ISTITUTO COMPRENSIVO STATALE CERISANO
a Indirizzo Musicale

UNIONE EUROPEA
Fondo sociale europeo
Fondo europeo di sviluppo regionale

Ministero dell'Istruzione

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) PER L'UTILIZZO DI SERVIZI IA (INTELLIGENZA ARTIFICIALE) DELLA PIATTAFORMA MICROSOFT 365

Trattamento: utilizzo di servizi di Intelligenza Artificiale (IA) in ambiente Microsoft 365 - Copilot.
Titolare del trattamento: Istituzione scolastica statale (di seguito, "Scuola").
Interessati: personale scolastico; alunni; famiglie.
Responsabile della Valutazione: Dirigente Scolastico Lorenzo CIACCO
DPO: dott.ssa Anna CIMA.
Versione documento: 1.0
Data: 28/01/2026
Revisione prevista: al verificarsi di modifiche sostanziali del trattamento o delle condizioni di servizio

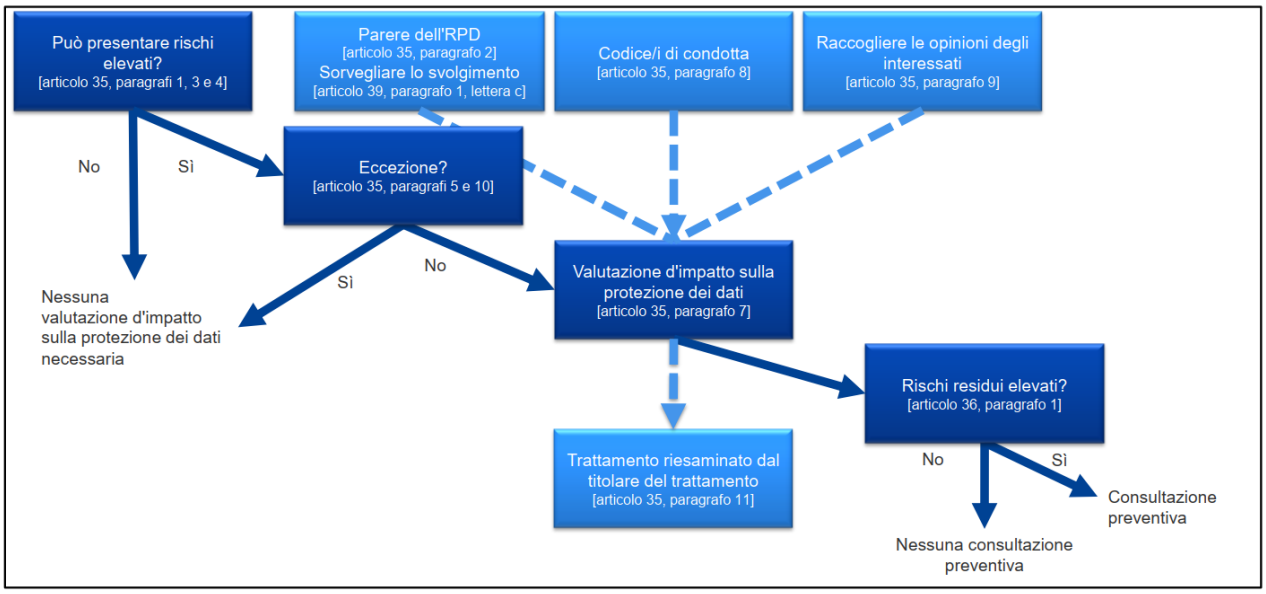
DPIA realizzata in parte sulla base del modello messo a disposizione dalla CNIL (Autorità francese per la protezione dei dati) e tradotta in italiano con la collaborazione del Garante per la protezione dei dati. La Valutazione è stata redatta con il supporto del DPO di questo Istituto.

1. Oggetto della DPIA

Servizi IA della piattaforma cloud Microsoft 365 (M365).

2. Introduzione e motivi della DPIA

La DPIA (Data Protection Impact Assessment), è una valutazione preliminare eseguita dal titolare del trattamento dei dati personali, relativa agli impatti e ai rischi determinati da un determinato trattamenti dati.
Secondo il GDPR, non è necessario/obbligatorio svolgere una valutazione d'impatto per ciascun trattamento, ma solo per quelli che "possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35 Regolamento UE 2016/679).



I criteri da prendere in considerazione per l'obbligo della DPIA (secondo il Gruppo art.29 "Comitato Europeo della protezione dei dati") sono i seguenti:

- Profilazione
- Decisioni automatizzate che producono significativi effetti giuridici
- Monitoraggio sistematico
- Trattamenti di dati sensibili, giudiziari o di natura estremamente personale
- Trattamenti di dati personali su larga scala
- Dati relativi a soggetti vulnerabili
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative
- Trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto

In presenza di almeno due di questi criteri, la DPIA è necessaria.

La presente DPIA ha lo scopo di:

- analizzare in modo sistematico i trattamenti di dati personali connessi all'utilizzo del servizio di Intelligenza Artificiale **Copilot**
- valutare la **necessità e proporzionalità** dei trattamenti rispetto alle finalità educative e istituzionali
- individuare i **rischi per i diritti e le libertà degli interessati**, con particolare riferimento agli **alunni minorenni**
- definire e valutare l'efficacia delle **misure tecniche e organizzative** adottate o da adottare
- determinare il **livello di rischio residuo** e la sua accettabilità

2.1 Processo di valutazione

Il processo che porta alla valutazione del rischio prevede alcune fasi, così riassunte:

Fase 1: identificazione dei trattamenti

Consiste nell'individuare tutti gli elementi del trattamento dati:

- Tipologia di dati
- Finalità
- Categorie di interessati

- Modalità di trattamento
- Misure tecniche/organizzative
- Destinatari
- Eventuale trasferimento extra UE

Fase 2: Panoramica dei rischi

Vengono individuati i potenziali rischi, cioè la probabilità con cui un evento dannoso possa verificarsi, e le relative conseguenze, determinando una scala di probabilità del rischio che va da "improbabile" a "quasi certo" e una scala di incidenza delle conseguenze che va da "trascurabili" a "gravissime".

Fase 3: Valutazione del rischio ed eventuali misure correttive

Si valutano rischi e conseguenze, determinando l'esito della DPIA.

3. DESCRIZIONE DEL CONTESTO ORGANIZZATIVO E TECNOLOGICO

3.1 Il Titolare del trattamento

Il Titolare del trattamento è l'Istituzione scolastica statale, che opera nell'ambito delle funzioni istituzionali attribuite dal sistema normativo nazionale in materia di istruzione e formazione.

La scuola utilizza la piattaforma Microsoft 365, già attiva e configurata con account istituzionali individuali assegnati a:

- personale docente
- personale ATA
- studenti, inclusi minorenni

3.2 I servizi di Intelligenza Artificiale oggetto della DPIA

Il trattamento riguarda l'utilizzo delle nuove tecnologie IA (Intelligenza Artificiale), per l'attuazione di un' ampliata e rinnovata offerta formativa che prevede l'utilizzo di strumenti digitali e forme nuove di apprendimento, l'organizzazione della didattica, le funzioni amministrative connesse, le attività di coordinamento/organizzazione/svolgimento delle varie attività didattiche e amministrative.

L'utilizzo dei servizi IA può avvenire, da parte del personale e degli alunni, sia a scuola durante le ore di attività, sia in ambito domestico (se previsto), con strumenti messi a disposizione dal titolare del trattamento (pc, tablet) o tramite strumenti propri dell'interessato (pc, tablet, smartphone).

L'interessato può utilizzare la connessione internet della scuola (se messa a disposizione) oppure il proprio piano dati internet utilizzato sul proprio dispositivo.

I servizi oggetto della presente valutazione sono:

- **Copilot**, assistente di Intelligenza Artificiale generativa integrato nella piattaforma M365

Tale servizio opera esclusivamente **all'interno del dominio Microsoft dell'istituzione scolastica**, secondo le configurazioni amministrative definite dal Titolare.

3.3 Gli interessati

Parere degli interessati: non è stato chiesto il parere agli interessati. Il Titolare del trattamento, nel rispetto del principio di accountability, definisce gli strumenti del trattamento dati funzionali al perseguimento di finalità istituzionali connesse all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Gli interessati sono adeguatamente informati su tutti gli aspetti del trattamento e possono, oltre ad esercitare i propri diritti, partecipare al miglioramento e adeguamento del trattamento qualora dovessero riscontrare criticità o volessero suggerire miglioramenti.

Categorie di interessati: personale scolastico, alunni, familiari/tutori alunni.

3.4 Ruoli e soggetti del trattamento

I soggetti coinvolti nel trattamento dati sono diversi, con funzioni complementari e con il compito di cooperare per una corretta gestione della piattaforma e del relativo trattamento dati. Vediamo quali sono le principali figura individuabili:

- **Il Titolare del trattamento**, *è la persona fisica o giuridica, l'autorità pubblica […] che determina le finalità e i mezzi del trattamento di dati personali* (art. 4 GDPR). In questo caso è l'Amministrazione scolastica legalmente rappresentata dal Dirigente scolastico, che determina quali dati trattare, per quali finalità, con quali strumenti, con quali modalità.
- **I docenti,** svolgono il ruolo di Incaricati al trattamento e agiscono sotto l'autorità del titolare del trattamento. Progettano la didattica con l'utilizzo dell'IA, può essere utilizzata per generare rapidamente alternative e spunti: esempi, esercizi, domande, consegne, mappe, attività di recupero e potenziamento. Producono contenuti che condividono con gli alunni della classe e gruppi di lavoro, su cui devono avere supervisione per assicurarsi che tutti gli alunni agiscano nel rispetto delle regole e delle prescrizioni di utilizzo fornite.
- **L'amministratore della piattaforma (admin),** è il soggetto che accede alla consolle e ha i privilegi necessari per gestire i servizi e gli utenti.
- **Il Responsabile del trattamento,** è il soggetto che tratta in modo stabile e continuativo i dati per conto del titolare, per effetto di un contratto o atto giuridico che vincoli il responsabile al titolare. Deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. In questo caso, il Responsabile del trattamento è Microsoft.
- **L'amministratore di sistema,** è nominato dal DS ed ha il compito di verificare la sicurezza informatica delle risorse hardware, provvedendo ad attivare le misure necessarie quali antivirus, anti malware, firewall, impostazioni di accesso fisico.
- **Il DPO,** è coinvolto per consulenza in materia di trattamento dati.

3.5 Dati trattati

L'uso di strumenti di IA in ambito scolastico è impostato per minimizzare i dati personali. In linea generale, la scuola promuove attività che non richiedono l'inserimento di dati identificativi degli studenti. Tuttavia, a seconda delle modalità di accesso e dello strumento utilizzato, potrebbero essere trattati:

- dati identificativi e di contatto legati all'account istituzionale (es. nome, cognome, username, classe, email istituzionale);
- dati tecnici e di utilizzo (es. log di accesso, indirizzo IP o identificativi del dispositivo, eventi di sicurezza, impostazioni e metadati);
- dati relativi alla didattica solo in forma non eccedente e, di regola, non riconducibile a situazioni personali o sensibili.

È espressamente previsto, come regola di comportamento per studenti e docenti, il divieto di inserire nei tool di IA: nomi e dati di altri studenti o docenti, riferimenti che rendano identificabile una persona, immagini di compagni e docenti, valutazioni individuali, documenti scolastici riservati, PEI/PDP, dati sulla salute o situazioni familiari.

I dati trattati sono quindi minimizzati a quelli strettamente necessari, ma l'utilizzo di un account personale nella forma nome.cognome@sitoscuola.edu.it determina il trattamento in chiaro del nome utente, per poter essere correttamente ed univocamente identificato all'interno della piattaforma.

4. Principi fondamentali

4.1 Proporzionalità e necessità

Gli scopi del trattamento sono quelli di perseguire le finalità istituzionali del titolare del trattamento, come:

- attuare il Piano Triennale dell'Offerta Formativa, che prevede nuove metodologie di apprendimento
- attuare le misure previste dalla Linee guida MIM sulla IA Versione 1.0/2025
- adeguarsi al CAD, che prevede la transizione digitale delle PA per efficientare i servizi
- favorire il passaggio al cloud, che è uno dei principali obiettivi del Piano Nazionale Scuola Digitale nell'ambito delle misure del PNRR, di cui la scuola è beneficiaria.

L'obiettivo è dunque quello di formare gli alunni ad un consapevole e funzionale uso delle tecnologie digitali, per poter guidare i più piccoli e preparare i più grandi verso un percorso di studi universitari e/o un mondo del lavoro che richiede competenze e capacita digitali. Del trattamento sono esplicitamente informati gli interessati con specifica informativa, che definisce tutti gli aspetti del trattamento e la legittimità dello stesso da parte del titolare, il quale agisce per il perseguimento di finalità istituzionali connesse all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Nell'ambito di tali finalità, il titolare definisce quali dati trattare e con quali strumenti, e questa DPIA è volta a valutare proprio il rischio di tale scelta.

4.2 Basi giuridiche che rendono lecito il trattamento

L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Nello specifico, la scuola organizza la propria attività per lo svolgimento, primariamente, degli obiettivi prefissati nel PTOF (Piano Triennale dell'Offerta Formativa), che rappresenta il documento identificativo della scuola e contiene un'indicazione chiara e dettagliata di obiettivi, linea d'azione e mezzi a disposizione per raggiungerli. Agisce poi in conformità del CAD (Codice dell'Amministrazione Digitale), il quale prevede e promuove l'uso delle nuove tecnologie nella PA per le attività amministrative e organizzative, e delle Linee guida MIM per l'IA.

4.3 Caratteristiche dei dati trattati

I dati personali trattati tramite l'utilizzo della piattaforma cloud e dei servizi IA sono nominativo (presente nell'account di accesso), altri come log di accesso, indirizzo IP o identificativi del dispositivo, eventi di sicurezza, impostazioni e metadati. I dati trattati, seppur limitati più possibile rispetto alle finalità, consentono di identificare l'utente in considerazione del nominativo inserito nell'account individuale, assegnato ad ogni interessato per poter identificare in maniere univoca l'utente all'interno della piattaforma. Non vengono gestiti dati sensibili né documenti che possano ricondurre a tale categoria di dati.
I dati vengono verificati e aggiornati periodicamente, eliminando gli utenti non più operativi, archiviando/cancellando i file non più pertinenti. Eventuali segnalazioni di rettifica da parte degli interessati vengono prese in carico dall'amministratore della piattaforma, dopo averne verificato l'attendibilità e applicabilità.
La conservazione dei dati è effettuata per il periodo necessario al perseguimento delle finalità. Successivamente, per i documenti rilevanti ai fini didattici/amministrativi, si procede all'archiviazione dai dati per il tempo previsto dalla normativa di riferimento. Per i documenti che costituiscono prove di valutazione, ad esempio, l'archiviazione ha la durata di almeno un anno e comunque deve rispettare i tempi previsti dalla circolare n.44 del 2005 della Direzione Generale degli Archivi. Altri tipi di prove e documenti, possono essere archiviati fino alla fine dell'anno scolastico o del percorso in cui si inserisce il documento.

5. Misure a tutela dei diritti degli interessati

5.1 Informativa e diritti

Gli interessati sono informati del trattamento dati con specifica e dettagliata informativa (art. 13 GDPR), contenente i dettagli e le caratteristiche del trattamento. L'Informativa è pubblicata sul sito web del titolare del trattamento e notificata a tutti gli interessati tramite il canale di comunicazioni del Registro elettronico.
Gli interessati possono esercitare i propri diritti contattando gli uffici del titolare del trattamento, chiedendo informazioni sui propri dati o l'esercizio di un diritto di cui dagli artt. 15 a 23 del GDPR, nella misura in cui applicabili alla tipologia di trattamento.

5.2 Obblighi dei Responsabili del trattamento

Microsoft 365 svolge il ruolo di Responsabile del trattamento dei dati personali dei clienti che vengono trasmessi, archiviati, inviati o ricevuti dal titolare attraverso i servizi della piattaforma e tratta tali dati per suo conto e dietro sue istruzioni. I trattamenti operati da Microsoft sono inoltre regolamentati tramite l'Addendum con etichetta "Condizioni del Regolamento Generale dell'Unione Europea sulla Protezione dei Dati, dove sono specificati gli obblighi in carico al Responsabile del trattamento. Il Contratto prevede che il Cliente è il titolare del trattamento e Microsoft è il Responsabile del trattamento. Ai sensi del Contratto, il Cliente sarà tenuto ad adempiere ai propri obblighi di Titolare del trattamento e Microsoft sarà tenuto ad adempiere ai propri obblighi di Responsabile del trattamento. Tuttavia, è opportuno sottolineare che questo Titolare del trattamento (la scuola), nella definizione di clausole contrattuali ha bassissimo se non nullo potere contrattuale, per cui è impossibile per lo stesso ottenere garanzie rafforzate e più tutelanti. Il fornitore Microsoft è inserito, inoltre, nell'elenco SaaS (Software as a Service) della Agenzia per la Cybersicurezza Nazionale (ex Agid), e in base a ciò è stata fatta una valutazione in merito ai requisiti di sicurezza e affidabilità informatica della piattaforma, oltre ad essere certificato ai sensi del Dpf (Data privacy framework).

5.3 Trasferimento dati al di fuori dell'Unione Europea

La Commissione Europea, in virtù dei negoziati tra UE e USA che hanno portato all'adozione dell'accordo UE-USA Data Privacy Framework, è giunta alla conclusione che gli Stati Uniti garantiscono un livello di protezione adeguato comparabile a quello dell'Unione europea, con protezioni e garanzie sufficienti sul trattamento dei dati personali. Sulla base della nuova decisione di adeguatezza, i dati personali possono circolare in modo sicuro dall'UE verso le imprese statunitensi che partecipano al quadro, senza la necessità di ulteriori garanzie per la protezione dei dati.

6. Rischi

Come abbiamo visto all'inizio di questa DPIA, alla Fase 1 "Identificazione dei trattamenti", seguono la Fase 2 "Panoramica dei rischi" e la Fase 3 "Valutazione del rischio ed eventuali misure correttive".
Il livello del rischio può essere misurato numericamente utilizzando due valori:

1) Probabilità di accadimento (P)
2) Conseguenze (C)

Il Livello di Rischio (LR) è dato dunque dalla relazione: LR=PxC
Alla probabilità P e alle conseguenze C sono associati valori numerico in relazione alla loro incidenza:

P	Probabilità di accadimento	C	Conseguenze
1	Improbabile	1	Trascurabili
2	Poco probabile	2	Limitate
3	Probabile	3	Gravi
4	Certo	4	Gravissime

Il livello di rischio LR, dunque, potrà variare da un valore minimo 1 a un valore massimo 16, così valutabile:

Entità del rischio	**Valori di riferimento**
Poco rilevante	1≥ LR ≤3
Basso	4≥ LR ≤7
Alto	8≥ LR ≤12
Altissimo	13≥ LR ≤16

Così è possibile ricavare, per ogni attività di trattamento, il Livello di Rischio di potenziale accesso illegittimo, modifica, perdita, distruzione di dati non autorizzata.
I livelli P e C vengono chiaramente stimati e assegnati ai rischi dal titolare in relazione ad una valutazione generale dei propri trattamenti, alla luce di tutti i parametri specificati nel corso di questa DPIA.

6.1 Misure esistenti o pianificate

Controllo degli accessi

Gli accessi logici degli utenti avvengono attraverso l'account individuale assegnato ad ognuno ed autorizzato, con eventuali limitazioni in base alla tipologia di utente (docente, alunno). Gli account di utenti non più interessati del titolare (es. docenti non più in servizio o alunni che si trasferiscono) vengono disattivati.

Minimizzare la quantità di dati personali

I dati personali vengono minimizzati più possibile, compatibilmente con il perseguimento delle finalità e il raggiungimento degli obiettivi. Tuttavia, consentono di identificare l'utente in considerazione del nominativo inserito nell'account individuale, assegnato ad ogni interessato per poter identificare in maniere univoca l'utente all'interno della piattaforma. Vengono inoltre acquisite dalla piattaforma una serie di altre informazioni, come ID del dispositivo, browser, sistema operativo, lingua selezionata, in parte classificabili come dati personali. Non vengono gestiti dati sensibili né documenti che possano ricondurre a tale categoria di dati.

Anonimizzazione dei dati

L'account contiene in chiaro il nome dell'utente, per poter identificare in maniera univoca il soggetto all'interno della piattaforma. La gestione di account anonimi non sarebbe attuabile, perché non consentirebbe di effettuare sulla piattaforma il controllo degli accessi logici compromettendo la sicurezza della stessa. Vengono anonimizzati/pesudonimizzati i dati eventualmente contenuti in documenti condivisi, la cui natura non consente di indicare le informazioni in chiaro (circostanza rara e non prevista per il trattamento dati tramite la piattaforma e i servizi IA). Il fornitore/responsabile cripta inoltre i dati per impostazione predefinita.

Misure di sicurezza informatica

I sistemi di sicurezza dei dispositivi in uso presso e della scuola vengono periodicamente verificati e aggiornati e sono dotati di antivirus, anti malware e firewall. I pc amministrativi sono dotati di credenziali per l'accesso, mentre quelli dei laboratori ne sono sprovvisti per motivi ovvi (utilizzo trasversale da parte di tutti gli alunni), i quali tuttavia non contengono alcun tipo di documenti e informazioni, ma vengono solo utilizzati per attività didattiche ed esercitazioni. Le misure di sicurezza proprie della piattaforma sono attuate direttamente dal fornitore/responsabile del servizio (Microsoft).

Istruzioni agli operatori

Gli operatori sono stati istruiti sul corretto uso dei sistemi, attraverso attività informative, specifici regolamenti e linee guide rivolte a personale e alunni. Sono state fornite informazioni e indicazioni sia da un punto di tecnico, per il corretto uso dello strumento e delle funzioni messe a disposizione, sia da un punto di vista del trattamento dati, per un adeguato uso dei dati e dei documenti da poter condividere tramite la piattaforma e una corretta valutazione dei dati da escludere da questo tipo di trattamento. Le istruzioni e linee guida.

6.2 Valutazione del rischio

L'analisi del rischio connessa all'impiego degli strumenti di Intelligenza Artificiale considerati si concentra sul rischio residuo, ossia su quei profili di pericolo che possono manifestarsi anche qualora l'uso delle applicazioni avvenga in assenza di un trattamento intenzionale di dati personali.
Il presupposto di base è che i servizi siano configurati e utilizzati in modalità senza dati, ma che permanga un margine fisiologico di rischio riconducibile prevalentemente al fattore umano, soprattutto in ambito scolastico.

Analisi dei rischi

>Inserimento non autorizzato o alterazione involontaria di dati personali

Origine del rischio

Il principale profilo di rischio individuato non deriva dal funzionamento intrinseco degli strumenti di IA, ma dalla condotta dell'utente finale.
In particolare, il rischio consiste nella possibilità che docenti o studenti, in modo non intenzionale o per errata valutazione, inseriscano nei prompt o nei materiali caricati dati personali, in contrasto con le istruzioni e i divieti impartiti dall'istituzione scolastica.
Tale evenienza è riconducibile esclusivamente ad errore umano, non a una carenza strutturale delle misure di sicurezza tecnologiche.

Misure di prevenzione e mitigazione

Per contenere tale rischio, l'istituzione scolastica ha predisposto un sistema integrato di misure organizzative e procedurali, fondato sui seguenti elementi:

- Il personale docente e amministrativo è destinatario di attività informative specifiche, con particolare riferimento alla minimizzazione, alla selezione consapevole delle informazioni e all'uso corretto degli strumenti di IA in ambito didattico.
- L'istituto ha previsto un Regolamento IA e delle Linee guida che vietano espressamente l'utilizzo di tool di IA per la redazione, l'analisi o il caricamento di documenti contenenti dati personali.
- Nei casi eccezionali in cui si renda necessario fare riferimento a situazioni riconducibili a persone fisiche, è previsto l'uso sistematico di tecniche di pseudonimizzazione o anonimizzazione, in modo da impedire l'identificazione diretta o indiretta degli interessati.

Valutazione del livello di rischio

- **Probabilità**
  L'eventuale inserimento di dati personali, in particolare se riferiti a minori o a categorie particolari di dati, è valutato come *Poco probabile (Livello P2)***,** in quanto sono state date chiare indicazioni sul divieto di inserimento di dati personali tramite la documentazione adottata, le informative, le linee guida
- **Conseguenze**
  Il *Poco probabile* inserimento di dati personali, in particolare se riferiti a minori o a categorie particolari di dati, è valutato come evento con *Conseguenze Gravi* (Livello C3), in quanto potenzialmente idoneo a incidere sui diritti e sulle libertà fondamentali degli interessati.

- **Livello di rischio**
  Il livello di rischio LR risulta pari a 2 × 3 = 6, su una scala massima di 16, e può pertanto considerarsi contenuto e sotto controllo.

>Perdita dei contenuti generati o analizzati dall'Intelligenza Artificiale

Origine del rischio

Un ulteriore profilo di rischio riguarda la perdita dei contenuti prodotti o elaborati tramite gli strumenti di IA**,** quali sintesi, bozze di testi o materiali di supporto alla didattica.
Tali contenuti non costituiscono documentazione amministrativa ufficiale né atti soggetti a obblighi di conservazione a lungo termine e, pertanto, non beneficiano delle medesime garanzie previste per i documenti istituzionali**.**

Misure di prevenzione e mitigazione

Le Linee guida di Istituto sulla IA stabiliscono che:

- i docenti sono tenuti a verificare criticamente i contenuti prodotti dall'IA;
- nessun contenuto generato dall'IA è considerato valido o utilizzabile senza una preventiva revisione umana;
- nessuna dato personale deve essere inserito nei prompt e nei documenti allegati ai tool di IA.

Valutazione del livello di rischio

- **Probabilità**
  Considerate le modalità operative per l'uso di tool di IA, la probabilità è stimata come *Improbabile (Livello P1)***.**
- **Conseguenze**
  L'eventuale perdita di un prompt, di una bozza o di un elaborato preliminare è valutata come evento con *Conseguenze trascurabili* (Livello C1), in quanto non compromette la continuità dell'azione amministrativa né la missione istituzionale della scuola.
- **Livello di rischio**
  Il livello di rischio LR risulta pari a 1 × 1 = 1, su una scala massima di 16, e può pertanto considerarsi Poco rilevante.

>Accesso illegittimo ai dati

Origine del rischio

Il rischio di un accesso illegittimo ai dati può avvenire per cause dolose o colpose/accidentali, come cessione a terzi non autorizzati delle proprie credenziali di accesso, errata attribuzione dei permessi sulla piattaforma, azione dolosa di hackeraggio sulla piattaforma da parte di terzi.

Misure di prevenzione e mitigazione

Le misure tecniche e organizzative utili a mitigare il rischio di un accesso illegittimo sono quelle descritte nel corso di questa DPIA, e cioè (elenco in continuo aggiornamento):

- Impostazioni tecniche sulla piattaforma
- Formazione tecnica agli utenti
- Definizione delle policy
- Verifica periodi degli utenti attivi e di quelli da disattivare
- Minimizzazione dei dati
- Anonimizzazione e pseudonimizzazione se e quando necessario
- Periodici appelli per una corretta gestione delle credenziali di accesso

Valutazione del livello di rischio

- **Probabilità**

Sulla base delle misure adottate, delle indicazioni agli utenti sulla corretta gestione della piattaforma, la probabilità è stimata come *Poco Probabile (Livello P2)***.**

- **Conseguenze**
  In base alla natura dei dati trattati (considerando che non è previsto il trattamento di dati sensibili), le conseguenze sono valutate come *Limitate* (C=2).
- **Livello di rischio**
  Il livello di rischio LR risulta pari a 2 × 2 = 4, su una scala massima di 16, e può pertanto considerarsi Basso.

Sintesi della valutazione dei rischi

Livello di Rischio (LR)

Rischio	Probabilità (P)	Conseguenze (C)	Livello di Rischio (LR)	Entità rischio
Inserimento dati personali	2	3	6	Basso
Perdita di contenuti	1	1	1	Poco rilevante
Accesso illegittimo	2	2	4	Basso

7. Valutazione complessiva e condizioni di ammissibilità

L'analisi svolta evidenzia che i rischi associati all'utilizzo di Copilto Microsoft 365 in configurazione priva di dati personali, si collocano stabilmente al di sotto della soglia di rischio accettabile.
L'adozione dello strumento è pertanto ritenuta compatibile con le finalità didattiche dell'istituzione scolastica, a condizione che vengano mantenuti e rafforzati tutti i presìdi organizzativi previsti.

ISTITUTO COMPRENSIVO STATALE CERISANO • 87044 CERISANO (CS) •

Il Dirigente scolastico
Ing. Lorenzo Ciacco
Firma autografa sostituita a mezzo stampa
ex art.3, c. 2 D.l.gs. n. 39/93