Istituto Comprensivo Statale ad Indirizzo Musicale
" Guastella - Landolina"
via Ettore Majorana snc- C.da Gabatutti – 90036 Misilmeri (Pa)
Tel. 0917525597-091546899-C.F. 97382260822
Email (PEO):PAIC8BW002@istruzione.it (PEC) PAIC8BW002@pec.istruzione.it
Sito web: https://www.icsguastellalandolina.edu.it
_____Sede dell'Osservatorio di Area sulla Dispersione Scolastica Distretto 9_____

PROTOCOLLO DI ADOZIONE INTELLIGENZA ARTIFICIALE

Versione: 1.0 – Data: **14.04.2026**
Istituzione scolastica: I.C. GUASTELLA LANDOLINA DI MISILMERI
Codice meccanografico: PAIC8BW002

0. Scopo, campo di applicazione e definizioni

0.1 Scopo

Stabilire regole, processi e controlli per introdurre, utilizzare e monitorare sistemi di Intelligenza Artificiale (IA) in modo **antropocentrico, sicuro, trasparente, equo** e conforme a:

- AI Act (rischi, obblighi di deployer, trasparenza, alfabetizzazione IA);
- GDPR e Codice Privacy (tutela dati personali, minori, DPIA);
- D.Lgs. 33/2013 e obblighi PA (trasparenza e accountability dove pertinenti);
- Linee guida MIM 2025 per l'IA nelle scuole .

0.2 Campo di applicazione

Il Protocollo si applica a:

- sistemi IA acquistati/contrattualizzati dalla scuola (SaaS, piattaforme, app);
- sistemi IA resi disponibili tramite piattaforme istituzionali;
- sperimentazioni/POC/Progetti PNRR o fondi vari;
- utilizzi "operativi" di IA (didattica, segreteria, comunicazione, supporto decisionale);
- utilizzi individuali del personale **quando** impattano dati/servizi della scuola (es. inserimento dati studenti in LLM).

0.3 Definizioni operative

- **Sistema di IA**: qualsiasi soluzione che generi output (testo, immagini,

raccomandazioni, classificazioni) con metodi di machine learning o inferenza.

- **Deployer**: la scuola quando usa un sistema IA sotto la propria autorità.
- **Fornitore**: chi sviluppa o mette sul mercato un sistema IA.
- **IA ad alto rischio (scuola)**: IA usata per ammissione/assegnazioni, valutazioni apprendimenti, definizione livello educativo, proctoring/monitoraggio comportamenti in prove, profilazione.
- **DPIA**: valutazione impatto privacy (art. 35 GDPR).
- **FRIA**: valutazione impatto diritti fondamentali per sistemi IA ad alto rischio (AI Act) da integrare nella DPIA.

1. Principi vincolanti di adozione

La scuola adotta e applica i seguenti principi (obbligatori nel presente Protocollo):

1. **Centralità della persona e sorveglianza umana**: l'IA non sostituisce la responsabilità umana nelle decisioni che impattano studenti e personale.
2. **Equità e inclusione**: prevenzione attiva di bias e discriminazioni.
3. **Trasparenza e spiegabilità**: utenti informati, processi comprensibili, documentazione conservata, audit possibile.
4. **Tutela dati e minori**: minimizzazione, privacy-by-design/by-default, protezioni rafforzate per soggetti vulnerabili.
5. **Sicurezza tecnica e resilienza**: misure proporzionate, gestione incidenti, controllo accessi.
6. **Sostenibilità**: valutazione costi/benefici, impatto organizzativo e continuità.

2. Governance: ruoli, responsabilità e flussi decisionali

2.1 Ruoli

Dirigente scolastico (Responsabile della governance IA)

- autorizza iniziative IA;
- nomina referenti e gruppo di lavoro;
- assicura sorveglianza umana, accountability e monitoraggio.

DSGA (Responsabile processo amministrativo/contrattuale)

- cura affidamenti e contratti;
- verifica requisiti tecnici/fornitore;

- gestisce inventario applicativi e rapporti con fornitori.

DPO (Supporto obbligatorio in data protection)

- parere su base giuridica, DPIA/FRIA, informativa, art. 28;
- supporto su misure e gestione rischi residui;
- indirizza eventuale consultazione preventiva Garante (art. 36).

Referente IA di istituto (coordinamento operativo)

- raccoglie richieste, mantiene registro IA;
- coordina formazione e comunicazione interna;
- presidia i controlli periodici.

Team IA (facoltativo ma consigliato)

Composto da: animatore digitale/FS PNSD, referente cybersicurezza/tecnico, rappresentante docenti, rappresentante ATA, referente inclusione, RLS (ove utile), eventuale genitore/studente negli organi collegiali per consultazione.

2.2 Decisioni e organi collegiali

- **Uso didattico**: informativa e consultazione in Collegio Docenti e organi collegiali (coerenza con libertà di insegnamento).
- **Uso organizzativo/servizi**: Consiglio d'Istituto per indirizzi e contratti (quando dovuto).
- **Coinvolgimento studenti/famiglie**: necessario quando l'IA riguarda apprendimento o dati degli studenti.

3. Processo standard di adozione (end-to-end)

Ogni iniziativa IA segue obbligatoriamente le seguenti fasi ("gates") con esito documentato.

FASE 1 – Proposta e pre-valutazione (Gate 1: Ammissibilità)

Output: Scheda Proposta IA (Allegato A – da predisporre nel prossimo

step) La proposta deve indicare:

- finalità (didattica/organizzativa/servizi);
- benefici attesi e KPI;
- destinatari (docenti/ATA/studenti/famiglie);
- categorie dati trattati (se presenti);
- livello di autonomia decisionale del sistema;

- stima costi e risorse.

Controllo di ammissibilità (obbligatorio):

1. Verifica che non rientri in pratiche vietate (AI Act art. 5) incluse: manipolazione, social scoring, emotion recognition studenti (salvo eccezioni), categorizzazioni biometriche sensibili.
2. Verifica compatibilità con finalità istituzionali e PTOF/PIAO.
3. Verifica "data minimization": è possibile raggiungere lo scopo senza dati personali o con dati aggregati/sintetici?

Esito Gate 1: APPROVATO / RESPINTO / DA INTEGRARE.

FASE 2 – Classificazione rischio IA (Gate 2: Risk classification)

Output: Scheda Classificazione Rischio IA

La scuola deve classificare:

- **IA ad alto rischio** (educazione: ammissione/assegnazione, valutazione apprendimenti, definizione livello educativo, proctoring/monitoraggio condotte in prove, profilazione).
- **IA a rischio limitato** (interazione diretta con persone → obblighi trasparenza).
- **IA a rischio minimo** (nessun impatto diretto, raccomandati codici di condotta).

Regola d'oro scuola: se incide su **valutazioni, percorsi, accesso, controllo comportamenti**, trattare come **alto rischio** salvo prova contraria documentata.

Esito Gate 2: Classe rischio definita e firmata (DS + Referente IA + DPO per presa visione).

FASE 3 – Valutazione Privacy e Diritti (Gate 3: Conformità GDPR + FRIA se applicabile)

Output obbligatori:

- DPIA (sempre raccomandata; di fatto necessaria con IA per minori/nuove tecnologie).
- FRIA integrata nella DPIA se IA ad alto rischio.
- Aggiornamento Registro trattamenti.
- Definizione base giuridica (documentata).
- Informative (studenti/famiglie/personale) aggiornate o nuove.

Contenuti minimi DPIA:

- descrizione trattamento, flussi dati, attori, trasferimenti;

- necessità e proporzionalità;
- rischi (privacy, bias, sicurezza, minori);
- misure tecniche/organizzative;
- residual risk e piano trattamento rischi;
- periodicità di revisione.

Quando consultare il Garante (art. 36 GDPR):

- se DPIA evidenzia rischi residui elevati non mitigabili.

Esito Gate 3: OK / OK con prescrizioni / STOP (rischio non accettabile).

FASE 4 – Due diligence del fornitore e contrattualistica (Gate 4: Procurement s compliance)

Output:

- check requisiti tecnici e sicurezza (es. ISO/IEC 27001, qualificazioni AgID per SaaS se pertinenti).
- verifica localizzazione dati e trasferimenti extra UE (es. Data Privacy Framework quando applicabile).
- contratto + Allegati:
    - **Accordo art. 28 GDPR** se il fornitore è responsabile del trattamento;
    - SLA assistenza/manutenzione;
    - obblighi su log, audit, subfornitori, data breach;
    - configurazioni privacy by default (no training su prompt, no retention, ecc., dove possibile).

Clausole minime consigliate:

- divieto uso dati scuola per addestramento, salvo esplicita autorizzazione e garanzie;
- tracciabilità accessi e log;
- diritto di audit;
- tempi risposta incidenti;
- cancellazione e portabilità dati a fine contratto;
- obblighi di supporto per richieste interessati.

Esito Gate 4: Contratto conforme firmato / non firmabile.

FASE 5 – Configurazione, sicurezza e messa in esercizio (Gate 5: Go-live) Output:

- piano di configurazione (privacy by default);
- manuale operativo d'uso e limiti;
- ruoli e autorizzazioni (IAM);
- procedure incident response e segnalazioni.

Misure obbligatorie "scuola" (minimo comune):

- account istituzionali, niente account personali per attività scolastiche;
- blocco/limitazione inserimento dati personali nei prompt, soprattutto minori;
- disattivazione funzionalità non necessarie (cronologia conversazioni, servizi accessori, tracking) quando possibile.
- registro delle configurazioni (chi/come/quando).

FASE 6 – Formazione e alfabetizzazione IA (Gate 6: Readiness)

Obbligatoria la **AI literacy** per personale che usa/gestisce il sistema.

Output:

- Piano formazione (docenti/ATA/dirigenti);
- registro presenze e materiali;
- moduli specifici per rischi (bias, hallucination, copyright, dati personali, sicurezza).

Requisito minimo:

- nessun go-live se il personale chiave non è formato (referente IA, amministratori, utilizzatori principali).

FASE 7 – Comunicazione, trasparenza e gestione "non partecipazione"

Output:

- comunicazione a famiglie/studenti (uso, finalità, limiti);
- informativa privacy dedicata IA;
- procedura "diritto di non partecipazione" se dati usati per training o trattamenti non

necessari (opt-out senza penalizzazione).

FASE 8 – Monitoraggio continuo, audit e miglioramento

Output periodici:

- report trimestrale/semester (KPI + rischi + incidenti);
- revisione DPIA (annuale o al mutare rischi/sistema).
- test bias e qualità output (campionamento);
- registro incidenti e near-miss.

Trigger di revisione immediata:

- modifica modello/fornitore;
- nuove funzionalità (es. proctoring, scoring);
- data breach o evento di sicurezza;
- reclami di famiglie/studenti/personale.

4. Regole d'uso per categorie (minimo comune)

4.1 Docenti

- IA come supporto, non sostitutivo della progettazione didattica;
- divieto inserire dati identificativi studenti nei prompt;
- obbligo di verifica fonti/accuratezza output (rischio "allucinazioni").
- obbligo di dichiarare agli studenti quando un contenuto è prodotto con IA se rilevante per la valutazione.

4.2 Personale ATA/Segreteria

- IA solo su dati minimizzati/necessari;
- nessun caricamento di atti contenenti dati particolari (salute, BES, disabilità) salvo specifica autorizzazione e misure rafforzate.
- tracciamento delle attività e conservazione secondo policy.

4.3 Studenti

- uso guidato e supervisionato;
- istruzioni su prompt "sicuri" e divieto di condividere dati personali propri/altrui;
- educazione al pensiero critico (verifica output, bias, fonti).

4.4Famiglie

- informazione chiara su finalità e tutele;
- canale di reclamo/istanze;
- gestione opt-out dove applicabile.

5. Gestione rischi: catalogo minimo e contromisure

La scuola deve valutare e mitigare almeno i seguenti rischi:

1. **Rischio privacy/minori** → minimizzazione, ambienti controllati, informative, DPIA, divieti prompt con dati identificativi.
2. **Bias/discriminazione** → test periodici, controllo dataset/fornitore, revisione umana, canali reclamo.
3. **Allucinazioni/errore contenuti** → policy "human-in-the-loop", fact-check, rubriche valutative.
4. **Opacità** → documentazione fornitore, spiegabilità, log, audit.
5. **Cybersecurity** → MFA, patching, logging, incident response, SLA.
6. **Dipendenza/deskilling** → formazione, limiti d'uso, attività che valutano competenze autentiche.
7. **Rischi reputazionali** → comunicazione trasparente, gestione reclami, registro decisioni.

6. Documentazione obbligatoria e registri (kit "minimo")

Per ogni iniziativa IA la scuola deve conservare in fascicolo dedicato:

1. Scheda Proposta IA + autorizzazione DS
2. Classificazione rischio (AI Act)
3. DPIA (+ FRIA se alto rischio)
4. Base giuridica e aggiornamento Registro trattamenti
5. Contratto + art. 28 GDPR + SLA
6. Informative e comunicazioni a famiglie/studenti/personale
7. Piano formazione + registri presenze
8. Registro configurazioni e accessi
9. Registro incidenti e report monitoraggio

7. Indicatori di efficacia (KPI) e di rischio

(KRI) KPI (beneficio):

- riduzione tempi attività amministrative;
- miglioramento accessibilità/inclusione (es. strumenti compensativi);
- qualità percepita da utenti.

KRI (rischio):

- numero incidenti privacy/sicurezza;
- reclami su output discriminatori;
- non conformità emerse in audit;
- eventi di utilizzo improprio (prompt con dati personali).

8. Procedura reclami e segnalazioni

La scuola istituisce:

- canale dedicato (email/registro) per segnalazioni su IA;
- tempi risposta (es. 10 giorni lavorativi);
- escalation (Referente IA → DS/DSGA → DPO → eventuale fornitore).

G. Entrata in vigore e revisione del Protocollo

- Il Protocollo entra in vigore dalla data di approvazione.
- Revisione: almeno annuale o al mutare di norme/Linee guida MIM/strumenti IA.

Il presente Protocollo di adozione I.A. è stato approvato con delibera n. 2 del 14.04.2026 del Collegio dei Docenti e con delibera n. 2 del 14.04.2026 del Consiglio di Istituto.

ALLEGATI OPERATIVI

ALLEGATO A – SCHEDA PROPOSTA IA

1. DATI GENERALI
Proponente: _____
Ruolo: _____
Data proposta: _____
Sistema IA (nome commerciale): _____
Fornitore: _____
Finalità (didattica/organizzativa/servizi): _____

2. DESCRIZIONE TECNICA
Tipologia (LLM, chatbot, analytics, proctoring, ecc.): _____
Modalità utilizzo: _____
Utenti coinvolti: ☐ Docenti ☐ ATA ☐ Studenti ☐ Famiglie
Categorie dati trattati: ☐ Nessun dato ☐ Dati comuni ☐ Dati minori ☐ Dati particolari

3. VERIFICA PRATICHE VIETATE (AI ACT ART. 5)
☐ Tecniche manipolative o subliminali
☐ Social scoring
☐ Emotion recognition su studenti
☐ Categorizzazione biometrica sensibile
☐ Profilazione discriminatoria
Esito: ☐ Ammissibile ☐ NON Ammissibile

4. INDICATORI ALTO RISCHIO (AMBITO EDUCATIVO)
☐ Ammissione studenti
☐ Assegnazione percorsi
☐ Valutazione automatizzata
☐ Monitoraggio esami/prove
☐ Profilazione studenti
Classificazione preliminare: ☐ Alto rischio ☐ Non alto rischio

ALLEGATO B – MODELLO CLASSIFICAZIONE RISCHIO AI ACT
Sistema IA: _____
Descrizione sintetica: _____

1. CATEGORIA DI RISCHIO
☐ Vietato
☐ Alto rischio
☐ Rischio limitato
☐ Rischio minimo

2. OBBLIGHI CONSEGUENTI
Se ALTO RISCHIO:
- FRIA obbligatoria
- DPIA rafforzata
- Supervisione umana strutturata
- Monitoraggio continuo
Se RISCHIO LIMITATO:
- Informazione utenti
- Trasparenza interazione IA

Motivazione giuridica: _____
Firma DS: _____
Firma DPO: _____

ALLEGATO C – DPIA IA + SEZIONE FRIA

1. DESCRIZIONE TRATTAMENTO
Finalità: _____
Base giuridica: _____
Flussi dati: _____
Conservazione: _____
Trasferimenti extra UE: ☐ Sì ☐ No

2. ANALISI NECESSITÀ E PROPORZIONALITÀ
Motivazione uso IA: _____
Alternative valutate: _____

3. ANALISI RISCHI
Rischio privacy minori: _____
Rischio bias: _____
Rischio allucinazioni: _____
Rischio cybersecurity: _____

4. FRIA (se alto rischio)
Impatto su non discriminazione: _____
Impatto su inclusione: _____
Misure mitigazione aggiuntive: _____

Esito finale: ☐ Accettabile ☐ Accettabile con prescrizioni ☐ Non accettabile
Firma DS: _____
Parere DPO: _____

ALLEGATO D – INFORMATIVA PRIVACY IA

La scuola informa che utilizza sistemi di Intelligenza Artificiale per:

_____

Base giuridica: compito di interesse pubblico.

Categorie dati trattati: _____

Non vengono adottate decisioni completamente automatizzate.

Diritti esercitabili: accesso, rettifica, limitazione, opposizione.

Modalità opt-out (se applicabile): _____

Titolare: _____

DPO: _____

ALLEGATO E – REGOLAMENTO D'USO IA

1. PRINCIPI GENERALI

L'IA è strumento di supporto e non sostituisce la responsabilità umana.

2. DOCENTI

- Divieto inserire dati identificativi studenti nei prompt.
- Verifica sempre l'accuratezza degli output.
- Dichiarare utilizzo IA se incide su valutazioni.

3. ATA

- Utilizzo esclusivamente per finalità istituzionali.
- Divieto caricamento dati sensibili senza autorizzazione.

4. STUDENTI

- Uso supervisionato.
- Divieto condivisione dati personali.

Violazioni soggette a regolamenti disciplinari.

ALLEGATO F – CLAUSOLE CONTRATTUALI + ART. 28 + SLA (CONTRATTO VINCOLANTE CON FORNITORE DI SERVIZI) IA

1. Divieto utilizzo dati scuola per addestramento modelli.
2. Notifica data breach entro 24 ore.
3. Accordo art. 28 GDPR dettagliato.
4. SLA:
- Uptime minimo 99%
- Presa in carico incidenti critici entro 4 ore
- Ripristino entro 24/48 ore
5. Diritto audit scuola.
6. Cancellazione dati a fine contratto.

ALLEGATO G – PIANO FORMAZIONE AI LITERACY
Obiettivi: consapevolezza rischi IA, bias, privacy, sicurezza.
Destinatari: ☐ Dirigente ☐ Docenti ☐ ATA ☐ Studenti
Durata minima: 6 ore annue personale.

REGISTRO FORMAZIONE
Data Corso Partecipanti Firma