

ISTITUTO COMPRENSIVO CORTONA 2 “GINO BARTALI”

Sede Via dei Combattenti, TERONTOLA – 52044 CORTONA (AR) tel 0575 67519 CF: 92082410512 -
cod. MIUR: ARIC841007 email: aric841007@istruzione.it - pec: aric841007@pec.istruzione.it

REGOLAMENTO D'ISTITUTO PER L'USO DELL'INTELLIGENZA ARTIFICIALE (RI-IA)

ISTITUTO COMPRENSIVO - CORTONA 2-CORTONA Prot. 0005725 del 12/08/2026 I-4 (Uscita)
--

Collegio dei docenti - delibera n. 6 del 29.06.2026

Consiglio d'Istituto - delibera n. 57 del 30.06.2026

Elaborazione e Redazione a cura del G.L.I.A. (Gruppo di Lavoro per l'Intelligenza Artificiale)

1. PRINCIPI FONDAMENTALI E CAMPO DI APPLICAZIONE

1.1 Introduzione, Finalità e Principio Antropocentrico

Il presente **Regolamento d'Istituto per l'uso dell'Intelligenza Artificiale (RI-IA)** costituisce il documento procedurale e operativo con cui l'Istituzione Scolastica si impegna a dare piena attuazione al proprio **Piano d'Istituto per l'Intelligenza Artificiale (PIA)** e alle direttive nazionali e comunitarie in materia.

L'Intelligenza Artificiale rappresenta una profonda innovazione culturale, che incide in maniera significativa sulle metodologie di insegnamento, sui processi di apprendimento e sull'organizzazione complessiva della vita scolastica. L'obiettivo primario è garantire che l'introduzione di tali tecnologie avvenga secondo principi di **consapevolezza, etica e sicurezza**.

Ambito di Applicazione

Il Regolamento disciplina l'utilizzo degli strumenti di IA da parte di:

- **Docenti:** per l'attività di insegnamento, valutazione e progettazione didattica.
- **Studenti:** per attività di apprendimento, studio e produzione di elaborati.
- **DS, DSGA, Personale Amministrativo (ATA):** nel ambito delle proprie funzioni e nel rispetto del principio di pertinenza.

Tecnologie Ricomprese

- Sistemi generativi di testo, immagini, suoni e video.
- Assistenti virtuali e chatbot educativi.
- Piattaforme di apprendimento adattivo.
- Ogni altra applicazione che impieghi algoritmi capaci di apprendere, generare o prendere decisioni in autonomia.

Finalità Generali

- **Regolamentare e Istruire:** definire in maniera chiara le regole d'uso per l'intera comunità scolastica.
- **Sicurezza e Privacy:** assicurare la rigorosa conformità al Regolamento Europeo sulla Protezione dei Dati (GDPR), prevenendo la diffusione o il trattamento improprio di dati personali.
- **Formazione e Consapevolezza:** promuovere la formazione continua del personale e l'acquisizione dell'AI Literacy (alfabetizzazione all'IA) per studenti e famiglie.
- **Innovazione e Critica:** sfruttare le potenzialità dell'IA per favorire l'inclusione e la personalizzazione, sviluppando al contempo un robusto pensiero critico verso l'automazione e i suoi bias.

Principio Antropocentrico e Principi Guida

Il principio guida dell'Istituto è l'**approccio antropocentrico**: l'IA deve servire l'uomo e l'educazione. L'attività scolastica si conforma ai seguenti principi fondamentali:

- **Centralità della persona:** l'IA costituisce un supporto e non un sostituto del pensiero critico umano; le decisioni didattiche restano sempre di competenza del docente.
- **Legalità e responsabilità:** rispetto della normativa in materia di dati personali, diritto d'autore e tutela dei minori.
- **Trasparenza e tracciabilità:** i processi decisionali basati su IA devono essere comprensibili e verificabili.
- **Affidabilità ed accuratezza:** uso di piattaforme certificate o dotate di adeguate garanzie di qualità.
- **Equità e non discriminazione:** divieto di utilizzare sistemi che possano generare bias o trattamenti differenziati.
- **Proporzionalità e minimizzazione:** utilizzo delle sole funzioni strettamente necessarie, evitando raccolte di dati eccessive, privilegiando sistemi che non addestrano le AI con i dati degli utenti e che rispettino al massimo la privacy.

1.2 Quadro Normativo di Riferimento

L'Istituto garantisce il continuo aggiornamento del Regolamento in conformità alle seguenti fonti normative:

- **Normativa Ministeriale:** Decreto Ministeriale n. 166 del 09/08/2025 e Linee Guida MIM per l'introduzione dell'IA nelle Istituzioni scolastiche.
- **Regolamento Europeo sulla Protezione dei Dati (GDPR):** Regolamento UE 2016/679 e D.Lgs. 196/2003 per la massima tutela dei dati di studenti e personale, escludendo strumenti privi di Privacy by Design.

- **AI Act (Regolamento UE 2024/1689):** conformità dell'Istituto in qualità di Deployer, mediante un approccio basato sul rischio e il rispetto dei divieti a tutela dei diritti fondamentali.
- **Normativa Antibullismo e Cyberbullismo:** Legge n. 71/2017 per la prevenzione ed il contrasto del cyberbullismo e della lesione della dignità personale.

1.3 Visione Etica dell'Istituto: L'IA come Sostegno, non Sostituto

L'IA è considerata un **"Alleato Educativo"** in grado di:

- **Personalizzare l'apprendimento:** supportando percorsi didattici adattivi per i bisogni specifici di ogni alunno.
- **Supportare la creatività:** fornendo strumenti per la risoluzione di problemi complessi e liberando tempo al docente per la relazione educativa.
- **Favorire l'inclusione:** offrendo ausili tecnologici avanzati per alunni con Bisogni Educativi Speciali (BES) o Disturbi Specifici dell'Apprendimento (DSA).

L'IA non potrà mai essere:

- **Sostituto del docente:** l'IA non sostituisce l'empatia, il giudizio umano e l'insostituibile relazione pedagogica.
- **Strumento di controllo invasivo:** è esclusa l'adozione di sistemi volti a profilare in modo invasivo o a esercitare controlli non necessari.

1.4 Definizioni e Assetto delle Responsabilità

1.4.1 Qualifica Giuridica di Deployer (Utilizzatore)

Ai sensi dell'AI Act, l'Istituzione Scolastica assume in via esclusiva la qualifica giuridica di **Deployer** in quanto soggetto pubblico che impiega sistemi di IA nello svolgimento delle proprie attività istituzionali sotto la propria autorità. L'Istituto è l'unico responsabile di:

- Scelta strategica e adozione dei sistemi di IA.
- Verifica dell'adeguatezza e configurazione dei servizi.
- Definizione dei casi d'uso consentiti e dei perimetri di sicurezza.
- Supervisione umana generale e protezione dei dati personali.

1.4.2 Qualifica Giuridica di Provider (Fornitore)

Il **Provider** è il soggetto che sviluppa un sistema di IA per immetterlo sul mercato. La presenza di obblighi legali in capo al Provider **non esonera l'Istituto dalle proprie responsabilità di**

Deployer. L'Istituto si impegna a verificare la soluzione, configurare il servizio per limitare i dati, definire i casi d'uso, garantire accordi DPA e mantenere la supervisione umana (Human Oversight).

1.4.3 Qualifica di Utilizzatori Autorizzati

I singoli docenti, il personale ATA e gli studenti **non sono Deployer**, ma sono qualificati esclusivamente come **Utilizzatori Autorizzati**. Essi devono:

- Rispettare le istruzioni e le policy impartite dalla scuola.
- Utilizzare esclusivamente gli strumenti presenti nel "Registro degli strumenti autorizzati".
- Esercitare la supervisione umana critica sugli output.

La responsabilità individuale derivante da un eventuale uso degli strumenti contrario alle regole non modifica la titolarità delle scelte organizzative e delle responsabilità istituzionali in capo alla scuola. L'Istituzione rimane il soggetto responsabile della governance, mentre l'utilizzatore risponde del mancato rispetto delle procedure che devono essere esplicitate in maniera chiara.

1.4.4 Ruolo Consultivo del DPO (Data Protection Officer)

Il DPO esercita una funzione prettamente **consultiva e di sorveglianza** in piena indipendenza. È consultato obbligatoriamente su informativa, accordi DPA, analisi dei rischi (DPIA/FRIA) e gestione dei data breach. Il DPO non partecipa ai processi gestionali né all'autorizzazione tecnica delle infrastrutture, la cui responsabilità resta in capo al Dirigente Scolastico.

2. AMBITI DI INTERVENTO, STRUMENTI E GOVERNANCE

L'introduzione dell'intelligenza artificiale nel nostro Istituto è strutturata su un approccio incrementale che distingue nettamente tra una fase di addestramento e una fase operativa avanzata. Questa ripartizione, definita nel Piano (PIA) e nel Regolamento (RI-IA), serve a garantire la massima protezione dei dati durante l'apprendimento delle competenze necessarie.

2.1 Fase 1 e Fase 2 per l'adozione dell'Intelligenza Artificiale

L'Istituto ha deciso di organizzare l'utilizzo dell'AI attraverso 2 fasi. La distinzione tra le due fasi non riguarda solo il tipo di software, ma soprattutto **l'infrastruttura e il tipo di dati trattati**, con una transizione verso sistemi interni per la gestione delle informazioni più sensibili. La **Fase 1** si appoggia su **servizi esterni** operando solo su dati astratti e sintetici per motivi di sicurezza; la **Fase 2** punta all'uso di un **server interno (locale)** per poter gestire in sicurezza dati reali e sensibili dell'Istituto.

2.1.1 Fase 1: La "Fase Iniziale Protetta" (Alfabetizzazione e Simulazione)

La Fase 1 è dedicata esclusivamente all'alfabetizzazione critica (AI Literacy) e alla sperimentazione metodologica. Il suo obiettivo è permettere al personale e agli studenti di esplorare le potenzialità dell'IA in un ambiente a rischio nullo per la privacy.

- Vincolo di Riservatezza Assoluto: È tassativamente vietato l'inserimento di dati personali reali, documenti riservati o riferimenti a casi specifici di studenti (nomi, PEI, PDP reali).
- Cosa si può fare:
 - Prompting Astratto: I docenti possono utilizzare l'IA per generare strategie didattiche basate su descrizioni pedagogiche astratte (es. "metodologie per un alunno con discalculia") senza fare riferimento a studenti reali.
 - Uso di Dati Sintetici: Si utilizzano dati generati artificialmente (fittizi) che non si riferiscono a persone esistenti. Questo è lo strumento principale per formare i docenti sulla gestione di casi complessi in totale sicurezza.
 - Supporto Operativo Amministrativo: Creazione di bozze per circolari generiche, avvisi e ricerche normative rapide, sempre con validazione umana obbligatoria.
- Scopo Didattico: Familiarizzazione con la logica dei prompt, comprensione dei limiti (allucinazioni) e dei bias della tecnologia.

Nella Fase 1 (Fase Iniziale Protetta), l'Istituto autorizza l'interazione con motori di IA tipicamente esterni (i "Provider"), ma impone restrizioni severissime proprio per mitigare i rischi legati alla trasmissione di dati a terzi.

- Software: Si utilizzano i sistemi messi a disposizione dai fornitori (es. Google, Microsoft o altri tool nel Registro Tecnico).
- Vincolo: È tassativamente vietato inserire dati personali reali, documenti riservati o riferimenti a casi specifici di studenti nei prompt di questi sistemi esterni.
- Attività: L'interazione è limitata a modelli didattici astratti, ricerca e sperimentazioni su dati sintetici (fittizi).

In questa fase l'interazione con l'IA è consentita unicamente su:

- Modelli didattici e amministrativi generici e astratti.
- Testi privi di riferimenti a persone reali.
- Dati Sintetici: dati generati artificialmente che non si riferiscono a soggetti identificabili.

L'uso di dati sintetici è lo strumento principale per la formazione del personale alla gestione di PEI e PDP: i docenti si eserciteranno su profili di studenti fittizi creati ad hoc, per acquisire la competenza necessaria a validare criticamente gli output (Human Oversight) prima del passaggio a dati reali in Fase 2 con l'utilizzo di un LLM interno all'istituto.

2.1.2 Fase 2: La "Fase Successiva" (Integrazione Operativa e Analisi)

La Fase 2 segna il passaggio all'uso operativo dell'IA su dati reali e complessi, ma è soggetta a rigidi prerequisiti tecnici e formativi.

- Il Pivot Tecnologico (Server LLM Locale): L'attivazione di questa fase è subordinata al collaudo dell'infrastruttura Server LLM On-Premise. Questo server interno è progettato per ridurre la trasmissione di dati verso l'esterno, permettendo trattamenti più delicati all'interno del perimetro protetto della scuola.
- Cosa si potrà fare (Progetti Pilota):
 - Analisi dei Dati Sensibili: Monitoraggio aggregato e anonimizzato di assenze, esiti scolastici e flussi di iscrizione per prevenire la dispersione scolastica.
 - Gestione di Pratiche Riservate: Elaborazione di documenti d'ufficio che richiedono la gestione di dati reali, precedentemente esclusi.
- Condizioni di Attivazione: La Fase 2 non è automatica. Richiede la conclusione della formazione obbligatoria del personale, una nuova analisi dei rischi, la redazione di una DPIA (Valutazione d'Impatto) specifica e l'autorizzazione formale del Dirigente Scolastico, sentito il DPO.

Questa fase è caratterizzata dal tentativo di spostare il trattamento dei dati su una infrastruttura locale per superare i limiti della fase precedente.

- Software/Infrastruttura: Il passaggio a questa fase è subordinato al collaudo di un Server LLM Locale (On-Premise), ovvero un sistema che risiede fisicamente o logicamente all'interno del perimetro protetto dell'Istituto.
- Scopo: L'uso di un LLM interno serve a ridurre la trasmissione di dati verso l'esterno, permettendo così (previa DPIA e formazione specifica) di iniziare a trattare dati reali per attività complesse come l'analisi delle assenze o il supporto alla redazione di documenti sensibili che nella Fase 1 erano vietati.
- Monitoraggio: Anche in questa fase, l'uso rimane sotto stretto controllo umano (Human in the Loop) e non garantisce comunque una "riservatezza assoluta", richiedendo nuove responsabilità tecniche per la scuola.

2.2 Procedura di Progettazione e Rendicontazione dei Progetti

- **Prima dell'Attività (Progettazione):** Il docente (o il team di docenti) compila la Scheda di Progetto e la invia al GLIA, che ne verifica il rispetto dei vincoli di sicurezza e la inserisce nel registro delle sperimentazioni. Il progetto deve essere autorizzato formalmente dal dirigente.
- **Durante l'Attività (Svolgimento):** Il docente svolge l'attività secondo le metodologie UDL approvate, monitorando l'interesse e lo spirito critico degli alunni.
- **Dopo l'Attività (Rendicontazione):** Entro la fine dell'anno scolastico, il docente, o il team docente, compila la Scheda di rendicontazione. I dati raccolti confluiranno direttamente nella Relazione Annuale d'Istituto.

2.3 Ambiti di Applicazione dell'IA a Scuola

Area Didattica e Inclusione (Universal Design for Learning - UDL)

L'IA supporta l'insegnamento e l'abbattimento delle barriere all'apprendimento secondo il framework UDL:

- **Progettazione didattica:** generazione di idee, materiali di approfondimento e simulazioni.
- **Molteplici mezzi di rappresentazione:** scalabilità linguistica, semplificazione testuale e trasposizione multimodale.
- **Molteplici mezzi di azione ed espressione:** l'uso dell'IA come tutor e facilitatore personalizzato, cioè uno strumento capace sia di accompagnare gradualmente l'alunno nella comprensione di un compito (scaffolding), sia di modulare i materiali e i linguaggi in base alle specifiche caratteristiche e priorità educative dell'alunno (strategie differenziate), fermo restando il divieto assoluto di inserire dati personali reali nei prompt.
- **Molteplici mezzi di coinvolgimento:** contestualizzazione dei contenuti in base agli interessi della classe.
- **Strumenti inclusivi autorizzati:** OCR intelligenti, sintesi vocale (Text-to-Speech), traduzione simultanea per alunni NAI (Neo-Arrivati in Italia), generatori di mappe concettuali e piattaforme di apprendimento adattivo.

Vincolo di Riservatezza UDL: È fatto divieto assoluto ai docenti di inserire nei prompt dati identificativi, documentazione clinica, verbali L. 104/92, PEI o PDP. La personalizzazione deve basarsi solo sulla descrizione astratta del bisogno didattico. Per favorire l'inclusione già nella Fase 1 (**Fase iniziale Protetta**), il docente deve utilizzare la tecnica del Prompting Astratto: l'input fornito all'IA deve contenere solo le caratteristiche didattiche della difficoltà e gli obiettivi di apprendimento, agendo come una consultazione metodologica generale piuttosto che come una redazione di atto personale.

Area Amministrativa (Personale ATA)

L'uso dell'IA in ambito amministrativo segue il principio di gradualità e cautela:

- **Attività autorizzate in Fase Protetta:** redazione di bozze per circolari generiche, sintesi normative e revisione stilistica di testi anonimi.
- **Attività differite (Limitazioni DPO):** analisi delle assenze, gestione di pratiche riservate (es. procedimenti disciplinari), elaborazione di orari o graduatorie con dati personali.
- **Obbligo di Validazione Umana e Figure Responsabili:** Nessun atto formale può essere prodotto in modo automatizzato. Ogni output generato dall'IA deve essere tassativamente verificato e validato da un operatore umano identificato nelle figure del Dirigente, del DSGA o dell'assistente amministrativo competente, che ne assume la piena responsabilità.

Prospettiva di Sviluppo: Progetto Pilota Server LLM Locale (On-Premise) Fase 2

L'Istituto valuta la futura sperimentazione di un'infrastruttura locale per l'esecuzione di modelli linguistici. Tale server interno è configurato come **progetto pilota eventuale** e non come assetto ordinario.

- **Natura dei rischi:** l'uso di un server locale riduce la trasmissione di dati a terzi, ma **non garantisce una "riservatezza assoluta"**, non elimina il rischio di data breach e non previene le "allucinazioni" dell'IA.
- **Prerequisiti obbligatori:** l'attivazione richiede uno studio di fattibilità, una valutazione di sicurezza informatica, la verifica della conformità cloud-first, la nomina degli amministratori e una disciplina rigorosa dei log di sistema, nonché un'adeguata struttura hardware e software.

2.4 Registro Tecnico degli Strumenti Autorizzati

Il **Registro Tecnico** è l'unico riferimento giuridico per gli strumenti IA consentiti nell'Istituto. L'uso di piattaforme non inserite nel Registro è tassativamente vietato per scopi istituzionali.

2.4.1 Criteri di Valutazione e Contenuti del Registro

Ogni strumento viene valutato dal Dirigente Scolastico e dal Gruppo di Lavoro IA (GLIA), sentito il DPO, concentrandosi sullo specifico **caso d'uso**. Al fine di garantire una sorveglianza effettiva e una tracciabilità totale, il Registro Tecnico deve riportare obbligatoriamente per ogni applicazione o piattaforma validata i seguenti elementi informativi:

- **Identificazione:** Nome dello strumento e versione specifica oggetto di validazione.
- **Soggetto Responsabile:** Fornitore (Provider) del sistema.
- **Profili di Accesso:** Categorie di utenti autorizzati (docenti, studenti, personale ATA).
- **Perimetro Operativo:** Casi d'uso consentiti e casi d'uso tassativamente vietati.
- **Governance dei Dati:** Categorie di dati utilizzabili (es. solo dati sintetici, testi privi di riferimenti personali).
- **Conformità Anagrafica:** Limiti di età stabiliti dal servizio e verifica della conformità normativa.
- **Misure di Sicurezza:** Configurazioni amministrative e misure tecniche implementate dall'Istituto (Deployer) per mitigare i rischi.
- **Audit e Riesame:** Data dell'ultima verifica di conformità e indicazione del Responsabile del riesame periodico.

Pubblicità del Registro

- **Elenco Sintetico (Pubblico):** consultabile sul sito web e sul Registro Elettronico per famiglie e studenti. Specifica anche se uno strumento è abilitato solo per la "Fase 1" (senza dati personali) o se è incluso nel "Progetto Pilota Fase 2" (con dati pseudonimizzati in server locale).

- **Registro Tecnico Completo (Interno):** riservato agli organi di controllo e al GLIA per preservare i dettagli sulla sicurezza delle infrastrutture.

2.5 Governance e Ripartizione dei Ruoli

- **Dirigente Scolastico:** garante dell'attuazione del Regolamento, approva l'introduzione di nuove tecnologie e coordina la formazione.
- **Referente IA e Gruppo di Lavoro IA (GLIA):** supporto tecnico-pedagogico, monitoraggio annuale, conduzione dello screening preliminare sui rischi.
- **Responsabile della Protezione dei Dati (DPO):** consulenza indipendente su privacy, DPIA e conformità GDPR/AI Act.
- **Direttore dei Servizi Generali e Amministrativi (DSGA):** sovrintende all'integrazione dell'IA nei flussi amministrativi, garantendo la tracciabilità delle procedure e la validazione umana degli atti formali.
- **Comunità Scolastica (Docenti, ATA, Studenti, Famiglie):** adozione etica e responsabile degli strumenti nel rispetto delle rispettive competenze.

3. NORME PER I DOCENTI E IL PERSONALE ATA

3.1 Dovere di Supervisione Umana (Human Oversight)

Il docente e l'operatore amministrativo mantengono la piena responsabilità professionale su ogni processo:

- **Verifica degli Output:** qualsiasi testo, quiz o sintesi generata da IA deve essere sottoposta a controllo umano per correggere errori algoritmici o bias.
- **Paternità delle Decisioni:** la responsabilità finale della valutazione didattica o dell'atto amministrativo resta in capo all'operatore umano.
- **Condivisione di Buone Pratiche:** documentazione e condivisione delle esperienze positive all'interno della comunità educante.

3.2 Formazione Continua e Sviluppo dell'AI Literacy

I percorsi formativi per il personale e gli studenti sono progettati in coerenza con i quadri di riferimento europei, dei quali si forniscono le definizioni operative:

- **DigCompEdu:** per lo sviluppo delle competenze digitali professionali e pedagogiche dei docenti, finalizzate a una didattica innovativa e inclusiva.
- **DigComp 3.0:** per l'alfabetizzazione digitale e l'esercizio di una cittadinanza digitale matura e consapevole da parte degli studenti e del personale.

Inoltre:

- **Necessità di formazione:** la formazione sull'IA è parte integrante dell'aggiornamento professionale di Docenti e ATA.
- **Comunità di Pratica:** promozione di laboratori operativi e momenti di co-progettazione tra colleghi.
- **Formazione per Alto Rischio:** nel caso eccezionale di adozione di strumenti ad alto rischio, è prescritta una formazione avanzata e specifica obbligatoria.

3.3 Sicurezza dei Dati (GDPR) e Fase Protetta

3.3.1 Regole Rigide sulla Riservatezza

È vietato inserire in motori di IA esterni:

- Dati personali identificativi (nomi, cognomi, codici identificativi).
- Dati appartenenti a categorie particolari (salute, PEI, PDP, relazioni psicopedagogiche).
- Documenti d'ufficio coperti da segreto o riservati.

Chiarimento Tecnico su Anonimizzazione e Pseudonimizzazione: La semplice sostituzione del nome con un codice o un'iniziale costituisce **pseudonimizzazione** e non anonimizzazione. Il dato pseudonimizzato rimane un dato personale e non può essere inserito in strumenti di IA non autorizzati. La pseudonimizzazione non autorizza l'invio di dati (anche se codificati) a motori di IA esterni durante la Fase 1, poiché il rischio di re-identificazione mantiene il dato sotto la tutela del GDPR.

Screening del Rischio e Valutazione d'Impatto (DPIA)

- **Scheda di Screening Preliminare:** analizza ogni nuovo caso d'uso per valutare se sussista un rischio elevato.
- **DPIA Completa (Art. 35 GDPR):** qualora lo screening evidenzia un rischio elevato, viene redatta una DPIA completa in consultazione con il DPO. Non è ammesso l'uso di modelli ridotti o "DPIA semplificate".

4. NORME PER GLI ALUNNI, INTEGRITÀ SCOLASTICA E VALUTAZIONE

4.1 Diritti degli Studenti e Gradualità per Fasce d'Età

Gli studenti sono **Utilizzatori Autorizzati** e hanno diritto alla trasparenza sui sistemi usati e ad una corretta alfabetizzazione digitale. L'accesso è modulato in base all'età:

- **Scuola dell'Infanzia e Primaria:** l'uso avviene esclusivamente con la **mediazione diretta del docente**; gli alunni non possiedono account personali di IA.

- **Scuola Secondaria di I Grado:** introduzione guidata all'**alfabetizzazione critica**, con interazioni supervisionate volte a comprendere i limiti, le allucinazioni e la struttura dei prompt. Possono avere account personali di AI solo se espressamente autorizzati secondo quanto previsto dal regolamento.

4.2 Integrità Scolastica e Trasparenza

- **Uso Consentito:** l'IA può essere usata come supporto alla ricerca, alla comprensione o alla revisione.
- **Obbligo di Dichiarazione:** lo studente deve dichiarare esplicitamente l'ausilio dell'IA in qualsiasi elaborato, specificando lo **strumento utilizzato** e la **funzione svolta** (es. "supporto alla strutturazione della scaletta", "traduzione per revisione", "revisione sintattica") applicando un watermark adatto.
- **Plagio e Disonestà Scolastica:** l'uso sostitutivo e non dichiarato dell'IA per simulare un'elaborazione personale è considerato plagio e sanzionato secondo i regolamenti dell'istituto.

4.3 Valutazione degli Apprendimenti e Divieto di Automazione

Divieto di Automazione Decisoria: È tassativamente vietato l'impiego di sistemi di IA per decisioni automatizzate definitive su voti, ammissioni o orientamento. L'atto valutativo è una prerogativa umana esclusiva.

Disciplina della Correzione:

- **Correzione Meccanica (Ammessa):** Consentita esclusivamente per **quiz a risposta chiusa**, a condizione che il docente abbia accuratamente validato preventivamente domande e soluzioni.
- **Elaborati Aperti (Vietata):** È esclusa l'attribuzione automatica di voti su temi, saggi o progetti. L'IA può fornire solo feedback formativi intermedi sotto la supervisione del docente.

Diritto alla Spiegabilità: L'Istituto assicura che ogni processo valutativo sia comprensibile per studenti e famiglie; il docente deve fornire la motivazione pedagogica umana di ogni esito, senza mai delegare la spiegabilità del voto alla macchina.

4.4 Prevenzione integrale del cyberbullismo, deepfake e tutela della dignità digitale

4.4.1 Definizione di Deepfake e Media Sintetici

Ai fini del presente Regolamento, si intende per **Deepfake o Media Sintetico** qualsiasi contenuto audio, video, fotografico o testuale generato o manipolato mediante algoritmi di IA generativa,

idoneo a far apparire veritiere immagini, parole, voci o comportamenti di una persona che nella realtà non ha mai pronunciato tali parole o compiuto tali azioni.

4.4.2 Divieti Tassativi per la Comunità Scolastica

È fatto **divieto assoluto** a tutti gli utenti (studenti, docenti, personale ATA) di utilizzare strumenti di IA generativa, sia all'interno dell'Istituto sia in contesti ad esso riconducibili, per:

- **Clonazione vocale o di tratti somatici:** creare o alterare registrazioni audio, fotomontaggi o avatar che riproducano la voce, il volto o la figura di studenti, docenti, dirigenti o personale scolastico senza esplicito e preventivo consenso formale.
- **Contenuti Denigratori, Diffamatori o Sessualizzati:** generare, modificare, conservare o diffondere materiale a carattere ingiurioso, discriminatorio, violento, decontestualizzato o ipersessualizzato avente ad oggetto membri della comunità scolastica.
- **Sostituzione di Persona e Profilazione Falsa:** creare profili social, bot o chatbot che simulino l'identità o il pensiero di un'altra persona per trarre in inganno terzi, deridere o danneggiare la vittima.
- **Amplificazione del Cyberbullismo:** utilizzare l'IA per automatizzare o potenziare molestie online, messaggi persecutori, campagne di denigrazione o dinamiche di esclusione dai gruppi di classe.

4.4.3 Obbligo di Trasparenza e Watermarking per Uso Didattico Autorizzato

Qualora l'uso di media sintetici sia espressamente autorizzato dal docente per sole finalità didattiche o creative (es. ricostruzioni storiche guidate, progetti artistici o teatrali):

- I contenuti generati devono riportare un'etichetta visibile o un **watermarking inequivocabile** (es. "Contenuto sintetico generato tramite IA per scopi didattici"), in conformità con l'AI Act.
- È vietato utilizzare immagini, voci o dati riferiti a persone reali ed esistenti senza autorizzazione scritta della persona o dei genitori, se minore.

4.4.4 Protocollo d'Intervento Rapido in Caso di Incidenti (Allegato Operativo)

In presenza di episodi accertati o presunti di deepfake o cyberbullismo realizzato mediante IA, l'Istituto attiva immediatamente la procedura d'emergenza specificata nel Regolamento d'Istituto sul Bullismo e Cyberbullismo, segnalando tempestivamente l'accaduto al Dirigente e preservando le prove. La produzione e diffusione di deepfake denigratori, nonché l'utilizzo malevolo delle AI, costituisce infrazione disciplinare e come tale verrà sanzionata.

5. NORME PER LE FAMIGLIE E LA COMUNITÀ SCOLASTICA

L'adozione dell'IA nella scuola si basa su un patto di fiducia e trasparenza con i genitori e gli studenti. Il loro coinvolgimento è una componente strutturale della gestione dell'IA. La scuola si impegna a spiegare chiaramente alle famiglie:

- Quali strumenti di IA vengono usati e per quali obiettivi formativi.
- I limiti rigidamente fissati (inclusi il divieto di trattamento di dati personali non autorizzati e la regolamentazione dell'uso autonomo).
- Canali di Comunicazione: Informazione costante tramite il sito web istituzionale, il registro elettronico, circolari e assemblee.

5.1 Ruolo Educativo e Trasparenza Informativa

- **Partner Educativo:** le famiglie sono invitate a collaborare con la scuola nel promuovere l'uso responsabile delle nuove tecnologie anche in ambito domestico.
- **Trasparenza:** l'Istituto mantiene aggiornata una sezione dedicata del sito web e invia comunicazioni periodiche tramite Registro Elettronico.
- **Informativa per Sistemi ad Alto Rischio:** qualora si adottino sistemi ad alto rischio (in via del tutto eccezionale), verrà fornita un'informativa dettagliata e preventiva a famiglie e studenti.
- **Consenso e Autorizzazione:** l'uso didattico ordinario non richiede un consenso scritto continuo, ma solo un'informativa generale; autorizzazioni scritte specifiche saranno richieste unicamente per progetti pilota sperimentali o quando previsto dai termini di servizio del fornitore.
- Il presente Regolamento IA integra il **Patto Educativo di Corresponsabilità**.

6. GESTIONE DEL RISCHIO E SICUREZZA (AI ACT E GDPR)

6.1 Classificazione dei Rischi e Pratiche Vietate

L'Istituto classifica gli strumenti in base al caso d'uso specifico e precisa che, in ambito digitale, non è possibile garantire un "rischio zero", operando per ridurre le minacce a un **"rischio minimo o contenuto"**.

Pratiche Vietate (Rischio Inaccettabile - Art. 5 AI Act)

È vietato tassativamente l'uso di:

- Sistemi di **riconoscimento biometrico emotivo** negli ambienti scolastici e lavorativi.
- Sistemi di **social scoring** o classificazione del comportamento volte a produrre punteggi di affidabilità.

- Sistemi di sorveglianza occulta o manipolativa.
- Generazione non consensuale di contenuti sintetici riguardanti persone reali (Anti-Deepfake).

Sistemi ad Alto Rischio

L'Istituto adotta una **politica di esclusione preferenziale** per i sistemi ad alto rischio (es. quelli volti a valutare o selezionare gli studenti). L'eventuale deroga può essere prevista in casi del tutto eccezionali e richiede una rigorosa procedura di valutazione e la garanzia della non-automazione delle decisioni.

6.2 Procedure di Valutazione (Screening, DPIA e FRIA)

- **Scheda di Screening Preliminare:** condotta dal GLIA su ogni nuova applicazione.
- **DPIA (Art. 35 GDPR):** avviata solo se lo screening evidenzia un rischio elevato per la protezione dei dati personali.
- **FRIA (Art. 27 AI Act):** Valutazione d'Impatto sui Diritti Fondamentali, riservata esclusivamente alle ipotesi eccezionali di adozione di sistemi ad alto rischio da parte dell'Ente pubblico, condotta esclusivamente qualora il Dirigente Scolastico autorizzi l'impiego di sistemi ad alto rischio per finalità pubbliche.

6.3 Monitoraggio e Aggiornamento Periodico

Il Regolamento ha validità triennale ma viene revisionato **annualmente** dal Gruppo di Lavoro IA, che redige un Rapporto di Monitoraggio sulle prassi applicate, sulle criticità e sull'evoluzione tecnologica e normativa. Il presente regolamento fa parte del PTOF come allegato e segue le sue scadenze.

7. DISCIPLINA DEGLI ACCOUNT E SCELTA OPERATIVA

Le funzionalità di Intelligenza Artificiale possono venire attivate a seguito di richieste da parte dei docenti secondo un modello scritto o online definito dalla scuola, debitamente autorizzate dal dirigente che deve comunicare in forma scritta al gestore dei sistemi informatici AI le indicazioni esatte per la configurazione puntuale dei servizi.

7.1 Discrezionalità e Conformità Operativa

L'Istituto valuta in modo prudente l'opportunità di attivare nuovi progetti basati su IA. L'avvio di qualsiasi iniziativa vincola l'Istituto al rispetto formale di tutte le norme di garanzia, inclusa la presenza costante del controllo umano (Human in the Loop).

7.2 Separazione tra Account Istituzionali e Personali

7.2.1 Obbligo di Account Istituzionale

Per ogni attività che comporti l'interazione con gli studenti, la produzione di atti ufficiali o il trattamento di dati personali, è obbligatorio l'uso esclusivo dell'identità digitale e dell'account istituzionale fornito dalla scuola. È fatto divieto assoluto di utilizzare account personali per:

- Interazioni dirette o indirette con gli studenti.
- Attività gestionali ed amministrative dell'Istituto.
- Produzione di atti e comunicazioni ufficiali.
- Trattamento di qualsiasi dato personale o documento riservato.

7.2.2 Uso Personale del Docente per Materiali Generici

I docenti possono utilizzare strumenti di IA tramite account personali **esclusivamente per la preparazione autonoma di materiali didattici generici ed astratti** (es. spunti per lezioni, esercitazioni generiche), a condizione che:

1. **Non vengano inseriti dati personali** di studenti, famiglie o colleghi.
2. **Non vengano caricati elaborati degli studenti** o documenti d'ufficio riservati.
3. Il docente effettui una rigorosa **validazione umana dell'output** prima di presentarlo in classe, assumendosene la piena responsabilità.

È tassativamente vietato l'uso di account personali per qualsiasi riflessione, anche astratta, che riguardi categorie particolari di dati (salute, disabilità) o situazioni delicate di classe, per le quali deve essere utilizzato esclusivamente l'**account istituzionale configurato in modalità protetta** dal Deployer.

7.2.3 Divieto per gli studenti di utilizzare account personali

È espressamente vietato ai docenti richiedere agli studenti l'uso di account personali o piattaforme non ufficialmente autorizzate dall'Istituto per lo svolgimento dei compiti scolastici.

8. DOCUMENTI COLLEGATI E ALLEGATI OPERATIVI

Al presente Regolamento sono associati i seguenti documenti allegati ed operativi:

1. Linee guida operative per i docenti sull'uso didattico dell'IA.
2. Linee guida operative per il personale ATA e altro personale scolastico (DS, DSGA, ...) sull'uso amministrativo dell'IA.
3. Linee guida operative per gli studenti sull'uso didattico e responsabile dell'IA.

4. Informativa sul trattamento dei dati personali (GDPR).
5. Scheda di Progettazione delle Attività per lo screening preliminare del rischio e di verifica della necessità di una DPIA.
6. Registro Tecnico degli strumenti autorizzati (Elenco pubblico ed elenco completo interno).
7. Protocollo d'intervento rapido in caso di Deepfake e Cyberbullismo.
8. Progetto pilota per l'implementazione e il collaudo dell'infrastruttura Server IA Locale (Privacy-First).
9. Ulteriori disposizioni e circolari operative emanate dall'Istituzione Scolastica.

Il Dirigente Scolastico
Dott. Leandro Pellegrini