

**MIM**Ministero dell'Istruzione
e del Merito– REGIONE SICILIANA –
AMBITO TERRITORIALE DI CATANIA**Liceo Artistico Statale "Emilio Greco"**

REGOLAMENTO PER L'USO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

Approvato con delibera del Collegio dei Docenti n. 18 del 18/05/2026
Approvato con delibera del Consiglio di Istituto n. 2601 del 18/05/2026

PREMESSA

Il presente Regolamento disciplina l'utilizzo di strumenti di intelligenza artificiale (IA) nell'ambito delle attività didattiche, amministrative e organizzative d'Istituto, in conformità al quadro normativo vigente e al Piano d'Istituto per l'Intelligenza Artificiale, una volta approvato e integrato nel PTOF.

Obiettivo principale: garantire un uso etico, trasparente e responsabile dell'IA che tuteli i diritti di studenti, famiglie e personale, mantenendo la centralità della persona e la relazione educativa.

Art. 1 - Oggetto e finalità

Il presente Regolamento disciplina l'uso degli strumenti di Intelligenza Artificiale (IA) nell'ambito delle attività didattiche e amministrative dell'istituzione scolastica.

Finalità del Regolamento:

- Garantire un uso responsabile, etico e conforme alla normativa degli strumenti IA;
- Tutelare i diritti e la privacy di studenti, personale e famiglie;
- Promuovere la trasparenza e la supervisione umana nelle decisioni che coinvolgono l'IA;
- Educare la comunità scolastica all'uso consapevole delle tecnologie intelligenti;
- Valorizzare le competenze umane e il pensiero critico.

Il Regolamento si basa su:

- **Regolamento UE 2024/1689** (AI Act) – disciplina l'intelligenza artificiale a livello europeo
- **Legge nazionale** del 10 ottobre 2025 n.132 – legislazione italiana su IA
- **Decreto Ministeriale** 9 agosto 2025 – Linee guida per l'IA nelle scuole
- **Regolamento GDPR** (UE 2016/679) e **Codice Privacy** italiano (D.Lgs. 196/2003)
- **DPR 275/1999** – Autonomia delle istituzioni scolastiche
- **Piano d'Istituto per l'Intelligenza Artificiale** – approvato da Collegio Docenti e Consiglio d'Istituto

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

Art. 2 - Ambito di applicazione

Il presente Regolamento si applica a:

- **Personale docente** (a tempo indeterminato e determinato, di sostegno, supplenti);
- **Personale ATA** (assistenti amministrativi, tecnici, collaboratori scolastici);
- **Studenti** di tutti gli ordini e gradi presenti nell'istituto;
- **Dirigente Scolastico** e staff di dirigenza;
- **Collaboratori esterni** che operano su dispositivi e reti della scuola.

Il Regolamento riguarda tutti gli strumenti di Intelligenza Artificiale utilizzati per finalità scolastiche, inclusi ma non limitati a: chatbot testuali, sistemi di generazione immagini/video/audio, assistenti di programmazione, strumenti di traduzione automatica, correzione testi, analisi dati.

Art. 3 - Principi fondamentali, concetti chiave, classificazione del rischio, compiti e ruoli

a) PRINCIPI FONDAMENTALI

L'uso dell'IA nell'istituto si ispira ai seguenti principi:

ETICITÀ E CONFORMITÀ	Garantire uso etico e conforme alla normativa.
TRASPARENZA	Dichiarare sempre l'uso di IA, comunicando finalità e modalità a tutti gli interessati. Occultare l'uso di IA è vietato. Assicurare trasparenza e controllo umano integrale.
SUPERVISIONE UMANA	Ogni output IA deve essere validato e approvato da personale umano competente prima dell'uso. La responsabilità finale resta sempre del docente/personale, non dell'IA. L'IA è strumento di supporto, non sostituto. La dimensione relazionale, emotiva ed etica dell'educazione non può essere automatizzata.
PRIVACY BY DESIGN	Applicare rigorosamente i principi GDPR: minimizzazione dati personali inseriti in sistemi IA, anonimizzazione ove possibile, conservazione limitata, sicurezza adeguata. I dati personali di studenti minorenni meritano una "protezione rafforzata". Un sistema IA può avere impatto significativo su diritti e opportunità fondamentali. Esempi: sistemi per valutare gli studenti, per ammettere a percorsi formativi, per monitorare comportamenti durante gli esami.
EQUITÀ	Gli strumenti IA devono essere valutati per identificare ed evitare bias algoritmici che potrebbero discriminare studenti per genere, etnia, disabilità, lingua, condizione socio-economica. L'IA deve ridurre le disuguaglianze, prevenire discriminazioni, garantire pari opportunità di accesso.
PENSIERO CRITICO	Educare a valutare criticamente gli output IA, riconoscendo limiti e bias.
TUTELA DEI DIRITTI	Proteggere diritti fondamentali di studenti, famiglie, personale.
CHIAREZZA REGOLAMENTARE	Definire con precisione usi consentiti, vietati o sconsigliati e le procedure.
INNOVAZIONE DIDATTICA	Promuovere IA nell'educazione, rispettando la centralità della persona.
RESPONSABILIZZAZIONE	Educare il personale su opportunità e rischi.
SOSTENIBILITÀ	Privilegiare soluzioni open source, interoperabili, sostenibili economicamente e ambientalmente, che non creino dipendenza da fornitori specifici (vendor lock-in).

b) **CONCETTI CHIAVE****Intelligenza Artificiale (IA)**

Sistema automatizzato progettato per operare con autonomia variabile e generare output (previsioni, raccomandazioni, decisioni, contenuti) che influenzano ambienti fisici o virtuali.

Deployer (Utilizzatore)

Chi usa un sistema IA sotto la propria autorità. *L'istituzione scolastica è deployer dei sistemi IA usati dal personale.*

White List (Lista Bianca)

Elenco ufficiale degli strumenti IA **espressamente autorizzati** per l'uso in istituto, pubblicato sul sito web nella sezione "Intelligenza Artificiale". Solo questi strumenti si possono usare.

Black List (Lista Nera)

Elenco degli strumenti IA **esplicitamente vietati** per motivi di sicurezza, privacy, conformità normativa o inadeguatezza.

Supervisione Umana

Controllo e responsabilità umana integrale su output, decisioni e processi generati dall'IA. *Il docente/personale conserva sempre responsabilità finale.*

c) **CLASSIFICAZIONE DEL RISCHIO**

Livello	Caratteristica	Conseguenza
Inaccettabile	Viola diritti fondamentali	VIETATO ASSOLUTAMENTE
Alto Rischio	Impatta diritti e sicurezza	Autorizzazione speciale con garanzie rafforzate
Rischio Limitato	Interagisce con utenti	Autorizzazione standard + obbligo trasparenza
Rischio Minimo	Non comporta rischi significativi	Autorizzazione semplificata (White List)

d) **COMPITI E RUOLI****Cosa fa il Dirigente Scolastico**

1. **Decide** - Autorizza quali sistemi IA adottare, verificando coerenza con il PTOF e questo regolamento
2. **Garantisce** - Assicura il rispetto di tutte le norme, specialmente per sistemi ad alto rischio
3. **Forma** - Organizza corsi di formazione continua per il personale sull'uso etico e tecnico dell'IA
4. **Controlla** - Monitora l'impatto dei sistemi IA sulla comunità scolastica

Cosa fanno i Docenti e i Collaboratori esterni

1. **Mantengono il controllo** - La responsabilità pedagogica e valutativa resta sempre e solo loro. L'IA è un supporto, non un sostituto
2. **Usano l'IA come strumento** - Per personalizzare la didattica, creare materiali, innovare metodi. Nel rispetto della libertà di insegnamento
3. **Educano al pensiero critico** - Insegnano agli studenti a usare l'IA con consapevolezza, a riconoscere limiti e rischi (allucinazioni, bias, errori)
4. **Sono trasparenti** - Informano studenti e famiglie su quali strumenti IA usano e come

Cosa fa il Personale Amministrativo (ATA e DSGA)

1. **Ottimizza i processi** - Usa l'IA per gestione comunicazioni, organizzazione amministrativa, seguendo le direttive del Dirigente
2. **Protegge i dati** - Applica principi di minimizzazione e riservatezza nel trattamento dati personali attraverso sistemi IA

Cosa fanno gli Studenti

1. **Usano l'IA con onestà** - Se l'IA aiuta a fare un elaborato, lo dichiarano sempre al docente. (integrità accademica)
2. **Verificano le informazioni** - Non si fidano ciecamente. Controllano accuratezza, affidabilità e possibili bias di ciò che l'IA produce

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

3. **Pensano criticamente** - Riconoscono le allucinazioni (output errati o inventati), validano le fonti prima di usare le informazioni
4. **Segnalano problemi** - Se vedono output discriminatori, contenuti inappropriati o anomalie, informano subito docenti o Dirigente

Art. 4 - Uso dell'IA da parte dei DOCENTI e dei COLLABORATORI ESTERNI

4.1 Usi consentiti

I docenti e i Collaboratori esterni possono utilizzare strumenti di IA per le seguenti finalità, nel rispetto del presente Regolamento:

✓ USO CONSENTITO	CONDIZIONI
Preparazione materiali didattici (lezioni, schede, tracce)	Revisione critica obbligatoria prima della somministrazione
Differenziazione contenuti per studenti DSA/BES	Rispetto PDP/PEI. Dati sensibili solo se necessari e su piattaforme conformi GDPR
Traduzione testi	Verifica qualità traduzione. No dati sensibili
Generazione esempi, esercizi, quiz	Validazione didattica. Verifica accuratezza scientifica
Feedback su produzioni scritte (bozze)	Testi anonimizzati. Feedback sempre integrato da valutazione docente
Brainstorming e ideazione attività	Spunto iniziale. Personalizzazione necessaria
Creazione immagini/contenuti multimediali	Verifica diritti d'autore. Dichiarare fonte se mostrati a studenti
Ricerca e sintesi informazioni	Fact-checking obbligatorio. Citare fonti originali quando possibile
Utilizzo di procedure automatizzate e/o assistite da IA integrate in SW in utilizzo	Utilizzo di SW con licenza d'uso e acquistati o messi a disposizione dalla scuola.

4.2 Usi NON consentiti o sottoposti ad autorizzazione

✗ USO NON CONSENTITO	MOTIVAZIONE
Valutazione automatica finale senza supervisione umana	Voti e giudizi devono essere sempre attribuiti dal docente. Violazione Art. 3 AI Act (rischio alto)
Profilazione studenti senza consenso esplicito	Violazione GDPR. Necessaria informativa e consenso DPO
Inserimento dati sensibili (salute, religione, etnia) in IA non conformi	Alto rischio privacy. Serve autorizzazione DPO + strumento certificato GDPR
Sistemi di riconoscimento facciale/biometrico per controllo presenze	Rischio inaccettabile AI Act su minori. Vietato senza autorizzazioni specifiche
Orientamento scolastico/lavorativo automatizzato	Rischio alto AI Act. Serve valutazione impatto + supervisione umana rafforzata

4.3 Obblighi di trasparenza

1. **Dichiarazione uso IA:** quando si utilizzano contenuti generati da IA con gli studenti, informarli preventivamente specificando lo strumento e la finalità;
2. **Citazione fonte:** se si condividono materiali prodotti con IA, indicare sempre "Realizzato con supporto di [nome strumento IA]";
3. **Registro interventi:** documentare nel registro elettronico l'eventuale uso di strumenti IA per personalizzazione didattica su singoli studenti.

Art. 5 - Uso dell'IA da parte degli STUDENTI

5.1 Usi consentiti

Gli studenti possono utilizzare strumenti di IA per le seguenti finalità, sempre con supervisione o autorizzazione del docente:

✓ USO CONSENTITO	CONDIZIONI
Supporto allo studio (spiegazioni,	Verificare comprensione effettiva, non copiare

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

✓ USO CONSENTITO	CONDIZIONI
chiarimenti)	passivamente
Brainstorming e raccolta idee iniziali	Spunto di partenza. Elaborazione personale necessaria
Revisione ortografica/grammaticale	Dopo la stesura personale. Dichiarare l'uso al docente
Traduzione testi per comprensione	Non per sostituire il lavoro di traduzione assegnato
Ricerca e approfondimento fonti	Verificare informazioni, consultare fonti originali
Generazione bozze da rivedere con docente	Solo se previsto dal docente. Dichiarare sempre l'uso

5.2 Usi NON consentiti

✗ USO VIETATO	CONSEGUENZE
Presentare output IA come lavoro proprio senza dichiararlo	Equivale a plagio. Sanzioni disciplinari secondo Regolamento d'Istituto
Sostituzione integrale del lavoro personale	Annullamento verifica/compito. Valutazione gravemente insufficiente
Uso durante verifiche scritte/orali non autorizzato	Annullamento prova. Provvedimento disciplinare
Generazione contenuti offensivi, discriminatori, illegali	Segnalazione alla famiglia. Provvedimenti disciplinari gravi. Denuncia alla Autorità Giudiziaria.

5.3 Obbligo di dichiarazione

Gli studenti **DEVONO** sempre dichiarare l'uso di strumenti IA nei propri elaborati, specificando:

- Nome dello strumento utilizzato (es. ChatGPT, Gemini, DALL-E);
- Finalità d'uso (es. "brainstorming iniziale", "revisione ortografica", "traduzione");
- Livello di intervento (es. "10% contenuti generati da IA", "solo correzione errori").

La dichiarazione può essere inserita in nota a piè di pagina o in sezione dedicata dell'elaborato.

Art. 6 - Uso dell'IA da parte del PERSONALE ATA

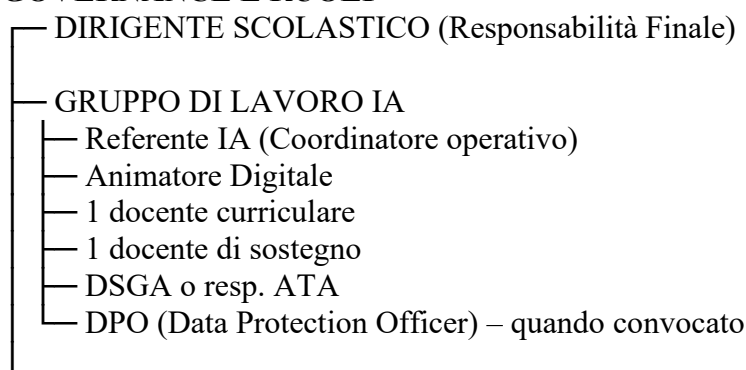
Il personale amministrativo, tecnico e ausiliario può utilizzare strumenti di IA per:

- **Bozze comunicazioni istituzionali** (revisione obbligatoria da parte del DSGA o DS);
- **Traduzione documenti amministrativi** (verifica accuratezza);
- **Supporto gestione dati** (analisi, reporting - solo dati aggregati e anonimi);
- **Assistenza tecnica** (risoluzione problemi informatici con assistenti IA).

DIVIETO ASSOLUTO: inserire dati personali di studenti, famiglie o personale in strumenti IA non autorizzati dal Gruppo di Lavoro IA e validati dal DPO.

Art. 7 - Procedure di autorizzazione

GOVERNANCE E RUOLI



- └ PERSONALE DOCENTE E ATA
- └ Utilizza strumenti White List con supervisione umana

Ruoli Principali

GRUPPO DI LAVORO IA

Compito	Frequenza
Autorizzare strumenti IA	Riunioni periodiche
Aggiornare White List / Black List	Entro 5 giorni
Monitorare implementazione Piano IA	Riunioni periodiche
Produrre report	Riunioni periodiche
Proporre modifiche Regolamento	Annuale

Funzionamento:

- Riunioni ordinarie: **minimo 1 volta al mese**
- Riunioni straordinarie: se richieste
- Quorum: **maggioranza semplice**
- Verbali obbligatori, protocollati e archiviati
- Delibere numerate progressivamente

REFERENTE IA

Docente o ATA nominato dal Dirigente con competenze digitali adeguate.

Funzioni principali:

- Coordinare operativamente il Gruppo di Lavoro
- Istruire richieste di autorizzazione degli strumenti
- Aggiornare White List e Black List
- Fornire supporto tecnico al personale
- Gestire sportello assistenza (fisico e online)
- Coordinare attività formative AI Literacy
- Redigere report periodici

DATA PROTECTION OFFICER (DPO)

Responsabile della Protezione dei Dati

Funzioni su IA:

- Consultazione obbligatoria preventiva per strumenti che trattano dati personali
- Parere vincolante su conformità GDPR
- Vigilanza su trattamenti dati con IA
- Gestione data breach e incident privacy
- Supporto su questioni privacy complesse

Audit periodico conformità GDPR

DIRIGENTE SCOLASTICO

Responsabilità:

- Conformità normativa dell'istituto come deployer di sistemi IA
- Potere di veto su autorizzazioni in casi eccezionali (motivati)
- Gestione procedimenti disciplinari per infrazioni gravi
- Rappresentanza verso autorità esterne (Garante Privacy, MIM, USR)
- Autorizzazioni provvisorie urgenti (max 30 giorni, poi ratifica Gruppo Lavoro)

7.1.1 Richiesta autorizzazione

Chiunque desideri utilizzare un nuovo strumento di IA non ancora approvato dall'istituto deve:

- **Compilare il modulo online** "Richiesta autorizzazione strumento IA" disponibile sul sito della scuola;

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

- **Specificare:** nome strumento, finalità d'uso, dati che si intendono inserire, destinatari, frequenza utilizzo;
- **Attendere risposta** entro 15 giorni lavorativi.

PROCEDURE AUTORIZZATIVE

Procedura Standard (Strumenti Rischio Minimo/Limitato)

Step 1 – Richiesta Iniziale (Docente/Collaboratore esterno/ATA richiedente)

Cosa fare:

1. Compilare integralmente **Modulo Richiesta Autorizzazione** (Allegato A disponibile su sito web)
2. Allegare:
 - Informativa privacy fornitore
 - Termini di servizio
 - Documentazione tecnica se disponibile
3. Inviare via mail al protocollo della scuola e per conoscenza al **Referente IA**.

Quando: Almeno **20 giorni lavorativi prima dell'uso previsto**

Esito: Ricevuta protocollata entro 2 giorni lavorativi

Step 2 – Istruttoria (Referente IA)

Cosa fa:

- Verifica completezza documentazione (se incompleta, richiede integrazioni entro 5 giorni)
- Compila **Scheda Valutazione Rischio Caso d'Uso** (Allegato B) entro **10 giorni**
- Consulta obbligatoriamente DPO se strumento tratta dati personali
- Effettua test funzionale se necessario
- Produce **sintesi istruttoria con raccomandazione:**
 - ✓ Favorevole
 - ✓ Favorevole con prescrizioni
 - X Contraria

Step 3 – Valutazione Collegiale (Gruppo Lavoro IA)

Cosa accade:

1. Iscrizione richiesta all'ordine del giorno della successiva riunione
2. Presentazione istruttoria da Referente IA (10-15 minuti)
3. Discussione collegiale
4. Eventuale richiesta integrazioni a richiedente (sospende istruttoria)
5. **VOTAZIONE:** Maggioranza semplice membri presenti
6. **Delibera motivata:**
 - ✓ Approvazione
 - ✓ Approvazione con prescrizioni
 - X Rigetto
 - ☒ Rinvio
7. Verbale con numero delibera progressivo

Step 4 – Comunicazione Esito (Referente IA)

Entro **3 giorni lavorativi** da delibera:

Se **APPROVATO:**

- Inserimento strumento in White List con codice WL-XXX
- Comunicazione codice
- Accesso credenziali/procedure

Se **APPROVATO CON PRESCRIZIONI:**

- Elenco dettagliato prescrizioni operative obbligatorie

Se **RESPINTO:**

- Motivazioni precise e complete
- Indicazione eventuale alternativa in White List

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

- Possibilità ripresentare richiesta se si risolvono criticità

Tempi Massimi Vincolanti:

15 giorni lavorativi dalla presentazione richiesta completa alla comunicazione esito

(Salvo necessità integrazioni documentali che sospendono i termini)

Procedura Semplificata Urgente (Casi Eccezionali)

In situazioni eccezionali documentate:

Esempio: Strumento necessario urgentemente per studente con disabilità sopraggiunta o progetto con scadenza imminente

Processo:

1. Proposta motivata da Referente IA al DS
2. **Autorizzazione provvisoria DS** (validità max 30 giorni)
3. Prescrizioni operative rafforzate
4. **Ratifica obbligatoria Gruppo Lavoro** in riunione successiva
5. Se non ratificata → revoca immediata autorizzazione

Diritti del Richiedente

- ✓ Ricevere supporto dal Referente IA per compilazione modulo
- ✓ Essere informato tempestivamente su avanzamento pratica
- ✓ Conoscere motivazioni dettagliate in caso di rigetto
- ✓ Accedere a verbale delibera Gruppo Lavoro (parte pubblica)
- ✓ Ripresentare richiesta risolvendo criticità evidenziate
- ✓ Ricevere indicazione alternativa autorizzata se disponibile

7.2 Valutazione

Il Gruppo di Lavoro IA valuta la richiesta secondo:

- **Classificazione rischio AI Act** (inaccettabile / alto / limitato / minimo);
- **Conformità GDPR** (consultazione DPO se tratta dati personali);
- **Policy privacy** (localizzazione server, termini servizio, età minima);
- **Rilevanza didattica/amministrativa** (effettiva necessità dello strumento).

7.3 Esiti possibili

- **APPROVATO** - Utilizzo libero secondo modalità indicate;
- **APPROVATO CON CONDIZIONI** - Utilizzo subordinato a specifiche prescrizioni (es. solo dati anonimi, supervisione rafforzata);
- **APPROVATO PER TEST PILOTA** - Sperimentazione limitata (1-2 mesi, classi specifiche) con monitoraggio;
- **RINVIATO** - Necessari approfondimenti (richiedente sarà contattato);
- **RESPINTO** - Non conforme a normativa o principi d'istituto (con motivazione dettagliata).

RESPINTO

Alcune pratiche sono inaccettabili perché violano diritti fondamentali. Vietate sempre, senza eccezioni (art. 5 AI Act).

- **Analisi delle emozioni** - È vietato usare IA per dedurre o analizzare stati emotivi di studenti o personale
- **Punteggio sociale** - È vietato classificare persone in base a comportamento sociale o caratteristiche personali, se ciò porta a trattamenti discriminatori

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

- **Sfruttamento vulnerabilità** - È vietato usare IA per manipolare comportamenti sfruttando età o fragilità delle persone
- **Manipolazione subliminale** - È vietato usare tecniche manipolative o ingannevoli per alterare comportamenti causando danni fisici o psicologici
- **Categorizzazione biometrica sensibile** - È vietato inferire da biometria dati sensibili come opinioni politiche, religione, orientamento sessuale

APPROVATO CON CONDIZIONI

Sistemi IA che possono impattare significativamente diritti e opportunità educative. Usabili solo seguendo procedure rigorose.

Rientrano qui i sistemi per:

- Determinare accesso o ammissione a percorsi formativi
- Valutare risultati dell'apprendimento
- Monitorare comportamento studenti durante prove

Protocollo obbligatorio per sistemi ad alto rischio

Se la scuola usa un sistema classificato ad alto rischio, deve seguire questo protocollo senza deroghe:

Passo 1: Verifica conformità del fornitore

Il Dirigente acquisisce documentazione che attesti conformità all'AI Act: dichiarazione UE e istruzioni d'uso dettagliate.

Passo 2: Valutazione d'impatto (DPIA + FRIA)

Prima di usare il sistema, sono obbligatorie due valutazioni: DPIA (protezione dati, GDPR) e FRIA (diritti fondamentali, AI Act). Analisi approfondita dei rischi per equità, non discriminazione, opportunità educative.

Passo 3: Sorveglianza umana sempre attiva

Una persona (docente, commissione, dirigente) deve monitorare costantemente il sistema. La decisione finale spetta SEMPRE all'essere umano, mai all'algoritmo. Non negoziabile.

Passo 4: Uso conforme alle istruzioni

Il personale usa il sistema seguendo scrupolosamente le istruzioni del produttore e le direttive interne. Garantisce funzionamento corretto e sicurezza.

Passo 5: Informazione completa agli interessati

Studenti e famiglie informati in modo chiaro e completo: cosa fa il sistema, come funziona, perché lo usiamo, come influenza decisioni che li riguardano.

APPROVATO (MA DA UTILIZZARE CON TRASPARENZA E OPPORTUNAMENTE)

La maggior parte degli strumenti IA per supporto didattico, ricerca informazioni, creazione contenuti, efficienza amministrativa. Uso incoraggiato, rispettando principi generali di trasparenza, etica e tutela dati.

Esempi comuni:

- Assistenti di scrittura e correzione
- Generatori di immagini per materiali didattici
- Traduttori automatici
- Sistemi di ricerca e organizzazione informazioni
- Tool per efficienza amministrativa

CATEGORIA A: USI VIETATI ASSOLUTAMENTE (Rischio Inaccettabile)

Questi usi sono **PROIBITI SENZA ECCEZIONE**:

a) Sorveglianza Biometrica Automatizzata



VIETATO: Sistemi di identificazione automatica tramite

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

- Riconoscimento facciale
- Riconoscimento dell'iride
- Riconoscimento vocale
- Altre caratteristiche biometriche

Finalità monitoraggio continuo studenti

b) Social Scoring (Valutazione Automatica Comportamento)

❌ **VIETATO:** Sistemi che assegnano automaticamente "punteggi comportamentali" a studenti con conseguenze automatiche (penalizzazioni, sanzioni, esclusioni)

Esempio vietato: App che assegna punteggi comportamento con penalizzazioni automatiche

c) Manipolazione Subliminale

❌ **VIETATO:** Sistemi progettati per manipolare il comportamento di studenti attraverso tecniche subliminali oltre la loro consapevolezza

d) Sfruttamento di Vulnerabilità

❌ **VIETATO:** Sistemi che sfruttano vulnerabilità specifiche di minori (età, disabilità, situazione sociale) per distorcere il comportamento con danni potenziali

e) Valutazione Scolastica Automatica Finale

❌ **VIETATO:** Sistemi che assegnano voti definitivi, decidono ammissioni/bocciature, orientamenti **senza revisione umana integrale**

Conseguenze violazione:

- Infrazione disciplinare **GRAVISSIMA**
- Responsabilità personale del dipendente
- Potenzialmente configurante illeciti penali
- Sanzione: **sospensione dal servizio o licenziamento**

CATEGORIA B: ALTO RISCHIO (Autorizzazione Speciale)

Questi usi richiedono **autorizzazione speciale con garanzie rafforzate:**

- Sistemi che determinano ammissione studenti a specifici corsi/cicli
- Sistemi di valutazione automatizzata apprendimenti (impatto $\geq 30\%$ sul voto finale)
- Sistemi di orientamento con raccomandazioni vincolanti
- Sistemi di monitoraggio comportamentale con conseguenze disciplinari automatiche

Condizioni autorizzazione:

- ✓ DPIA (Data Protection Impact Assessment) obbligatoria
- ✓ Parere DPO favorevole (vincolante)
- ✓ Formazione specifica utilizzatori (≥ 15 ore)
- ✓ Log completi attività tracciati
- ✓ Diritto contestazione sempre garantito
- ✓ Supervisione umana documentata
- ✓ Revisione semestrale funzionamento

Nota: In Fase I (2026-2027), **probabilmente NESSUN sistema alto rischio** sarà autorizzato. Valutazione eventuale dalla Fase II (2027+).

CATEGORIA C: RISCHIO LIMITATO (Autorizzazione Standard + Trasparenza)

Questi usi richiedono **autorizzazione standard + dichiarazione esplicita uso IA:**

Usi Consentiti:

- **Chatbot didattici e assistenti virtuali** – interagiscono con studenti per rispondere domande, fornire spiegazioni
- **Trascrizione automatica lezioni** – quando audio include voci studenti identificabili
- **Feedback personalizzati automatizzati** – l'IA analizza elaborati e genera commenti
- **Raccomandazione contenuti didattici** – IA suggerisce materiali e percorsi personalizzati

Prescrizioni Obbligatorie:

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

1. ✓ Autorizzazione Gruppo Lavoro IA
2. ✓ **Dichiarazione esplicita uso IA a studenti e famiglie sempre**
3. ✓ Supervisione umana docente sempre presente
4. ✓ Dati personali solo se strettamente necessari (base giuridica documentata)
5. ✓ Possibilità revisione umana sempre disponibile

Sanzione mancata dichiarazione: Infrazione media – Richiamo scritto (prima volta), multa (recidiva)

CATEGORIA D: RISCHIO MINIMO (Autorizzazione Semplificata)

La **maggioranza degli strumenti Fase I** rientra qui. Autorizzazione tramite White List semplificata.

USI DIDATTICI (Preparazione Materiali Docente):

- IA generative testuali per creare esercizi, verifiche, spiegazioni (es. ChatGPT Plus, Claude, Gemini con account istituzionale)
- Traduttori automatici per materiali didattici e comunicazioni (es. DeepL Pro, Google Translate)
- Sintesi vocale (TTS) per accessibilità studenti DSA, ipovedenti
- Generazione mappe concettuali, schemi, riassunti
- Revisione linguistica e correttori ortografici/grammaticali avanzati
- Semplificazione testi per studenti BES/DSA

USI AMMINISTRATIVI:

- Redazione bozze circolari e comunicazioni standard
- Traduzione comunicazioni per famiglie straniere
- Sintesi documenti lunghi per uso interno
- Generazione template moduli ripetitivi

Prescrizioni Obbligatorie:

1. ✓ Strumento presente in **White List con codice WL-XXX**
2. ✓ **Formazione AI Literacy Base completata** (attestato)
3. ✓ **DIVIETO ASSOLUTO:** Inserire dati sensibili studenti (nomi+voti nominativi, diagnosi, situazioni familiari, codici fiscali)
4. ✓ **Validazione output prima utilizzo**
5. ✓ **Dichiarazione uso IA** quando materiali usati con studenti (nota piè pagina o comunicazione verbale)
6. ✓ **Utilizzo account istituzionale** (non account personale docente)

Sanzione uso strumento non autorizzato: Richiamo verbale (prima infrazione), richiamo scritto (recidiva)

Art. 8 – WHITE LIST E BLACK LIST

White List – Strumenti Autorizzati

Dove Trovarla?

- **Sito web istituzionale** → Sezione "Intelligenza Artificiale" → "Strumenti Autorizzati"
- Accessibile a tutto il personale senza autenticazione
- **Formati: pagina web sempre aggiornata + PDF scaricabile**

Contenuti Scheda Strumento:

Ogni strumento autorizzato contiene:

Campo	Contenuto
Codice univoco	WL-001, WL-002, ecc.
Nome e produttore	Esempio: ChatGPT Plus (OpenAI)
Versione	Es. GPT-4

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

Categoria rischio	Minimo / Limitato / Alto
Finalità consentite	Elenco dettagliato usi
Prescrizioni operative	Obblighi specifici
Divieti specifici	Cosa NON fare
Formazione richiesta	Ore e contenuti
Modalità accesso	URL, credenziali, procedure
Trattamento dati	Sì/No, quali dati, garanzie
Data autorizzazione	Delibera Gruppo Lavoro
Referente tecnico interno	Chi contattare
Link documentazione	Documentazione completa

Aggiornamento:

- **Responsabile:** Referente IA
- **Tempistica:** Entro 5 giorni lavorativi da delibera nuova autorizzazione
- **Comunicazione:** Email personale a tutto per ogni aggiornamento significativo

Solo gli strumenti in White List si possono usare. Ciò che non è espressamente autorizzato è vietato.

Black List – Strumenti Vietati

Finalità:

Prevenire uso di strumenti noti ma non conformi per:

- Violazione privacy (dati usati per training, venduti, senza GDPR)
- Rischi sicurezza (vulnerabilità note, malware, data breach precedenti)
- Rischi inaccettabili (sorveglianza, manipolazione)
- Qualità inadeguata (output troppo inaffidabili)
- Costi eccessivi

Contenuti Black List:

Campo	Contenuto
Nome strumento	Quale è vietato
Produttore	Chi lo offre
Motivo divieto	Spiegazione dettagliata
Data inserimento	Quando è stato vietato
Alternativa autorizzata	Strumento sostitutivo in White List

Esempi Tipici:

- ChatGPT versione gratuita (dati usati per training)
- Chatbot online anonimi senza identificazione fornitore
- App generazione immagini con copyright dubbio
- Strumenti con termini servizio che violano GDPR

Conseguenze uso Black List: Infrazione media-grave – Richiamo scritto, multa, sospensione breve secondo gravità

Grey Area – Strumenti Non Classificati

Regola inderogabile: Strumenti non in White List né Black List **non possono essere usati** fino a classificazione formale.

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

Come fare? Compilare Modulo Richiesta Autorizzazione (Allegato A) → Procedura autorizzativa
→ Delibera Gruppo Lavoro entro 15 giorni lavorativi

Art. 9 - Protezione dati personali

9.1 Principi GDPR

- **Minimizzazione dati:** inserire in sistemi IA solo i dati strettamente necessari alla finalità;
- **Anonimizzazione:** rimuovere nomi, cognomi e identificativi quando possibile;
- **Consenso informato:** per trattamenti su dati sensibili di minori, richiedere consenso genitori tramite informativa specifica;
- **Server UE:** preferire strumenti con dati localizzati in Unione Europea;
- **Diritto alla cancellazione:** utilizzare strumenti che permettano eliminazione dati su richiesta.

9.2 Dati sensibili

È VIETATO inserire in strumenti IA non validati dal DPO le seguenti categorie di dati:

- Origine razziale o etnica;
- Opinioni politiche, religiose, filosofiche;
- Dati relativi alla salute (diagnosi, PEI dettagliati, certificazioni mediche);
- Dati genetici o biometrici;
- Vita sessuale od orientamento sessuale.

I dati personali, specialmente quelli dei minori, sono intoccabili. Massima tutela in conformità totale al GDPR.

Principi base (art. 5 GDPR)

Ogni trattamento dati con IA deve rispettare:

- **Liceità, correttezza, trasparenza** - Tutto alla luce del sole
- **Limitazione finalità** - Dati raccolti per scopi precisi e dichiarati
- **Minimizzazione** - Solo i dati strettamente necessari
- **Esattezza** - Dati corretti e aggiornati
- **Limitazione conservazione** - Non conserviamo più del necessario
- **Integrità e riservatezza** - Sicurezza massima

Privacy by Design e by Default

Selezioniamo solo sistemi IA che integrano protezione dati fin dalla progettazione e per impostazione predefinita. Trattiamo solo dati essenziali per ogni specifica finalità educativa o amministrativa.

Informativa agli interessati

Forniamo sempre informativa chiara, concisa e comprensibile sul trattamento dati personali da parte di sistemi IA (art. 13-14 GDPR). Niente gergo tecnico: informazione accessibile a tutti.

Tutela rafforzata per i minori

Il GDPR considera i minori soggetti vulnerabili meritevoli di specifica protezione. Massima attenzione quando trattiamo loro dati. Se necessario, richiediamo consenso di chi esercita responsabilità genitoriale.

Diritto di non partecipazione

Studenti e famiglie possono rifiutare che i dati personali siano usati per addestrare modelli IA. Il rifiuto non pregiudica in alcun modo l'accesso ai servizi educativi e agli strumenti didattici. Diritto garantito e gestito chiaramente.

Art.10 – OBBLIGHI E DIRETTI DEL PERSONALE

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

OBBLIGHI GENERALI PER TUTTO IL PERSONALE

1 Formazione AI Literacy

Cosa fare:

- Completare **Corso AI Literacy Base** (6 ore)
- **Entro dicembre 2026** – target: 70% personale
- Superare test valutazione finale e conseguire attestato nominativo
- Partecipare aggiornamento annuale (minimo 3 ore/anno)

2 Uso Esclusivo Strumenti Autorizzati

- ✓ Consultare **White List** sul sito web prima di usare nuovo strumento IA
- ✓ Utilizzare **SOLO** strumenti presenti in White List con codice WL-XXX
- X **MAI** usare strumenti in Black List
- ✓ Richiedere autorizzazione preventiva per strumenti non classificati

3 Supervisione Umana Integrale e CRITICA

Obblighi fondamentali:

- **Validare SEMPRE** ogni output IA prima dell'uso con studenti o in documenti ufficiali
- **Verificare:**
 - ✓ Accuratezza contenuti
 - ✓ Completezza
 - ✓ Appropriatelyzza
 - ✓ Assenza di errori o bias
- **Correggere, integrare, personalizzare** con competenza professionale
- **NON delegare responsabilità finale all'IA**
- La responsabilità **resta sempre del docente/personale**

4 Dichiarazione Uso IA (Obbligo Trasparenza) CRITICA

Quando: Quando materiali didattici o documenti sono elaborati con supporto IA

Come:

Materiali scritti:

- Nota a piè di pagina: *"Materiale elaborato con supporto di [nome strumento IA codice WL-XXX], validato da [nome docente], data [/]"*

Comunicazione verbale con studenti:

- Informare oralmente che l'attività utilizza strumenti IA

Registro elettronico:

- Annotazione quando significativo

Sanzione: Omissione = Infrazione media – Richiamo scritto (prima volta), multa (recidiva)

5 Rispetto Procedure Autorizzative

- ✓ Presentare richiesta formale per ogni nuovo strumento (Allegato A)
- ✓ Compilare integralmente moduli richiesti
- ✓ Attendere autorizzazione formale scritta prima dell'uso
- X Non usare strumenti "in prova" senza autorizzazione

PRESCRIZIONI SPECIFICHE PROTEZIONE DATI (OBBLIGATORIE)

6 DIVIETO ASSOLUTO: Dati Sensibili Studenti

È tassativamente VIETATO inserire in strumenti IA:

- X Nomi e cognomi completi studenti minorenni
- X Codici fiscali, numeri documento identità
- X Diagnosi mediche, certificazioni DSA/BES nominative
- X Informazioni sanitarie, terapie, situazioni cliniche
- X Situazioni familiari, sociali, economiche personali identificabili
- X Appartenenza etnica, religiosa, politica

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

X Orientamento sessuale

X Voti nominativi (nome studente + voto numerico associato)

X Immagini, audio, video studenti senza consenso informato specifico

Eccezione unica: Solo strumenti espressamente autorizzati per trattamento dati personali con parere DPO favorevole

Sanzione: Infrazione **GRAVE** – Sospensione dal servizio o licenziamento per infrazioni gravissime

7 Preferenza Dati Anonimi/Aggregati

✓ CORRETTO	X ERRATO
"Preparare esercizi matematica livello medio per classe 3A"	"Preparare esercizi per Mario Rossi, livello basso"
"La classe ha media 6.5 in storia"	"Mario 5, Lucia 8, Giovanni 7 in storia"
Se necessario: "Studente A", "Lucia" (senza cognome)	Nome + cognome + dati identificativi

8 Minimizzazione Dati

- Inserire **SOLO** dati strettamente necessari alla finalità specifica
- Non caricare elenchi classi completi se bastano informazioni parziali
- Cancellare dati da sistemi IA appena non più necessari
- Non conservare cronologie/log con dati personali oltre il necessario

9 Credenziali Personali e Sicurezza

- ✓ Utilizzare esclusivamente **proprie credenziali** (username + password personali)
- X **DIVIETO ASSOLUTO** di condivisione credenziali con colleghi
- ✓ Fare **LOGOUT** sempre al termine utilizzo
- ✓ Non lasciare dispositivi incustoditi con sessioni IA aperte
- ✓ **Segnalare IMMEDIATAMENTE** smarrimento credenziali o accessi sospetti a Referente IA e DSGA

10 Segnalazione Immediata Criticità

Segnalare TEMPESTIVAMENTE a Referente IA e DPO:

Malfunzionamenti gravi degli strumenti

Output inappropriati, discriminatori, palesemente errati

Sospette violazioni di sicurezza, accessi non autorizzati

Data breach: perdita, diffusione non autorizzata, accesso improprio a dati personali

Difficoltà operative significative

Comportamenti anomali degli strumenti

OBBLIGHI SPECIFICI PERSONALE DOCENTE

- ✓ Integrare uso IA nella programmazione didattica coerente con PTOF e Indicazioni Nazionali
- ✓ Dichiarare uso IA in registro elettronico quando materiali utilizzati con studenti
- ✓ Informare coordinatori e famiglie quando attività strutturate coinvolgono significativamente IA
- ✓ **Valutare sempre autonomamente studenti** – non delegare valutazione sommativa finale a sistemi automatici
- ✓ Promuovere uso critico, consapevole ed etico dell'IA presso studenti
- ✓ Educare studenti a riconoscere output IA, identificarne limiti, usarla responsabilmente

OBBLIGHI SPECIFICI PERSONALE ATA

- ✓ Utilizzare IA **SOLO** per finalità amministrative autorizzate (comunicazioni, modulistica, traduzioni, organizzazione)

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

- ✓ Non inserire dati sensibili personale dipendente o studenti in strumenti non specificamente autorizzati
- ✓ Verificare conformità output prima diffusione comunicazioni ufficiali
- ✓ Archiviare correttamente documenti prodotti con IA secondo procedure segreteria

DIRITTI DEL PERSONALE

Accanto agli obblighi, il personale ha diritto a:

- ✓ Ricevere **formazione gratuita e adeguata**, durante orario lavorativo quando possibile
- ✓ Accedere a **supporto tecnico qualificato** dal Referente IA (sportello, email, telefono)
- ✓ Consultare **White List, Black List, documentazione sempre aggiornata**
- ✓ Proporre nuovi strumenti e ricevere **risposta motivata entro 15 giorni**
- ✓ Essere ascoltato su difficoltà e criticità **senza conseguenze negative**
- ✓ Ricevere **tempo adeguato** per apprendere nuovi strumenti (curva apprendimento fisiologica)
- ✓ Partecipare a **decisioni strategiche** attraverso organi collegiali

10.1 Violazioni

In caso di sospetta violazione privacy (es. dati sensibili condivisi erroneamente), contattare IMMEDIATAMENTE:

- **DPO (Responsabile Protezione Dati):** gdpr@netsenseweb.com
- **Referente IA:** ia@liceoartisticocatania.it

Principi Generali

Il sistema sanzionatorio si ispira a:

- **Gradualità:** Sanzioni proporzionate alla gravità, recidiva, dolo vs colpa
- **Proporzionalità:** Conseguenze adeguate al danno potenziale o effettivo
- **Rieducatività:** Finalità formativa per infrazioni lievi, non meramente punitiva
- **Trasparenza:** Dipendente informato di contestazione con diritto di controdeduzioni
- **Giusto processo:** Garanzie procedurali CCNL Scuola completamente rispettate
- **Autonomia responsabilità:** Diverse forme di responsabilità (disciplinare, civile, penale) sono autonome e possono cumularsi

CATEGORIA A – Infrazioni Lievi

Cosa configura infrazione lieve:

- a) Prima violazione isolata: uso occasionale di strumento IA non in White List ma oggettivamente innocuo (es. correttore ortografico online), senza dati personali, senza diffusione contenuti problematici
- b) Omessa dichiarazione uso IA in materiale didattico (prima volta, senza conseguenze negative)
- c) Mancata consultazione White List prima nuovo strumento, senza danni
- d) Ritardo compilazione/presentazione modulo richiesta senza conseguenze operative
- e) Mancata partecipazione singola sessione formazione obbligatoria senza giustificazione valida

Sanzioni:

- **Prima infrazione:** Richiamo verbale informale da DS – nessuna annotazione fascicolo
- **Recidiva:** Richiamo scritto con annotazione fascicolo

Procedura:

1. Segnalazione infrazione al DS
2. Colloquio DS-dipendente (contraddittorio informale)
3. Richiamo verbale OPPURE scritto
4. Eventuale formazione integrativa

CATEGORIA B – Infrazioni Medie

Cosa configura infrazione media:

- a) Uso reiterato (≥ 3 volte) di strumenti non autorizzati dopo richiami precedenti
- b) Inserimento dati NON sensibili studenti (nomi+classe senza voti/diagnosi) in strumenti non autorizzati, senza danni

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

- c) Mancata supervisione output IA con diffusione contenuti imprecisi/inappropriati a studenti, senza danni gravi
- d) Condivisione credenziali personali con colleghi
- e) Omissione sistematica e reiterata dichiarazione uso IA dopo richiami
- f) Rifiuto prolungato senza giustificazione di partecipare formazione obbligatoria
- g) Uso strumenti Black List per negligenza (non dolo), senza conseguenze gravi

Sanzioni:

- **Multa:** 4-8 ore di retribuzione
- **Sospensione dal servizio:** 1-10 giorni con retribuzione ridotta

Procedura:

1. Contestazione formale scritta entro 20 giorni da conoscenza fatto
2. Controdeduzioni dipendente entro 5 giorni
3. DS valuta e decide sanzione entro 15 giorni
4. Comunicazione provvedimento motivato
5. Annotazione fascicolo personale
6. Ricorso possibile entro 15 giorni

CATEGORIA C – Infrazioni GRAVI

Cosa configura infrazione grave:

- a) Inserimento **dati sensibili studenti** (diagnosi cliniche, situazioni familiari, certificazioni sanitarie, dati biometrici) in strumenti non autorizzati → **VIOLAZIONE PRIVACY GRAVISSIMA**
- b) Uso sistemi **rischio inaccettabile** (sorveglianza biometrica, social scoring, manipolazione) → Violazione art. 5 AI Act
- c) **Decisioni automatizzate finali** senza supervisione umana con conseguenze negative documentate (valutazione delegata a IA con errori, ammissioni/esclusioni automatiche)
- d) **Data breach colposo grave** derivante da uso improprio IA con impatto su diritti studenti/personale
- e) Falsificazione documentazione per ottenere autorizzazioni indebite
- f) Recidiva sistematica infrazioni medie dopo sanzioni precedenti
- g) Uso **doloso** (intenzionale) strumenti Black List conoscendo rischi

Sanzioni:

- **Sospensione dal servizio:** 11 giorni a 6 mesi con privazione totale/parziale retribuzione
- **Licenziamento con preavviso:** Fatti gravissimi che ledono rapporto fiduciario
- **Licenziamento senza preavviso:** Fatti di rilevanza penale (es. diffusione illecita dati art. 167-bis Codice Privacy)

Segnalazione obbligatoria esterna:

Data breach → Notifica Garante Privacy entro 72h

Reati → Denuncia Autorità giudiziaria

Danno erariale → Segnalazione Procura Corte dei Conti

Circostanze Attenuanti e Aggravanti

ATTENUANTI (riducono sanzione):

- Prima violazione assoluto, precedente condotta irreprensibile
- Collaborazione immediata dopo rilevazione
- Ammissione spontanea errore con impegno rimedio
- Assenza danni concreti
- Insufficiente formazione ricevuta
- Errore scusabile in buona fede

AGGRAVANTI (aumentano sanzione):

- Recidiva specifica (stessa infrazione già sanzionata)
- Reiterazione nonostante richiami
- Dolo (intenzionalità), premeditazione
- Occultamento fatti, falsificazione
- Danno grave effettivo
- Violazione dopo diffide esplicite
- Abuso posizione di autorità

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

- Coinvolgimento studenti in comportamenti illeciti

Art. 11 - Formazione e supporto

11.1 Formazione obbligatoria

A tutto il personale docente e ATA viene data la possibilità di partecipare alla formazione base (6 ore) su:

- Cos'è l'IA e come funziona (LLM, prompt engineering);
- Potenzialità e limiti (allucinazioni, bias);
- Privacy, GDPR e AI Act;
- Uso responsabile e presente Regolamento.

11.2 Supporto continuo

L'istituto mette a disposizione:

- **Sportello IA:** Animatore Digitale disponibile per consulenze;
- **Repository risorse:** sezione dedicata su sito scuola con tutorial, FAQ, esempi prompt;
- **Email assistenza:** per dubbi su Regolamento, autorizzazioni, problemi tecnici.

Art. 12 - Sanzioni

12.1 Violazioni lievi

Mancata dichiarazione uso IA (prima volta), uso non autorizzato di strumento a basso rischio:

- **Per docenti/ATA:** richiamo verbale/scritto + obbligo formazione integrativa;
- **Per studenti:** richiamo formale + eventuale riduzione voto elaborato.

12.2 Violazioni gravi

Condivisione dati sensibili con IA non autorizzata, plagio sistematico, violazione privacy GDPR:

- **Per docenti/ATA:** provvedimenti disciplinari secondo CCNL, possibile segnalazione al Garante Privacy;
- **Per studenti:** sospensione da 1 a 5 giorni + annullamento prove + coinvolgimento famiglia.

12.3 Violazioni gravissime

Uso IA per generare contenuti illegali, diffamatori, discriminatori; profilazione non autorizzata di minori:

- **Sanzioni disciplinari massime** previste da Regolamento d'Istituto e CCNL;
- **Possibile denuncia** alle autorità competenti se configurano reato.

Art. 13 - Monitoraggio e revisione

Il Gruppo di Lavoro IA:

- Monitora l'applicazione del Regolamento tramite questionari trimestrali;
- Relaziona semestralmente al Collegio Docenti su criticità e proposte miglioramento;
- Aggiorna il Regolamento annualmente o in caso di modifiche normative significative.

Revisione e Aggiornamento

Frequenza: Almeno annuale

Motivi revisione:

- Modifiche normative rilevanti
- Evoluzione tecnologica
- Criticità applicative emerse
- Proposte migliorative da personale, famiglie, studenti
- Esiti monitoraggio e audit

Procedura:

- Modifiche sostanziali: Stesso iter approvazione iniziale
- Modifiche minori: Solo Gruppo Lavoro + ratifica DS
- Versioni: 1.0 → 1.1 (minori) → 2.0 (sostanziali)
- Storico modifiche documentato con data, versione, sintesi

ARTICOLO 14 – DISPOSIZIONI FINALI E TRANSITORIE

Firmato digitalmente da ANGELA ROSA MARIA PISTONE

Entrata in Vigore

Il Regolamento entra in vigore il **04 giugno 2026** (data pubblicazione sito web dopo approvazione organi).

Periodo Transitorio (Primo Mese)

Nel primo mese di applicazione (maggio 2026) si applica regime di **maggiore tolleranza**:

- ✓ Solo richiami verbali informativi, nessuna sanzione formale
- ✓ Finalità: permettere al personale piena consapevolezza regole
- **Eccezione:** Infrazioni gravi sanzionate anche in periodo transitorio

Norme Abrogate

Sono abrogate tutte le disposizioni interne incompatibili con il presente Regolamento.

Restano in vigore:

- Regolamento d'Istituto generale (per aspetti non IA)
- Codice Disciplinare CCNL Scuola
- Patto di Corresponsabilità Educativa (integrato su uso IA studenti)
- Informativa privacy già adottate (integrate con Allegati C, D)

Pubblicazione e Conservazione

- ✓ Pubblicato permanentemente sul sito web istituzionale
- ✓ Conservato in originale agli atti segreteria
- ✓ Distribuito a tutto il personale (copia digitale via email)
- ✓ Reso accessibile a famiglie e studenti (sintesi divulgativa)

Interpretazione Autentica

In caso di dubbi interpretativi, l'interpretazione autentica spetta al **Gruppo Lavoro IA con parere vincolante DPO** su aspetti privacy.

Interpretazioni rilevanti sono documentate e pubblicate come **FAQ sul sito web**.

Prevalenza Norme Sovraordinate

In caso di contrasto tra questo Regolamento e normativa sovraordinata (leggi, regolamenti europei/nazionali, CCNL), **prevale la norma sovraordinata**.

Tutti i membri della comunità scolastica sono tenuti al rispetto delle disposizioni in esso contenute.

PUBBLICATO sul sito web istituzionale in data 04/06/2026

Catania, lì 03/06/2026

Il Dirigente Scolastico

Prof.ssa Angela Rosa Maria Pistone

(Il documento è firmato digitalmente ai sensi del D.Lgs. 82/2005 s.m.i. e norme collegate e sostituisce il documento cartaceo e la firma autografa)

VISTO – REFERENTE IA

VISTO PER LA CONFORMITÀ PRIVACY – DPO



Firmato digitalmente da ANGELA ROSA MARIA PISTONE

APPENDICE: FAQ RAPIDE

D: Posso usare ChatGPT gratuito per lezioni?

A: NO. Solo versioni autorizzate in White List. ChatGPT free è in Black List (dati usati per training). Usare ChatGPT Plus con account istituzionale solo se in White List.

D: Come dichiaro uso IA ai genitori?

A: Nota a piè di pagina: "Materiale elaborato con supporto di [nome IA codice WL-XXX], validato da [nome docente], data []". O comunicazione verbale se attività in classe.

D: Posso usare IA per assegnare i voti automaticamente?

A: NO ASSOLUTO. Valutazione finale deve essere sempre umana. IA può suggerire feedback, non assegnare voti finali.

D: Cosa faccio se un collega usa strumento non autorizzato?

A: Segnala al Referente IA o DS. Non è una spia, è tutela dell'istituto.

D: Posso condividere mia password IA con un collega?

A: NO ASSOLUTO. Vietato. Ogni persona ha credenziali personali.

D: Come inserisco nome studente in IA?

A: Preferibilmente non farlo. Se necessario: pseudonimo "Studente A", "Lucia" (senza cognome). MAI nome+cognome+dati identificativi.

Documento aggiornato: Maggio 2026

Versione: 1.0

Prossima revisione: Dicembre 2026