacy, cybersecurity, proprietà intellettuale, trasparenza, integrità didattica, pratiche vietate e supervisione umana.

Per sistemi con accesso a dati reali, funzioni amministrative, valutazioni, integrazioni o rischi elevati, l'abilitazione può essere subordinata al completamento della formazione prevista dall'Istituto. Le attività e le prese visione rilevanti sono registrate in PS26-GOV-08.

Art. 10 - Utilizzo da parte del personale docente

Il docente mantiene piena responsabilità su correttezza, adeguatezza all'età, inclusività, coerenza disciplinare e decisioni didattiche. L'output dell'IA non costituisce fonte autorevole per il solo fatto di essere generato da un sistema tecnologico. Si applica anche PS26-PER-05.

- progettazione didattica, brainstorming, esempi, esercizi, quiz, rubriche, sintesi e traduzioni;
- predisposizione di materiali e attività inclusive, purché non vengano immessi dati personali o particolari in strumenti non autorizzati;
- supporto alla revisione linguistica e alla produzione di bozze;
- analisi orientativa di dati aggregati o anonimizzati;
- supporto alla ricerca e alla preparazione di spiegazioni, con verifica delle fonti e dei contenuti.

Art. 11 - Utilizzo da parte degli studenti

- l'uso dell'IA è consentito nei limiti definiti dal docente e dalla policy PS26-STU-04;
- la consegna del docente prevale e può autorizzare, limitare o vietare l'IA in relazione all'obiettivo formativo;

- lo studente non può presentare come integralmente proprio un lavoro prodotto in misura sostanziale dall'IA quando la consegna richiede elaborazione personale;
- quando richiesto, lo studente indica strumento, finalità e contributo dell'IA e conserva prompt/versioni utili a ricostruire il processo;
- è vietato inserire dati personali propri o altrui, immagini identificative, chat, PEI/PDP, dati sanitari, credenziali o documenti riservati in sistemi non autorizzati;
- l'uso deve sviluppare autonomia, pensiero critico e competenze, non sostituire sistematicamente lo studio o la produzione personale.

Art. 12 - Uso didattico, inclusione e personalizzazione

L'IA può supportare personalizzazione, accessibilità e inclusione solo se le scelte restano comprensibili e governate dal docente. Per studenti con disabilità, DSA/BES o altre esigenze educative, l'uso di IA non autorizza l'inserimento di diagnosi, PEI/PDP o informazioni sanitarie in servizi esterni non valutati.

Se un sistema utilizza profili individuali, dati comportamentali, dati particolari o inferenze per adattare il percorso educativo, deve essere sottoposto a valutazione preventiva rafforzata, con coinvolgimento del DPO/RPD e verifica dell'eventuale necessità di DPIA o della disciplina sui sistemi ad alto rischio.

Art. 13 - Valutazione, verifiche e integrità scolastica

- la valutazione formativa e sommativa resta responsabilità esclusiva del docente;
- un sistema IA non può essere l'unico decisore di voto, giudizio, ammissione, non ammissione, orientamento, sanzione disciplinare o altra decisione significativamente incidente sul percorso dello studente;
- l'IA può proporre feedback, griglie o analisi preliminari solo con verifica umana sostanziale;
- l'uso non autorizzato dell'IA durante prove o compiti è valutato secondo Regolamento d'Istituto e Statuto delle studentesse e degli studenti, privilegiando proporzionalità e finalità educativa;
- sistemi destinati al monitoraggio di comportamenti durante prove, proctoring o rilevazione automatica di condotte vietate richiedono preventiva verifica della disciplina AI Act e privacy.

Art. 14 - Utilizzo nelle attività amministrative e organizzative

- l'IA può supportare bozze di circolari, comunicazioni, verbali, schemi di atti, sintesi, classificazioni e pianificazione, purché l'output sia verificato prima di firma, protocollo, pubblicazione o invio;
- non è consentita l'adozione automatica di provvedimenti o determinazioni che producano effetti giuridici o analogamente significativi su studenti, famiglie, personale o terzi;
- per procedimenti amministrativi, il responsabile umano verifica presupposti, fonti, competenza, motivazione, dati, allegati e conformità normativa;
- l'IA non può essere utilizzata per profilare il personale o gli utenti, assegnare punteggi comportamentali, valutare affidabilità o merito in modo non autorizzato;

- dati contenuti in fascicoli, protocollo, personale, contabilità, inclusione o procedimenti riservati possono essere trattati con IA solo in sistemi previamente autorizzati per quel caso d'uso.

Art. 15 - Protezione dei dati personali e basi giuridiche

La base giuridica non è stabilita una volta per tutte dal presente Regolamento: deve essere individuata per ciascun trattamento e caso d'uso. Per i compiti istituzionali possono ricorrere, a seconda del caso, obbligo legale e/o compito di interesse pubblico; il consenso è utilizzato solo quando il trattamento è realmente facoltativo e la normativa lo rende appropriato.

- nei sistemi non autorizzati è vietato inserire dati personali reali di studenti, famiglie, personale o terzi;
- dati di salute, disabilità, DSA/BES, convinzioni, dati biometrici, giudiziari, disciplinari e altre categorie particolari richiedono presupposti specifici, stretta necessità, misure adeguate e valutazione preventiva;
- le informative sono aggiornate quando l'uso dell'IA introduce nuove modalità di trattamento rilevanti; utilizzare PS26-IA-03 quando pertinente;
- devono essere chiariti ruoli privacy, finalità, dati, destinatari, conservazione, trasferimenti, sub-responsabili e diritti degli interessati;
- per test e sperimentazioni si usano di regola dati fittizi, sintetici o anonimizzati.

Art. 16 - Minori, soggetti vulnerabili e categorie particolari di dati

Poiché il contesto scolastico coinvolge minori e altri soggetti vulnerabili, ogni nuovo uso IA che incida su apprendimento, inclusione, comportamento, orientamento, valutazione, benessere o accesso a opportunità è sottoposto a particolare cautela. Devono essere evitati design manipolativi, dipendenza indebita, inferenze non necessarie e raccolte eccedenti.

L'assenza di un consenso non rende di per sé illecito un trattamento istituzionale, così come la presenza di un consenso non sana un trattamento sproporzionato o vietato. La liceità è valutata sul caso concreto.

Art. 17 - Pratiche vietate e usi incompatibili

- pratiche vietate dall'art. 5 AI Act, incluse tecniche manipolative o ingannevoli nei casi previsti dalla norma;
- social scoring e classificazioni pregiudizievoli basate su comportamento sociale o caratteristiche personali nei casi vietati;
- categorizzazione biometrica finalizzata a inferire categorie sensibili nei casi vietati;
- riconoscimento o inferenza delle emozioni in ambito scolastico, salvo le eccezioni tassative previste dalla normativa;
- deepfake o contenuti sintetici di persone reali con finalità ingannevoli, offensive, denigratorie, discriminatorie, di molestia o non compatibili con le regole scolastiche;
- uso dell'IA per aggirare sistemi di sicurezza, sottrarre credenziali, creare malware o ottenere accessi non autorizzati;

- uso di strumenti non autorizzati per documenti riservati, fascicoli, credenziali o dati personali reali.

Art. 18 - Sistemi ad alto rischio, DPIA e valutazioni sui diritti fondamentali

Quando un sistema può rientrare tra i sistemi ad alto rischio dell'AI Act, l'Istituto non procede all'uso operativo fino alla verifica della classificazione, degli obblighi del fornitore e del deployer e delle misure richieste. Particolare attenzione è riservata ai sistemi destinati a incidere su accesso/ammissione, assegnazione a percorsi, valutazione dei risultati di apprendimento, determinazione del livello educativo o monitoraggio di comportamenti vietati durante prove, nei casi previsti dall'Allegato III.

Quando ricorrono i presupposti, l'Istituto effettua la DPIA ai sensi del GDPR e, per i sistemi ad alto rischio e i soggetti tenuti, la valutazione d'impatto sui diritti fondamentali prevista dall'AI Act. Le valutazioni possono essere coordinate, ma devono coprire i rispettivi requisiti. Il DPO/RPD fornisce parere nell'ambito delle proprie competenze; la decisione finale resta al Titolare.

Art. 19 - Trasparenza e informazione

- l'Istituto informa in modo chiaro quando l'IA è utilizzata in modo rilevante in un servizio, processo o attività didattica;
- le famiglie e gli studenti ricevono informazioni adeguate all'età e al contesto su finalità, regole, limiti e principali tutele;
- quando il trattamento riguarda dati personali, le informazioni previste dal GDPR sono rese o integrate secondo necessità, anche tramite PS26-IA-03;
- contenuti artificiali o manipolati sono identificati come tali quando necessario a evitare inganno/confusione e nei casi previsti dalla normativa;
- l'uso di IA in un elaborato o materiale può essere dichiarato quando è sostanziale o quando il docente/Istituto lo richiede.

Art. 20 - Sicurezza, account, accessi, API e integrazioni

- utilizzare account istituzionali e profili autorizzati quando previsti;
- non condividere password, MFA, chiavi API, token, segreti, configurazioni riservate o dati di autenticazione nei prompt;
- applicare minimo privilegio e separazione dei ruoli;
- sottoporre a preventiva autorizzazione plugin, estensioni, agenti e connettori con accesso a dati o sistemi istituzionali;
- configurare logging e conservazione dei log in modo proporzionato, senza sorveglianza generalizzata;
- segnalare immediatamente esposizioni di dati, output anomali, compromissioni, accessi impropri o vulnerabilità.

Art. 21 - Fornitori, contratti, training dei modelli e conservazione

- prima dell'adozione si verificano ruolo privacy, DPA, subfornitori, ubicazione dei dati, trasferimenti extra SEE, conservazione, cancellazione, sicurezza, audit e gestione degli incidenti;
- l'uso dei dati scolastici per addestrare, perfezionare o migliorare modelli del fornitore non è ammesso per default: deve essere escluso quando possibile o specificamente valutato e autorizzato se giuridicamente e tecnicamente compatibile;
- quando il servizio lo consente, le funzioni di training sui contenuti dell'Istituto e la conservazione non necessaria delle conversazioni sono disattivate per impostazione predefinita;
- condizioni d'uso consumer o account gratuiti non costituiscono da sole una base sufficiente per trattare dati istituzionali;
- modifiche sostanziali del servizio, del modello, delle finalità o delle condizioni contrattuali determinano riesame dell'autorizzazione.

Art. 22 - Qualità, affidabilità, bias e verifica degli output

- verificare fatti, dati, citazioni, riferimenti normativi, formule, traduzioni e fonti;
- non assumere come esistente una fonte soltanto perché indicata dal sistema;
- controllare errori, allucinazioni, contenuti obsoleti, bias, stereotipi e discriminazioni;
- effettuare revisione umana completa prima di atti ufficiali, comunicazioni esterne, valutazioni o pubblicazioni;
- nelle attività didattiche verificare appropriatezza all'età, correttezza disciplinare, inclusività e coerenza con gli obiettivi formativi.

Art. 23 - Proprietà intellettuale, riservatezza e segreti

- rispettare diritto d'autore, licenze e condizioni d'uso;
- non caricare opere, banche dati, software o materiali protetti/riservati in servizi non autorizzati quando ciò violi diritti o obblighi contrattuali;
- non inserire segreti d'ufficio, dati coperti da riservatezza, documenti non pubblici o informazioni confidenziali in sistemi non autorizzati;
- verificare sempre le citazioni e distinguere contenuti originali, fonti e contributo dell'IA;
- non attribuire a persone reali dichiarazioni, immagini o voci sintetiche in modo ingannevole o lesivo.

Art. 24 - Monitoraggio, controllo e sospensione

L'Istituto assicura monitoraggio continuo e proporzionato dei sistemi autorizzati, senza finalità di sorveglianza generalizzata. Il monitoraggio verifica almeno conformità al caso d'uso, sicurezza, qualità degli output, rispetto delle condizioni contrattuali, permanenza delle garanzie privacy e adeguatezza della supervisione umana.

Il Dirigente può sospendere, limitare o disattivare sistemi o funzionalità, anche cautelativamente, quando emergano criticità significative. Le misure devono essere motivate e proporzionate e, ove possibile, accompagnate da strumenti alternativi per garantire continuità didattica e amministrativa.

Art. 25 - Incidenti, anomalie e data breach

- ogni incidente, perdita, divulgazione, accesso non autorizzato, compromissione di account, output contenente dati inattesi o utilizzo improprio deve essere segnalato senza ritardo tramite PS26-DBR-01;
- se può esservi violazione di dati personali si applica il flusso data breach PS26, inclusa PS26-DBR-03 e il coinvolgimento del DPO/RPD;
- solo il Titolare decide eventuale notifica al Garante o comunicazione agli interessati;
- si preservano evidenze utili e proporzionate: data/ora, sistema, prompt rilevanti, output, screenshot, log, soggetti coinvolti e misure adottate.

Art. 26 - Uso improprio e misure correttive

L'uso difforme dal presente Regolamento, dalle istruzioni interne o dalle condizioni di autorizzazione costituisce uso improprio. Le misure correttive sono graduate in funzione di gravità, intenzionalità, rischio, danno, reiterazione e contesto educativo.

Per il personale si applicano normativa, contratto e regolamenti interni; per gli studenti si applicano Statuto delle studentesse e degli studenti e Regolamento d'Istituto, privilegiando quando possibile interventi educativi e di accompagnamento. L'uso di un sistema IA non esclude né attenua automaticamente la responsabilità personale per gli atti compiuti.

Art. 27 - Entrata in vigore, pubblicazione e aggiornamento

Il Regolamento entra in vigore dalla data indicata nell'atto di adozione ed è comunicato a personale, studenti e famiglie con modalità adeguate ai destinatari. La versione vigente è resa disponibile nei canali istituzionali individuati dall'Istituto.

Il Regolamento è riesaminato almeno annualmente e ogni volta che intervengano modifiche normative, nuove indicazioni MIM, nuovi sistemi IA, cambiamenti dei fornitori o dei trattamenti, incidenti significativi o evidenze di audit. Il PS26-IA-02, se adottato, deve restare coerente con il presente Regolamento e con gli altri documenti del Kit Base.

ALLEGATO A - Matrice rapida degli utilizzi

Scenario	Esito	Regola	Documento/azione PS26
Bozza di testo non riservato	AMMESSO	Revisione umana obbligatoria	-

Scenario	Esito	Regola	Documento/azione PS26
Materiale didattico con dati fittizi	AMMESSO	Verifica accuratezza e adeguatezza	-
IA con dati personali reali	CONDIZIONATO	Solo sistema autorizzato e caso d'uso valutato	GEN-03; eventuale GOV-03/RSK-02
Nuovo agente collegato a Drive o posta	CONDIZIONATO	Autorizzazione preventiva, sicurezza e permessi minimi	GEN-03 + GEN-06
IA per voto/giudizio automatico	NON AMMESSO come unico decisore	Valutazione umana sostanziale; verifica high-risk	GEN-03 + RSK-02
PEI/PDP in chatbot non approvato	VIETATO	Dati particolari/minori	DBR-01 se già avvenuto
Deepfake offensivo di studente/docente	VIETATO	Lesivo e non autorizzato	Regolamento d'Istituto + eventuale incidente
IA in compito dello studente	CONDIZIONATO	Dipende dalla consegna e dalla trasparenza richiesta	STU-04

ALLEGATO B - Flusso di autorizzazione di un nuovo sistema IA

1. Proposta: finalità, utenti, dati, output, integrazioni e benefici attesi.
2. Test controllato con dati fittizi/sintetici; nessun dato reale finché non autorizzato.
3. PS26-GEN-03: valutazione preventiva.
4. Fornitore/privacy/sicurezza: DPA, subfornitori, trasferimenti, conservazione, training, misure tecniche.
5. PS26-RSK-02: screening rischio e trigger DPIA/high-risk.
6. PS26-GOV-03/04: parere DPO quando pertinente.
7. Decisione del Dirigente/Titolare: autorizzazione, limiti, utenti, formazione e data di riesame.
8. PS26-GEN-06: inventario IA.
9. PS26-GOV-08: formazione/prese visione.
10. Monitoraggio: riesame a ogni modifica significativa.

ALLEGATO C - Regola pratica prima di inserire un prompt

- Sto usando uno strumento autorizzato per questa finalità?
- Posso evitare di inserire dati personali o utilizzare dati fittizi/anonimizzati?
- Il prompt contiene nomi, email, immagini, PEI/PDP, salute, credenziali, fascicoli o documenti riservati?
- Il sistema può conservare o riutilizzare il contenuto per training?

- L'output influenzerà una valutazione, una decisione o un atto ufficiale?
- Posso verificare l'output con fonti affidabili e assumermene la responsabilità?
- Se emerge un rischio o un dubbio, interrompere l'uso e attivare il Referente IA o funzione competente e il flusso GEN-03/GOV-03.

ALLEGATO D - Formula breve di trasparenza sull'uso dell'IA

Per la preparazione di questo contenuto è stato utilizzato un sistema di Intelligenza Artificiale come strumento di supporto per ideazione, sintesi, traduzione, bozza o altra attività dichiarata. Il contenuto finale è stato verificato, corretto e approvato dalla persona responsabile.

Documenti PS26 collegati

- PS26-GOV-09 - Atto di individuazione del Referente IA;
- PS26-IA-02 - Piano e Strategia di Istituto per l'adozione dell'IA;
- PS26-IA-03 - Informativa integrativa privacy sull'utilizzo dei sistemi IA;
- PS26-PER-05 - Disciplinare per l'uso dell'IA da parte del personale;
- PS26-STU-04 - Policy IA studenti;
- PS26-GEN-03 - Valutazione preventiva di software, cloud e IA;
- PS26-GEN-06 - Inventario sistemi IA;
- PS26-RSK-02 - Screening DPIA e valutazione sistemi IA;
- PS26-GOV-03/04 - Richiesta e parere DPO/RPD;
- PS26-GOV-08 - Registro formazione/alfabetizzazione IA;
- PS26-DBR-01/03 - Segnalazione e valutazione incidenti/data breach.

Adozione

Elemento	Valore
Data di adozione	25/09/2026
Estremi atto/delibera	Delibera n°34 del C.I. del 25/09/2026
Dirigente scolastico	Giuseppe Mingione
RPD/DPO	Francesco Iaquinandi - francesco.iaquinandi@iissspantaleo.edu.it - tel. +39 338 9475706