# REGOLAMENTO PER L'USO DELL'INTELLIGENZA ARTIFICIALE (IA) I. C. S. “A.B. SABIN” CAPISTRELLO

I.C.- "ALBERT BRUCE SABIN"-CAPISTRELLO
Prot. 0003085 del 14/05/2026
I (Uscita)

## INTRODUZIONE E QUADRO STRATEGICO

Il presente documento costituisce il Regolamento interno per l'uso dell'Intelligenza Artificiale (IA) e dell'IA Generativa (GenAI) da parte di tutte le componenti della Comunità Scolastica (Dirigente, Personale Docente, Personale ATA e Studenti). L'integrazione di queste tecnologie rappresenta una trasformazione profonda, superando la semplice digitalizzazione per abbracciare un modello di "intelligenza aumentata" che richiede una governance etica e una pianificazione strategica rigorosa.

La diffusione di strumenti come ChatGPT, Gemini e Copilot impatta irreversibilmente l'attività didattica e amministrativa, promettendo di ottimizzare l'efficienza e la qualità dei servizi, ma portando con sé profili di rischio significativi, in particolare riguardo alla privacy, all'equità e alla responsabilità decisionale. L'obiettivo primario di questo Regolamento è duplice: massimizzare l'efficacia e l'efficienza dei processi didattici e amministrativi, promuovendo un uso progressivo, critico e innovativo dell'IA, pur garantendo il pieno rispetto della normativa nazionale ed europea e tutelando i diritti fondamentali della persona.

## TITOLO I: DISPOSIZIONI GENERALI E QUADRO NORMATIVO

### Art. 1: Obiettivi, Finalità e Principio di Intelligenza Aumentata

Il Regolamento si fonda sul principio pedagogico e organizzativo dell'**Intelligenza Aumentata** (IAu), un approccio che concepisce l'IA come un *ausilio* o un *toolkit* per estendere le capacità umane, non per sostituirle. L'IA deve supportare la comprensione, stimolare la curiosità e aiutare nella rielaborazione dei contenuti, evitando l'uso passivo e non dichiarato.

Le finalità includono:

1. **Potenziamento Cognitivo:** Utilizzare l'IA per personalizzare i percorsi di apprendimento, fornire feedback immediato e potenziare il pensiero critico e creativo negli studenti.
2. **Efficientamento Organizzativo:** Ottimizzare l'uso delle risorse scolastiche e automatizzare compiti amministrativi ripetitivi, riducendo il carico di lavoro del personale.
3. **Governance Etica:** Stabilire un quadro etico per l'uso dell'IA che garantisca trasparenza, equità, robustezza e rispetto della persona, evitando che l'IA sostituisca gli elementi umani e sociali (relazioni, empatia) che sono indispensabili nel contesto educativo.

## Art. 2: Riferimenti Normativi, Ambito di Applicazione e Termini Chiave

Il presente Regolamento si applica a tutte le attività e a tutti gli attori della comunità scolastica. L'istituzione si conforma ai seguenti riferimenti normativi e quadri di indirizzo:

1. **Normativa Europea:** Regolamento UE 2024/1689 (AI Act) [1], Regolamento UE 2016/679 (GDPR) [1] e Direttiva NIS 2.[1] La data di adeguamento generale agli obblighi dell'AI Act, per la maggior parte delle scuole, è fissata al 2 agosto 2026.[1]
2. **Normativa Nazionale:** LEGGE 23 settembre 2025 , n. 132. Disposizioni e deleghe al Governo in materia di intelligenza artificiale, D.Lgs 196/2003, c.d. "Codice Privacy", Codice dell'Amministrazione Digitale (CAD), Linee guida MIM per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche ( Decreto Ministeriale n. 166 del 9 agosto 2025, aggiornato il 29.98.2025) e Linee Guida AgID sull'adozione dell'IA nella Pubblica Amministrazione (PA).

Ai fini del presente Regolamento, si definiscono:

| Termine Chiave | Definizione di Riferimento | Rilevanza per la Scuola |
|---|---|---|
| **Sistema di IA** | Sistema automatizzato con autonomia variabile che produce output (previsioni, contenuti, raccomandazioni). | Obbliga a valutare il rischio e definire misure di controllo umano. |
| **Allucinazione dell'IA** | Fenomeno per cui il sistema genera informazioni false, imprecise o incoerenti ma presentate come plausibili. | Sottolinea la necessità imprescindibile della verifica umana e del pensiero critico. |
| **Istituzione Scolastica** | Agisce prevalentemente come **Deployer** (Utilizzatore) di sistemi IA di terze parti (es. Google, Microsoft). | Richiede l'obbligo di monitorare e verificare la conformità dei sistemi adottati. |

Un punto cruciale è la comprensione del ruolo che la scuola riveste nell'adozione di questi strumenti. Utilizzando software forniti da grandi aziende tecnologiche, l'istituzione scolastica assume il ruolo di **Deployer** (o Utilizzatore) ai sensi della normativa europea. Tale qualifica impone al Dirigente Scolastico, in qualità di Titolare del Trattamento e responsabile dell'innovazione digitale, l'obbligo di condurre valutazioni d'impatto approfondite (FRIA/DPIA) sui sistemi classificati ad Alto Rischio e di garantire la

verifica della conformità dei sistemi forniti esternamente. Questo posizionamento sposta l'onere della mitigazione del rischio sulla governance interna della scuola, indipendentemente dalle garanzie offerte dai fornitori esterni.

### Art. 3: Classificazione del Rischio e Approccio Cautelativo

Il Regolamento adotta il sistema di classificazione del rischio stabilito dall'AI Act (Inaccettabile/Vietato, Alto, Limitato, Minimo/Nullo) per determinare le misure di governance e di sicurezza da applicare.

La Dirigenza Scolastica,per prevenire usi non controllati o non documentati, adotta il seguente principio cautelativo per l'avvio dell'anno scolastico:

**Sospensione Temporanea** dell'uso di strumenti di IA per tutte le attività (didattiche o amministrative) che implichino il trattamento di **dati personali** (studenti, docenti, personale ATA, famiglie), **a meno che lo strumento non sia stato formalmente autorizzato dal Dirigente Scolastico su proposta del Gruppo IA e previa DPIA/FRIA.** La sospensione permane fino alla definizione di Policy, Governance e Misure Tecniche idonee a gestire i rischi associati.

## TITOLO II: GOVERNANCE, ETICA E GESTIONE DEL RISCHIO

### Art. 4: Struttura di Governance dell'IA (Accountability)

Per garantire un approccio organico all'adozione dell'IA, la scuola deve formalizzare una struttura di governance che risponda ai principi di responsabilità (*accountability*) e trasparenza.

### 4.1. Responsabilità Direttiva/Organizzativa

Il Dirigente Scolastico (DS), in qualità di legale rappresentante pro-tempore dell'Istituzione scolastica, è il responsabile dell'innovazione digitale e dell'adozione degli strumenti di IA a livello di singolo istituto. Il DS garantisce l'allocazione delle risorse necessarie per finanziare la formazione specifica (*AI Literacy*) e le infrastrutture tecnologiche, dimostrando l'impegno a gestire l'innovazione nel rispetto dei diritti e delle libertà stabilite dalla normativa.

### 4.2. Istituzione del Gruppo di Lavoro IA

È formalmente istituito un Gruppo di Lavoro per l'Innovazione Digitale e l'IA, composto dal Dirigente, dal DSGA, da Docenti, da Personale ATA e dal Referente IA nominato. Il Gruppo IA opera come motore per la definizione delle strategie di adozione, per la redazione di linee guida e regolamenti, e per la

promozione dell'alfabetizzazione digitale. L'innovazione in segreteria deve superare la visione a "silos" e coinvolgere il personale amministrativo (DSGA e ATA) in una logica di co-progettazione, assicurando che le soluzioni IA rispondano ai bisogni reali e siano integrate efficacemente nei processi gestionali.

### 4.3. Supporto Esterno Specialistico

Si riconosce che l'IA richiede competenze specialistiche in ambito giuridico, tecnologico e organizzativo che spesso non sono disponibili internamente. Il supporto di consulenti esterni specializzati **PUÒ** essere formalmente incaricato per assistere il Gruppo IA e il DPO nelle attività complesse, quali la valutazione dei rischi (DPIA, FRIA) e l'elaborazione di *policy* dettagliate. La presenza di esperti esterni funge da risorsa abilitante, colmando il divario tra la complessità normativa e le risorse interne disponibili, garantendo un'adozione consapevole e conforme.

## Art. 5: L'Etica dell'IA e i Divieti Assoluti (Rischio Inaccettabile)

L'adozione dell'IA deve aderire ai principi etici fondamentali di Trasparenza, Equità, Robustezza, Affidabilità e Sicurezza cibernetica.

### 5.1. Supervisione Umana (Human-in-Command)

Qualsiasi sistema di IA utilizzato per decisioni che abbiano un impatto sugli interessati (studenti, personale) **DEVE** essere soggetto a un livello adeguato di supervisione umana. L'IA è uno strumento di supporto, ma la responsabilità ultima delle decisioni adottate, anche se assistite dall'IA, ricade sempre sulla persona fisica (Docente, DSGA, DS) che ha utilizzato il sistema per crearle o adottarle. Il sistema deve essere progettato per consentire sempre la verifica, la correzione o la sostituzione della decisione da parte del personale umano qualificato.

### 5.2. Divieti Espliciti (AI Act)

L'istituto **NON DEVE** adottare, sviluppare o utilizzare sistemi di IA che rientrino nella categoria di Rischio Inaccettabile (vietato) o che siano gravemente lesivi dei diritti fondamentali. In particolare, è proibito:

1. Sistemi di **Social Scoring** e classificazioni reputazionali automatiche per studenti o personale.
2. Sistemi di **Riconoscimento delle Emozioni** per prendere decisioni amministrative o valutative sugli studenti (es. riconoscimento delle espressioni facciali, segnale vocale, stati fisiologici)
3. Tecniche che impiegano meccanismi di sfruttamento di persone vulnerabili o che utilizzano **Tecniche Manipolative o Subliminali** volte a distorcere il comportamento degli studenti.
4. Sistemi di **Sorveglianza Digitale Pervasiva** che monitorano email, documenti, ricerche online o social media degli studenti 24 ore su 24, anche fuori dall'orario scolastico.

### Art. 6: Gestione del Rischio (Risk-Based Approach) e Valutazioni di Impatto

L'adozione di un approccio basato sul rischio richiede l'identificazione, la valutazione e la mitigazione dei potenziali impatti negativi prima che i sistemi IA vengano implementati.

#### 6.1. Valutazioni d'Impatto (DPIA e FRIA)

Per tutti i sistemi di IA che rientrano nella classificazione di **Alto Rischio** o che comportano un trattamento di dati personali a rischio elevato, la scuola **DEVE** effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA, ai sensi del GDPR) e, se applicabile, una Valutazione d'Impatto sui Diritti Fondamentali (FRIA, ai sensi dell'AI Act), in collaborazione con il Responsabile della Protezione dei Dati (DPO). I risultati di tali valutazioni, che devono essere documentati e conservati, guidano la decisione finale del DS in merito all'adozione.

#### 6.2. Protocollo di Adozione di Strumenti IA

Qualsiasi strumento IA destinato all'uso istituzionale (didattico o amministrativo) **DEVE** seguire un processo di autorizzazione formale:

1. **Fase 1: Richiesta:** Il Docente/Personale interessato segnala l'intenzione di utilizzare un determinato strumento IA per una specifica attività.
2. **Fase 2: Valutazione Preliminare:** Il Gruppo IA valuta la richiesta in merito al rischio, alla finalità, all'efficacia pedagogica/amministrativa e alla disponibilità di *policy* adeguate.
3. **Fase 3: Parere DPO:** Il DPO fornisce un parere vincolante sulla conformità normativa e sulla necessità di eseguire una valutazione di impatto (DPIA e/o FRIA).
4. **Fase 4: Autorizzazione DS e approvazione da parte degli organi collegiali:** Il Dirigente Scolastico, tenuto conto del parere e delle misure di mitigazione, autorizza o non autorizza l'uso istituzionale dello strumento e sottopone al Consiglio di Istituto l’approvazione e regolamentazione dello stesso.

#### 6.3. Registro dei Sistemi IA

L'istituto **DEVE** mantenere un Registro dei Sistemi IA utilizzati, che includa la descrizione delle funzionalità, il livello di rischio classificato, la finalità d'uso, la documentazione tecnica e le misure di mitigazione adottate (es. esecuzione DPIA/FRIA, parere DPO).

## TITOLO III: UTILIZZO NELL'ATTIVITÀ DIDATTICA E FORMATIVA (DOCENTI E ALUNNI)

### Art. 7: Revisione Metodologica e Nuove Forme di Compito (AI-Friendly)

L'introduzione dell'IA esige una revisione delle metodologie didattiche e delle modalità di assegnazione

e valutazione dei compiti, per valorizzare le competenze umane che la macchina non può replicare: autonomia intellettuale, pensiero critico e creatività.

### 7.1. Compiti Obsoleti e Pratiche da Evitare

L'assegnazione di compiti compilativi o nozionistici che possono essere risolti in pochi minuti da strumenti di IA Generativa (es. riassunti letterali, saggi brevi su argomenti generici, traduzioni automatiche non critiche) **NON DEVE** costituire l'oggetto principale della valutazione. L'uso di tali compiti disincentiva lo sforzo personale, portando a superficialità e potenziale plagio.

### 7.2. Compiti AI-Friendly e Sviluppo Critico

I docenti sono incoraggiati a promuovere attività *AI-friendly* che trasformano l'IA in oggetto di studio o strumento di potenziamento:

1. **Analisi Critica dell'Output IA (IA Detective):** Assegnare compiti che richiedano agli studenti di generare un testo o una soluzione con l'IA per poi analizzarne e correggerne attivamente gli errori, le *allucinazioni* o i *bias* trovati, documentando il processo di verifica con almeno tre fonti affidabili. Questo sposta il focus dal *risultato* al *processo*.
2. **Prompt Engineering:** Richiedere la progettazione, il *testing* e il miglioramento di una sequenza di *prompt* per ottenere un risultato specifico dall'IA (es. spiegare un concetto difficile a un pubblico definito).
3. **Metacognizione e Diario di Interazione:** Incoraggiare gli studenti a tenere un "Diario di Interazione" che documenti gli obiettivi di studio, i *prompt* utilizzati e il modo in cui l'output dell'IA è stato utilizzato o modificato. Questa pratica favorisce la riflessione sul proprio stile e ritmo di apprendimento.

L'adozione di queste metodologie innovative (come il *Neural Teaching* e la *Flipped Classroom* con IA) richiede che il docente assuma il ruolo di "Architetto del Sapere" e di facilitatore nell'ambiente di *onlife learning*, progettando Unità di Apprendimento (UdA) che integrino l'IA in modo coerente con i riferimenti pedagogici (Costruttivismo, PBL).

## Art. 8: Uso dell'IA da Parte degli Studenti e Sanzioni

### 8.1. Obbligo di Citazione e Trasparenza (Plagio)

Qualsiasi uso di strumenti IA nella preparazione o nell'elaborazione di compiti e verifiche **DEVE** essere esplicitamente dichiarato. La trasparenza è un requisito fondamentale per l'integrità accademica.

1. **Obbligo di Dichiarazione:** Gli studenti **DEVONO** citare l'uso dell'IA nei loro elaborati, specificando lo strumento (es. ChatGPT 3.5, Gemini Pro), la versione e lo scopo del *prompt* utilizzato (es. "IA usata per la generazione di una bozza iniziale, poi rielaborata manualmente").[1]

2. **Equiparazione del Plagio:** L'uso occulto, non dichiarato e sostitutivo dell'impegno personale di contenuti generati dall'IA è considerato equivalente al plagio tradizionale e comporta sanzioni disciplinari graduate in base alla gravità della violazione.

### 8.2. Verificabilità degli Elaborati

I docenti **POSSONO** utilizzare strumenti di rilevazione di testo generato dall'IA (es. GPTZero) per identificare elaborati sospetti. Tuttavia, tali strumenti devono essere usati solo come **supporto investigativo** e non come prova definitiva, dato il rischio di *falsi positivi* o *falsi negativi*. La valutazione finale di autenticità e la comprensione dei contenuti **DEVONO** essere verificate attraverso un colloquio orale o un confronto con i lavori precedenti dello studente.

### 8.3. Autorizzazione all'Uso per STUDENTI e PERSONALE

L'utilizzo da parte di studenti e del personale di strumenti IA che richiedono un account utente, un'iscrizione o un trattamento di dati personali (anche solo per l'accesso) è consentito solo previa **autorizzazione scritta e annuale da parte del soggetto che ha raggiunto la maggiore età o, se minore, da parte di chi esercita la responsabilità genitoriale nel rispetto di quanto previsto dal Regolamento UE 2016/679 e del Codice in materia di protezione di dati personali di cui al decreto legislativo 30 giugno 2003**, come misura di tutela della privacy.

## Art. 9: Casi d'Uso Didattici a Rischio (Alto/Vietato) e Gestione

### 9.1. Sistemi di Valutazione (Alto Rischio)

I sistemi di IA destinati alla valutazione automatica di componimenti (es. saggio breve) o all'attribuzione di voti **NON POSSONO** operare senza la validazione e l'intervento umano del docente. L'IA può supportare:

1. **Correzione Oggettiva:** Correzione meccanica di quiz a risposta chiusa.
2. **Pre-valutazione:** L'IA può attribuire voti o giudizi preliminari come *proposta* al docente, ma è obbligatorio che il Docente assegni e formalizzi il voto finale, mantenendo il controllo decisionale (*Human-In-Command*).

### 9.2. Analisi Dati per Personalizzazione e Inclusione (Rischio Minimo/Limitato)

L'IA è promossa come strumento per l'inclusione e l'accessibilità (es. sintesi vocale, trascrizione automatica delle lezioni) in linea con l'UDL, classificandosi come rischio minimo.

L'uso di IA per l'analisi di dati aggregati sull'andamento della classe o per la pianificazione delle risorse didattiche **DEVE** garantire la protezione dei dati personali. Se l'analisi riguarda il rendimento o il

comportamento del singolo studente, è obbligatorio procedere alla **pseudonimizzazione** dei dati (sostituendo nome/cognome con un codice identificativo), garantendo così la minimizzazione dei dati personali e l'anonimizzazione delle statistiche.

# TITOLO IV: UTILIZZO NELL'ATTIVITÀ AMMINISTRATIVA E GESTIONALE (PERSONALE ATA E DSGA)

## Art. 10: Governance Amministrativa e Necessità di Co-Progettazione

L'IA deve estendersi all'attività amministrativa per affrontare il sovraccarico burocratico delle segreterie e l'inefficienza operativa.

L'adozione dell'IA in segreteria deve essere gestita attraverso i Gruppi Misti (Art. 4.2), che includano il DSGA e il personale ATA. Questo approccio è indispensabile per la *reingegnerizzazione* dei processi, assicurando che l'innovazione sia supportata e gestita da chi opera quotidianamente i procedimenti amministrativi.

L'IA non è solo uno strumento di efficientamento, ma anche di *explainability* amministrativa: l'uso dell'IA per l'estrazione e l'organizzazione dei metadati documentali può migliorare la trasparenza e la tracciabilità dei processi, trasformando l'IA da potenziale rischio di opacità a garante della chiarezza amministrativa.[1]

## Art. 11: Casi d'Uso Amministrativi (Rischio Nullo vs. Alto Rischio)

L'adozione iniziale dell'IA in ambito amministrativo **DEVE** concentrarsi sui casi d'uso a rischio nullo, per familiarizzare con lo strumento senza trattare dati particolari.

### 11.1. Rischio Nullo (Incentivato)

Si incoraggia l'uso di IA Generativa per attività che non implicano il trattamento di dati personali o informazioni riservate dell'istituto:

1. **Redazione di Documenti Generici:** Supporto alla stesura di bozze di circolari, comunicazioni formali (es. bandi generici, modelli di atti amministrativi standard), migliorando la chiarezza e la correttezza formale.
2. **Ricerca Normativa:** Analisi e sintesi di testi normativi pubblici (es. CAD, AI Act, normative di settore) per supportare l'aggiornamento procedurale del personale.[1]
3. **Materiali Formativi:** Creazione di materiali didattici o *FAQ* generiche sui servizi amministrativi per il personale ATA.

### 11.2. Rischio Alto (Strictly Regulated)

I sistemi che automatizzano o supportano processi critici che incidono sui diritti di terzi o sulla gestione del personale sono classificati ad Alto Rischio. La loro adozione è permessa solo dopo DPIA/FRIA e con

rigorose misure di mitigazione e controllo umano:

1. **Gestione del Personale (Alto Rischio):** L'IA può supportare l'analisi dei *curricula* per la selezione del personale, l'allocazione delle risorse umane o l'elaborazione di graduatorie provvisorie, ma l'assegnazione finale e qualsiasi decisione che incida sul rapporto di lavoro **DEVE** essere validata e formalizzata dal Dirigente Scolastico e dal DSGA.
2. **Classificazione Documentale con Dati Personali:** Strumenti di IA per l'assegnazione automatica di codici di protocollo o la classificazione della corrispondenza in entrata, se trattano dati personali (es. codice fiscale, nome studente), richiedono DPIA e un rigoroso protocollo di **logging** e controllo degli accessi.

# TITOLO V: DATI, PRIVACY E GESTIONE DELLE PIATTAFORME ISTUZIONALI

## Art. 12: Protezione dei Dati Personali (GDPR)

La protezione dei dati personali, in linea con l'Art. 5 del GDPR, è un requisito vincolante.

1. **Minimizzazione e Finalità:** L'uso di sistemi IA **DEVE** rispettare i principi di minimizzazione e limitazione della finalità. I dati personali devono essere raccolti, elaborati e conservati solo per il tempo strettamente necessario al conseguimento degli obiettivi.
2. **Trasparenza, Liceità e correttezza:** In particolare i dati dovranno essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
3. **Divieto di Uso non Autorizzato:** È rigorosamente proibito al personale scolastico e agli studenti utilizzare strumenti di AI esterni non autorizzati (es. versioni gratuite di *chatbot* senza DPA con la scuola) per inserire, trattare o elaborare dati personali riferiti a studenti, colleghi o familiari.

## Art. 13: Misure Tecniche e Organizzative Trasversali

L'istituto implementa misure per garantire la sicurezza cibernetica e la tracciabilità delle operazioni sui sistemi IA.

1. **Account Istituzionali:** L'accesso a qualsiasi piattaforma/ applicazione di IA adottata **DEVE** avvenire esclusivamente tramite account istituzionali (come Google Workspace, M365 ecc….) , ove disponibili, in quanto questi offrono maggiori garanzie di sicurezza, autenticazione e copertura contrattuale (DPA) rispetto agli account personali.
   **E' sempre opportuno valutare la conformità e la legittimità dell'utilizzo degli strumenti di AI in relazione alla tipologia di contratto/account di cui la scuola dispone.**
2. **Sicurezza e Robustezza:** I sistemi IA utilizzati devono essere dotati di meccanismi di registrazione

(*logging*) automatici per tracciare e conservare le operazioni svolte e devono essere protetti contro tentativi di alterazione, compromissione o uso illecito (*cybersecurity*).

### Art. 14: Specificità per Google Workspace for Education (GWE)

L'Istituzione Scolastica, nell'uso degli strumenti di AI integrati in Google Workspace for Education (GWE) (es. Gemini), si attiene alle garanzie fornite dal fornitore.

1. **Protezione dei dati e Garanzia di Non Addestramento:** Si prende atto che GwE opera come Responsabile del Trattamento (Data Processor) e dell'impegno di Google di non utilizzare i contenuti inseriti nei Core Services (documenti, email) per addestrare i propri modelli GenAI di base o per il *targeting* pubblicitario, in particolare per gli utenti K-12 (scuola primaria e secondaria).
2. **Compliance:** Si riconosce che i Core Services di GWE supportano la conformità con GDPR. Il personale **DEVE** essere consapevole che tali garanzie contrattuali mitigano significativamente il rischio di violazione della finalità.

### Art. 15: Specificità per Microsoft 365 Education/Copilot

L'Istituzione Scolastica, nell'uso di Microsoft 365 Copilot e Microsoft 365 Copilot Chat, si attiene ai termini del *Microsoft Products and Services Data Protection Addendum* (DPA).

1. **Protezione Dati:** Si prende atto che Microsoft opera come Responsabile del Trattamento (Data Processor) e che *prompts*, risposte e dati acceduti tramite *Microsoft Graph* **non sono utilizzati** per addestrare i modelli GenAI di base.
2. **Limiti di Copertura:** Il personale **DEVE** essere istruito sulla cautela nell'uso delle query web di Copilot, poiché, in genere, queste ricerche esterne non sono coperte dal DPA e **NON DEVONO** essere utilizzate per il trattamento di dati personali.
3. **Sicurezza e Copyright:** Le garanzie di Microsoft contro il *prompt injection* e il *Customer Copyright Commitment* sono considerate misure tecniche e contrattuali aggiuntive di mitigazione del rischio.

La comparazione delle politiche dati dei fornitori principali è riassunta di seguito:

Table: Implicazioni Privacy e Compliance Piattaforme (Google vs. Microsoft)

| **Caratteristica Critica** | **Google Workspace for Education** | **Microsoft 365 Copilot** |
|---|---|---|
| **Ruolo GDPR** | Responsabile (Processor). | Responsabile (Processor).[4] |
| **Addestramento Modelli** | No per Core Services (K- | No per |

| | | |
|---|---|---|
| **(Dati Utente)** | 12).[3] | Prompt/Risposte/Graph data. |
| **Uso per Pubblicità (K-12)** | Escluso. | Escluso (Coperto da DPA). |
| **Ambito di Copertura DPA** | Servizi Core. | M365 Education. |

# TITOLO VI: FORMAZIONE, AGGIORNAMENTO CONTINUO E ADATTAMENTO

## Art. 16: L'Obbligo di AI Literacy e Sviluppo Professionale

La formazione è l'elemento chiave per garantire un uso consapevole, etico e non superficiale dell'IA.

1. **AI Literacy come Obbligo:** L'*AI Literacy* è considerata un requisito obbligatorio (imposto anche dall'Art. 4 dell'AI Act). Il personale (Docente e ATA) **DEVE** completare i percorsi formativi sull'IA prima di essere autorizzato all'uso istituzionale di tali strumenti.
2. **Contenuti Formativi:** I percorsi (che possono avvalersi di enti accreditati o poli formativi specializzati, c) devono essere allineati ai framework DigComp e includere moduli specifici su:
   - Etica dell'IA (gestione di *bias*, non discriminazione).
   - Competenze Tecniche (es. *Prompt Engineering* per ottimizzare l'interazione con l'IA).
   - Sicurezza e Privacy (gestione sicura dei dati cloud, *phishing*).
   - Metodologie Didattiche (integrazione dell'IA nel curricolo, supporto BES/UDL).

La scuola deve promuovere una cultura di apprendimento continuo (*Long Life Learning*), sperimentando costantemente nuovi strumenti e approcci per adattarsi all'incessante evoluzione tecnologica.

## Art. 17: Monitoraggio, Revisione e Miglioramento Continuo

Il presente Regolamento e le *policy* operative interne sono considerati in uno stato di "perpetual beta," soggetti a revisione e aggiornamento continuo.

1. **Revisione Annuale:** Il Gruppo IA **DEVE** condurre una revisione annuale del Regolamento e delle *policy* adottate, tenendo conto dell'evoluzione normativa, delle esperienze interne (casi d'uso e criticità emerse) e dei risultati delle Valutazioni d'Impatto (DPIA/FRIA).
2. **Valutazione della Maturità:** La scuola **DOVREBBE** periodicamente valutare il proprio livello di maturità nell'adozione dell'IA in cinque dimensioni chiave (Dati, Metodologie, Organizzazione, Cultura, Relazione con Utenza) per definire obiettivi realistici (*TO BE*) e mirati per l'anno scolastico successivo.

## TITOLO VII: DISPOSIZIONI FINALI

### Art. 18: Sanzioni e Misure Correttive

L'inosservanza delle disposizioni contenute nel presente Regolamento, in particolare quelle relative all'uso non autorizzato dell'IA, alla mancata citazione dell'output o alla violazione dei divieti in materia di dati personali, è considerata una violazione grave.

1. **Sanzioni Disciplinari:** Le sanzioni per gli studenti saranno graduate in base alla gravità della violazione e in conformità con il Regolamento d'Istituto e lo Statuto delle Studentesse e degli Studenti. Per il personale scolastico, le violazioni comporteranno l'applicazione di misure disciplinari in linea con il Codice di Comportamento.
2. **Gestione degli Incidenti (Data Breach):** In caso di violazione della protezione dei dati personali (es. immissione accidentale di dati particolari in un sistema IA non autorizzato), il personale coinvolto ha l'obbligo di segnalare immediatamente l'incidente al DPO per l'attivazione immediata delle procedure di mitigazione e l'eventuale notifica al Garante, ai sensi del GDPR.

### Art. 19: Entrata in Vigore

Il presente Regolamento entra in vigore a partire dalla data di approvazione da parte del Consiglio d'Istituto.

## CONCLUSIONI E RACCOMANDAZIONI OPERATIVE

L'adozione dell'Intelligenza Artificiale in una scuola secondaria non è un'opzione, ma un'esigenza dettata dall'evoluzione della società e della normativa. Il successo di questo processo dipende dalla capacità della scuola di trasformare l'IA da un mero strumento tecnologico a un elemento integrato della cultura organizzativa ed educativa.

Il presente Regolamento fornisce il quadro normativo e procedurale per gestire tale transizione in modo conforme e consapevole. Le principali raccomandazioni operative che derivano dall'analisi del quadro documentale sono:

1. **Priorità alla Governance e all'AI Literacy:** La prima azione concreta deve essere l'istituzione formale e il rafforzamento del Gruppo di Lavoro IA e l'avvio immediato di percorsi di *AI Literacy* per tutto il personale, in quanto l'alfabetizzazione è un prerequisito normativo (AI Act) e pedagogico per un uso responsabile.
2. **Approccio Cautelativo (Zero Data Personali):** Nella fase iniziale, si raccomanda l'implementazione di una *policy* conservativa che proibisca l'uso dell'IA per il trattamento di dati personali. La sperimentazione deve concentrarsi sui **casi d'uso a rischio nullo** (es. supporto alla scrittura generica

o ricerca normativa su testi pubblici) o l'analisi di dati didattici precedentemente **pseudonimizzati**.

3. **Integrazione Metodologica:** Il corpo docente deve spostare il focus didattico dal *risultato* al *processo*, incoraggiando compiti *AI-friendly* che richiedano la verifica critica dell'output dell'IA (Fact-Checking e IA Detective) e l'acquisizione di competenze di *Prompt Engineering*.
4. **Conformità e Trasparenza per Fornitori:** Indipendentemente dalla piattaforma utilizzata (Google o Microsoft), che si configurano come Responsabili del Trattamento (Processor), la scuola deve mantenere la piena *Accountability* (Titolare del Trattamento). L'uso di sistemi ad alto rischio (es. per l'allocazione delle risorse o la diagnosi degli apprendimenti) è condizionato all'esecuzione di una DPIA/FRIA documentata e alla garanzia di un controllo umano effettivo (*Human-In-Command*).

La sfida finale è utilizzare l'IA per coltivare negli studenti il senso critico, la responsabilità e l'autonomia intellettuale, trasformando la scuola in un ambiente capace di governare e gestire consapevolmente la complessità tecnologica.

## Bibliografia


1. Generative AI, Privacy, and Google Cloud, https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf
2. Enterprise data protection in Microsoft 365 Copilot and Microsoft 365 Copilot Chat, https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection