

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

DPIA e TIA per l'adozione della piattaforma Microsoft 365 nello svolgimento delle attività didattiche ed amministrative

IST. MAGISTRALE ST. - "C. LORENZINI"-PESCIA
Prot. 0001507 del 20/02/2026
I-1 (Uscita)

Premessa

La DPIA (Data Protection Impact Assessment) e la TIA (Transfer Impact Assessment) sono valutazioni da effettuare per valutare e gestire i rischi del trattamento dati e il loro trasferimento extra-UE, ai sensi del GDPR.

La DPIA analizza i rischi per i diritti degli interessati e la TIA valuta la sicurezza dei dati trasferiti in Paesi terzi. Quest'ultima risulta di particolare importanza a seguito della sentenza Schrems II del 16 luglio 2020 emessa dalla Corte di Giustizia dell'Unione Europea, che ha invalidato il Privacy Shield UE-USA, stabilendo che le leggi USA sulla sorveglianza non garantiscono una protezione adeguata e imponendo garanzie aggiuntive e una valutazione rigorosa per il trasferimento di dati extra-UE.

DPIA (Data Protection Impact Assessment - Valutazione d'Impatto sulla Protezione dei Dati)

- Finalità: Identificare e mitigare i rischi elevati per i diritti e le libertà degli interessati derivanti da un trattamento (art. 35 GDPR).
- Obbligo: Necessaria quando il trattamento utilizza nuove tecnologie, prevede un monitoraggio sistematico, o tratta dati sensibili su larga scala.
- Contenuto: Descrizione del trattamento, valutazione della necessità/proporzionalità, analisi dei rischi e misure di mitigazione.

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

TIA (Transfer Impact Assessment - Valutazione d'Impatto sul Trasferimento)

- Finalità: Analizzare se la normativa del paese terzo garantisce un livello di protezione equivalente a quello dell'UE, a seguito della sentenza Schrems II.
- Procedura: L'esportatore di dati (titolare/responsabile) deve valutare la legislazione locale del paese importatore e implementare garanzie aggiuntive se necessario.
- Data Privacy Framework (DPF): Con il nuovo accordo UE-USA, per i trasferimenti verso aziende statunitensi certificate DPF, la TIA potrebbe non richiedere garanzie aggiuntive, sebbene la verifica resti necessaria.

In sintesi la DPIA è una valutazione interna e strutturale del rischio di un trattamento e la TIA è una valutazione specifica per il trasferimento dei dati al di fuori dello Spazio Economico Europeo. Entrambi i documenti sono fondamentali per dimostrare l'accountability del Titolare del trattamento.

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Titolo: DPIA/TIA per l'adozione della piattaforma Microsoft 365 for Education nello svolgimento delle attività didattiche ed amministrative

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

L'adozione degli strumenti della presente DPIA è finalizzata al perseguimento di un rilevante interesse pubblico e non si è ritenuto necessario richiedere un parere agli interessati. Qualora vi fossero suggerimenti da parte dell'utenza, l'amministrazione si impegna ad effettuare successivi aggiornamenti della presente DPIA che tengano conto delle stesse.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Questa DPIA è atta alla valutazione dell'impatto connesso all'uso della piattaforma Microsoft 365 for Education nello svolgimento delle attività svolte dall'amministrazione scolastica. Il documento valuta i trattamenti operati in ambito didattico e quelli operati in ambito amministrativo, pur riconoscendo che la medesima piattaforma viene utilizzata per entrambe le finalità.

Ambito didattico/formativo

Per quanto riguarda l'ambito didattico/formativo, la piattaforma è utilizzata principalmente per condurre le attività didattiche e favorire la comunicazione fra alunni e docenti. Tali attività possono essere svolte sia da scuola che da casa, garantendo continuità didattica in qualsiasi circostanza.

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Ambito amministrativo e organizzativo

La medesima piattaforma Microsoft viene utilizzata per favorire la comunicazione e la collaborazione fra le varie componenti scolastiche per finalità organizzative ed amministrative.

Quali strumenti si vogliono adottare?

La piattaforma adottata dispone di strumenti di comunicazione e di lavoro collaborativo che possono essere utilizzati da alunni e docenti per le attività didattico/formative ma anche dal personale amministrativo e dai diversi organi collegiali dell'istituto per le proprie finalità. Ogni utente della piattaforma deve avere una sua identità digitale ed una casella di posta elettronica ad esso riconducibile rilasciata dalla scuola stessa. Non è infatti possibile, anche per rispettare le disposizioni del Regolamento UE 679/2016 (nel seguito GDPR), utilizzare per le finalità perseguite dalla scuola le caselle email personali di dipendenti, alunni o loro familiari.

Con la propria identità digitale ciascun utente registrato deve poter utilizzare:

- Strumenti di videocomunicazione
- Strumenti per la realizzazione e la condivisione di documenti
- Strumenti di presentazione
- Strumenti per la gestione delle lezioni
- Strumenti di produttività e di lavoro collaborativo Tali strumenti sono stati scelti sulla base dei seguenti criteri:
- Rispetto della normativa sulla protezione dei dati personali
- Facilità di impiego da parte degli utenti
- Semplicità di gestione da parte di personale non esperto
- Efficienza
- Sicurezza
- Costi

Perché questa DPIA?

Sulla base dei criteri sopra esposti il nostro istituto ha deliberato per l'adozione della piattaforma Microsoft 365 a seguito delle disposizioni contenute nei decreti, emanati ai sensi dell'art. 3 del d.l. 23 febbraio 2020, n. 6, che hanno disposto - per tutta la durata della sospensione delle attività

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

didattiche “in presenza” nelle scuole a causa della diffusione di Covid 19 - l’attivazione di modalità di didattica a distanza.

La scelta è stata fatta valutando gli aspetti sopra riportati e sulla base delle indicazioni provenienti dal Ministero dell’Istruzione che ha riportato nel suo sito l’elenco delle risorse che le scuole potevano prendere in considerazione per lo svolgimento dell’attività DAD, fra le quali era anche presente la piattaforma poi adottata dalla scuola. Si è altresì provveduto a verificare la certificazione AgID dell’applicazione adottata (oggi gestita da Agenzia della Cybersicurezza Nazionale), condizione prevista come necessaria all’adozione di piattaforme cloud da parte della pubblica amministrazione.

Opzione 1 (scuole che emettono DPIA per la prima volta)

A causa della situazione emergenziale in cui ha dovuto allora operare, la scuola non ha effettuato alcuna valutazione di impatto sul trattamento di dati personali operati sulla piattaforma come peraltro ammesso dal provvedimento del garante Privacy 26 marzo 2020, n.64 che, oltre a indicare come non necessaria la redazione di una DPIA, si era anche impegnato a vigilare sulle soluzioni adottate e quindi a comunicare alle scuole eventuali impedimenti all’uso delle piattaforme cloud. In considerazione dell’importanza e della rilevanza assunta dai trattamenti operati sulla piattaforma cloud oggi condotti anche con strumenti di intelligenza artificiale (valutati all’interno di altra DPIA specifica) riteniamo di dover procedere alla redazione della presente Data Privacy Impact Assessment (DPIA).

Quali sono le finalità del trattamento?

La base giuridica dei trattamenti operati per le attività sopra menzionate è costituita dall’esecuzione di un compito di interesse pubblico di cui è investita la scuola (art. 6 comma 1 lettera e del GDPR).

In generale si rileva che da anni i vari governi che si sono succeduti si impegnano a favorire, per l’attuazione del D. Lgs 82/2005 (CAD), la transizione digitale delle pubbliche amministrazioni, vista come strumento per contenere i costi e garantire una migliore efficienza dei servizi. La transizione digitale e il passaggio al cloud **sono** quindi uno dei principali obiettivi stabiliti dal **Piano Nazionale Scuola Digitale**, dai **piani triennali per l’informatica nelle PA** ed una delle attività finanziate dal **PNRR**. Questo è anche vero nel contesto scolastico in cui l’insegnamento di competenze digitali integrate è da considerarsi centrale nell’educazione dell’individuo in qualsiasi fascia di età, e

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

l'utilizzo consapevole di questi strumenti durante l'attività didattica è una delle metodologie che possono facilitarne l'apprendimento. La messa a disposizione e l'utilizzo continuo di strumentazioni digitali di coordinamento, comunicazione e gestione di contenuti digitali proposti dalla piattaforma, infatti, rientra pienamente nell'approccio innovativo di apprendimento “Learning by Doing” più volte consigliato dal ministero, sulla scorta delle competenze chiave europee, per l'apprendimento delle discipline STEAM e, più in generale, di tutte le discipline scolastiche, nonché per lo sviluppo delle *life skills*.

E' necessario richiedere il consenso per l'utilizzo della piattaforma?

In considerazione dell'interesse pubblico perseguito non è necessario richiedere il consenso al trattamento da parte degli interessati. D'altronde la negazione del consenso, ove richiesto, impedirebbe alla scuola di conseguire le proprie finalità istituzionali. Questo è anche il parere espresso dal garante nel provvedimento 26 marzo 202, n.64.

Ci sono standard applicabili al trattamento?

Primo riferimento relativo ai trattamenti in questione è costituito dal documento edito dall'European Data Protection Board (EDPD) intitolato **“2022 Coordinated Enforcement Action Use of cloud-based services by the public sector”** ([link](#)) nel quale sono indicate le misure di sicurezza e le azioni da intraprendere per garantire al meglio la protezione dati degli utenti durante l'utilizzo di piattaforme cloud. L'EDPD ha pubblicato in precedenza le **“Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE”** ([link](#)) che vengono in rilievo per il trasferimento di dati all'estero.

Ulteriori indicazioni provengono dal Ministero dell'Istruzione che ha pubblicato nell'estate del 2020 le Linee Guida per la Didattica Digitale Integrata (DDI) ([link](#)) contenenti indicazioni operative per la redazione di un piano per la didattica digitale integrata da parte di ciascun istituto scolastico. In relazione alla individuazione dei fornitori viene in rilievo la **circolare AGID n. 2 del 09/04/2018** ([link](#)) che dispone che le Pubbliche Amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati da AGID (oggi attività demandata a Agenzia per la Cybersicurezza Nazionale – ACN). In relazione all'adozione delle piattaforme cloud da parte delle istituzioni scolastiche si è preso anche di riferimento il **Provvedimento del Garante del 26 marzo 2020 - "Didattica a distanza: prime indicazioni"** ([link](#)) nel quale si dichiara come non necessaria la valutazione di impatto, ex art. 35 del GDPR che tuttavia viene redatta nel presente documento.

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Dati, processi e risorse di supporto

Quali sono i dati trattati?

In ambito didattico, la didattica da remoto permette di utilizzare le modalità di didattica cooperativa rese possibili dalle peculiari capacità di condivisione dati proprie delle strumentazioni digitali. Nel caso specifico, gli strumenti hardware di proprietà della scuola o degli studenti vengono utilizzati con l'intento di svolgere compiti didattici o di avere accesso a materiale formativo.

Le attività didattiche sono quindi svolte tramite la piattaforma elettronica che facilita la condivisione dei dati e l'organizzazione del lavoro di gruppo. La piattaforma, facendo utilizzo di tecnologie cloud, si trova quindi a contenere, oltre alle informazioni necessarie per identificare univocamente alunni, docenti ed eventuali altri interessati, tutta una serie di dati e informazioni da essi prodotti, che perlopiù potrebbero essere condivisi tra diverse parti in causa, specialmente durante la loro stesura nel caso di progetti di didattica cooperativa.

Questo tipo di dati include dati relativi alla didattica degli alunni e dei docenti. Tali informazioni dipenderanno ovviamente dalla natura e materia didattica svolte, ma potrebbero contenere dati o informazioni a rischio per la privacy degli interessati. A titolo di esempio, potrebbero contenere degli scritti che definiscono esplicitamente l'orientamento politico, la razza o la condizione sanitaria degli interessati, che potrebbero essere di minore età.

Dati trattati in ambito amministrativo

In ambito amministrativo, la piattaforma viene utilizzata per il trattamento di dati personali del personale scolastico (docenti e personale ATA) e per la gestione della documentazione istituzionale. In particolare, vengono trattati: dati identificativi e di contatto del personale; comunicazioni interne relative all'organizzazione del lavoro; verbali delle riunioni degli organi collegiali; documentazione relativa ai progetti e alle attività dell'istituto; corrispondenza istituzionale.

Per quanto riguarda i dati particolari (ex dati sensibili), sia in ambito didattico che amministrativo, è necessario definire delle policy specifiche che ne limitino l'uso sulla piattaforma, in considerazione delle caratteristiche tecniche della stessa e delle garanzie che può offrire in relazione alla localizzazione dei dati, come meglio specificato nella sezione dedicata al trasferimento dati extra UE.

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

L'intero ciclo di vita dei dati passa attraverso delle fasi che presentano dei rischi potenziali. In particolare l'istituto attiva per gli studenti delle utenze personali sulla piattaforma cloud che dovranno essere utilizzate, con dispositivi di proprietà della scuola o degli studenti, per lo svolgimento delle attività istituzionali. Durante le attività didattiche tali servizi saranno utilizzati per affidare agli studenti dei compiti, a volte da svolgere in team, che prevedono la produzione di materiale. Tale materiale verrà con tutta probabilità conservato su server cloud e condiviso tra i vari membri del team. Alla fine della produzione dello stesso, si potrà procedere all'archiviazione del materiale da parte dei docenti interessati, che ne potrebbero fruire all'atto di esprimere (ed eventualmente di giustificare) una valutazione sull'operato degli studenti. A tal fine, la documentazione ottenuta si potrebbe profilare quale atto amministrativo endoprocedimentale. In questo particolare caso, sarebbe compito del docente procedere all'archiviazione dei documenti nel momento in cui non sia più necessaria alcuna modifica da parte degli alunni. L'archiviazione dovrà essere effettuata in modo tale da rendere non accessibile la documentazione agli interessati, che potranno averne accesso o richiederne la modifica, rettifica o cancellazione solamente tramite richiesta scritta che non limiti le finalità del trattamento, orientate al corretto svolgimento dell'attività didattica.

Per quanto riguarda la cancellazione dei dati, la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" prescrive la conservazione di elaborati delle prove scritte, grafiche e pratiche per almeno un anno, e la conservazione di documentazione campione un anno ogni dieci (si suggerisce per omogeneità di non scartare i documenti relativi agli anni scolastici terminanti in 7/8, es. '67/'68, '77/'78 etc.).

Quali sono le risorse di supporto ai dati?

I dati oggetto del trattamento risiedono sulla piattaforma Microsoft 365 for Education. L'accesso alla piattaforma avviene attraverso molteplici dispositivi quali tablet, pc e smartphone, che a loro volta possono essere basati su diversi sistemi operativi e permettere la fruizione dei servizi tramite diversi browser o app. I dispositivi utilizzati possono essere di proprietà della scuola o dell'utente. L'accesso può avvenire sia dai locali scolastici sia da casa.

Liceo Statale "C. Lorenzini"

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Trasferimento dati extra UE

E' previsto il trasferimento di dati al di fuori dell'Unione europea?

Microsoft ha avviato il progetto UE Data Boundary che limita l'archiviazione dei dati sulla piattaforma Office 365 al territorio europeo per i clienti che attivano il servizio dall'Italia. Esistono tuttavia scenari in cui:

- Microsoft continuerà a trasferire dati al di fuori del **limite dei dati dell'UE** per soddisfare i requisiti operativi del servizio cloud
- I dati archiviati nel **limite dei dati dell'UE** saranno accessibili in remoto dal personale situato al di fuori del **limite dei dati dell'UE**
- L'uso di Servizi **limiti dati dell'UE** da parte di un cliente comporterà il trasferimento dei dati al di fuori del **limite dei dati dell'UE** per ottenere i risultati desiderati del cliente

In tutti questi casi Microsoft garantisce che i trasferimenti di dati dei clienti al di fuori del **limite dei dati dell'UE** siano protetti da misure di sicurezza dettagliate nei contratti di servizi.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Sì. In data 10 luglio 2023 è stato approvato dalla Commissione Europea il Data Privacy Framework che stabilisce che gli Stati Uniti d'America garantiscono un livello di protezione adeguato al trasferimento dei dati personali dei cittadini europei alle aziende d'Oltreoceano e paragonabile a quello dell'Unione Europea. Ciò rende pienamente conformi al GDPR il trasferimento di dati personali verso aziende che, come Microsoft, sono certificate Dpf.

Le condizioni contrattuali sottoscritte forniscono garanzie di adeguatezza ex art. 46 GDPR?

A seguito dell'approvazione dello US-EU Data Privacy Framework il trasferimento dei dati sui sistemi Microsoft avviene sulla base di una dichiarazione di adeguatezza (art. 45 GDPR). Ciò detto anche le condizioni contrattuali prevedono delle specifiche condizioni di sicurezza.

I trattamenti operati da Microsoft sono regolamentati dal Data Processing Agreement (DPA) dove oltre ad attestare la conformità ed il rispetto delle disposizioni del GDPR, viene dichiarato quanto segue:

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Pag. 9 – trasferimento dei dati

Tutti i trasferimenti dei Dati Personali fuori dall'Unione Europea effettuati da Microsoft per fornire i Prodotti e i Servizi, verranno disciplinati dalle Clausole Contrattuali Tipo 2021 adottate da Microsoft. Tutti i trasferimenti di Dati Personali verso un paese terzo o un'organizzazione internazionale saranno soggetti alle misure di sicurezza appropriate descritte nell'Articolo 46 del GDPR e tali trasferimenti e misure di sicurezza saranno documentati conformemente all'Articolo 30(2) del GDPR

Pag. 10 – Posizione dei dati della società

Per quanto riguarda i Servizi Online, ai quali viene applicata la soluzione EU Data Boundary, Microsoft archiverà e tratterà i Dati della Società all'interno dell'Unione Europea come stabilito nelle Condizioni per l'Utilizzo dei Prodotti

La valutazione concreta dell'effettivo rispetto del GDPR nei trattamenti operati sulla piattaforma Microsoft è resa complessa dalle dimensioni della nostra amministrazione che, pur supportata dal proprio DPO, non può contare su personale interno con adeguate competenze tecniche. Gli istituti scolastici non hanno poi alcun potere contrattuale nei confronti delle multinazionali del settore per cui è difficile entrare nel merito di certi aspetti contrattuali ed ancor meno è possibile, ove necessarie, definire condizioni personalizzate (c.d. tailored) sulle garanzie e responsabilità delle parti relativamente a tutti i processi di trattamento dati gestiti da Microsoft. Come detto nel documento di EDPB “2022 Coordinated Enforcement Action Use of cloud-based services by the public sector” ([link](#)), è invece auspicabile un intervento di gruppo che permetta una contrattazione collettiva che garantisca una maggiore equità nel potere contrattuale delle parti. In questo senso riteniamo possa svolgere un ruolo fondamentale il Responsabile della Transizione Digitale per le scuole italiane, ruolo ricoperto dal Direttore Generale dei sistemi informativi del Ministero dell'Istruzione, che potrebbe avviare le interlocuzioni eventualmente necessarie con Microsoft e Google al fine di chiarire alcuni aspetti dei trattamenti operati sulle piattaforme.

Il trasferimento è necessario per importanti motivi di interesse pubblico?

SI. La base giuridica del trasferimento dei dati all'estero una dichiarazione di adeguatezza (art. 45 GDPR) ed i trattamenti operati sono necessari all'esecuzione di un compito di interesse pubblico di cui è investita la scuola. L'uso della piattaforma oggetto di analisi è finalizzato al perseguimento

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

delle finalità istituzionali di istruzione e formazione. Altro utilizzo del medesimo strumento è finalizzato a condurre la transizione digitale imposta alle PA dal D. Lgs 82/2005 (CAD), dal PNSD, dai piani triennali per l'informatica nelle PA e dal PNRR.

E' possibile perseguire l'interesse pubblico con altri strumenti?

Per lo svolgimento della propria attività istituzionale, la scuola adotta, ove possibile, le piattaforme ministeriali o quelle messe a disposizione dal proprio fornitore di segreteria digitale. Tali strumenti forniscono garanzie sulla collocazione in Italia dei sistemi e dei dati trattati. Tuttavia, la piattaforma Microsoft viene utilizzata per avere accesso a servizi e funzionalità non usufruibili con le altre piattaforme, in particolare per quanto riguarda gli strumenti di lavoro collaborativo, la videocomunicazione, la gestione delle classi virtuali e la condivisione di documenti in tempo reale. Si tratta di funzionalità oggi ritenute indispensabili per lo svolgimento dell'attività didattica e per garantire la continuità educativa in qualsiasi circostanza, nonché per favorire l'acquisizione delle competenze digitali da parte degli studenti. L'uso degli stessi strumenti è oggi necessario anche per lo svolgimento dell'attività amministrativa.

Esistono possibili alternative alla piattaforma adottata?

Il mercato delle piattaforme cloud per la collaborazione e la produttività è attualmente dominato da fornitori statunitensi, in particolare Google e Microsoft, che offrono soluzioni mature, affidabili e ampiamente diffuse. Ad oggi non esistono alternative equivalenti fornite da aziende europee che possano garantire il medesimo livello di funzionalità, integrazione, facilità d'uso e affidabilità. Per quanto riguarda le soluzioni opensource, pur esistendo piattaforme teoricamente utilizzabili, la loro adozione da parte di un'istituzione scolastica presenta notevoli difficoltà. Tali soluzioni richiedono infatti competenze tecniche specialistiche per l'installazione, la configurazione e la manutenzione, competenze di cui le scuole non dispongono e che non possono ragionevolmente acquisire. Inoltre, l'assenza di un supporto tecnico strutturato, la necessità di gestire autonomamente gli aggiornamenti di sicurezza e la minore stabilità rispetto alle soluzioni commerciali rendono le piattaforme opensource non praticabili nel contesto scolastico, dove è fondamentale garantire continuità di servizio e semplicità di utilizzo per utenti con competenze informatiche eterogenee.

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Quali misure di sicurezza sono state adottate?

Valutata l'inesistenza di possibili soluzioni alternative che diano maggiori garanzie di adeguatezza si è proceduto con l'applicare il principio di minimizzazione del rischio stabilito anche dal recente report di EDPB (Use of cloud-based services by the public sector Adopted - 17 January 2023 - [link](#)). A tal fine si sono prese in considerazione misure di sicurezza supplementari attuabili in un contesto scolastico tralasciando soluzioni tecniche troppo complesse da implementare e da gestire in assenza di personale tecnico specializzato.

Le misure di contenimento dei rischi che sono state prese in considerazione sono:

- **Coinvolgimento del DPO:** nella presente valutazione è stato coinvolto direttamente il DPO
- **Corretta attribuzione dei ruoli:** sono state adottate misure organizzative tali da garantire concretamente la gestione del rischio attraverso l'individuazione di specifici ruoli e responsabilità.
- **Valutazione dei dati da trattare:** anche la scelta dei dati personali oggetto di trattamento sulla piattaforma cloud è stata valutata alla luce dei principi di necessità (per i dati sensibili) e di riduzione del rischio (per i dati personali comuni).
- **Valutazione dei servizi necessari:** per la minimizzazione dei rischi si è anche valutato di limitare l'uso delle applicazioni da utilizzare nella piattaforma.
- **Anonimizzazione, cifratura e pseudonimizzazione:** per garantire adeguati livelli di protezione si sono prese in considerazione tecniche di anonimizzazione, cifratura e pseudonimizzazione.
- **Definire regolamenti e disposizioni specifiche per l'uso delle piattaforme:** l'istituto ha formato un coerente corpo documentale con informative, disciplinari e regolamenti atti a gestire il trattamento dei dati personali sulla piattaforma cloud e sui sistemi informatici dell'istituto in generale.

E' stato coinvolto il DPO nella valutazione dei rischi?

Sì. Il DPO ha fornito supporto ed assistenza nella redazione del presente documento come dell'altra documentazione prodotta per l'uso della piattaforma nel rispetto della normativa.

Sono stati attribuiti correttamente ruoli e responsabilità?

La complessità delle azioni e dei possibili rischi in termini di violazione dei Dati Personali implica

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

una collaborazione fattiva tra le varie parti in causa. Queste sono, in particolare:

- **Il titolare del trattamento:** in questo caso l'Amministrazione Scolastica, rappresentata legalmente dal Dirigente Scolastico (D.S.), che assume un ruolo centrale di supervisione e guida nei confronti dell'operato dei docenti e di tutte le parti che fruiscono del servizio. Inoltre, è compito del D.S. quello di definire un codice di condotta interno alla scuola che regoli l'utilizzo della strumentazione elettronica e la piattaforma utilizzate, e di sorvegliare sulla sua attuazione.
- **I docenti:** Il loro ruolo centrale nella produzione di compiti e contenuti deve essere associato ad un'attività di controllo nei confronti di tutte quelle attività suscettibili di violazioni della privacy e dei dati personali. I docenti hanno funzioni di supervisione delle modalità di utilizzo della piattaforma relativamente alle attività didattiche da loro gestite.
- **Il consiglio di classe:** Delibera sulla valutazione finale in fase di scrutini. Potrebbe quindi essere necessario allo stesso l'accesso ai documenti prodotti in modalità digitale, ivi inclusi i dati personali.
- **Il Responsabile della Protezione dei Dati (RPD/DPO):** ha il compito di fornire supporto a titolare, docenti e interessati, per tutte quelle questioni concernenti la protezione dei dati personali all'interno dell'ambito di applicazione del trattamento.
- **I responsabili del trattamento:** il fornitore della piattaforma deve agire come responsabile del trattamento e 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. Microsoft è stata verificata come inserita nel Cloud Marketplace gestito dall'Agenzia per la Cybersicurezza Nazionale nell'elenco SaaS.
- **Amministratore della piattaforma Microsoft:** è stato individuato fra il personale scolastico colui che, in possesso di adeguata esperienza e competenza, gestisce gli utenti ed i servizi erogati dalla piattaforma.

E' stato applicato un principio di minimizzazione dei dati personali trattati?

Con l'obiettivo di ridurre i rischi associati si è limitato il trattamento ai dati necessari per il conseguimento delle finalità sopra richiamate. In particolare per ogni utente la scuola ha caricato soltanto il nome ed il cognome a cui è stato poi attribuita una casella istituzionale costituita da nome.cognome@dominio.scuola. È stata disabilitata la possibilità di aggiungere ulteriori informazioni da parte dell'utente proprietario del profilo quali telefono, email alternative e foto.

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Il principio di minimizzazione dei dati personali dovrà essere tenuto in considerazione anche da tutti gli utenti che dovranno evitare di inserire nei documenti caricati sulla piattaforma dati personali non necessari e non pertinenti con la finalità del documento.

Sono state adottate particolari misure per il trattamento di dati sensibili?

Per il trattamento dei dati sensibili sono state date agli utenti indicazioni di stretta necessità dell'informazione prima del suo inserimento in un documento da caricare nella piattaforma cloud (riferimento Circolare n.43 del 01/10/2025 - Informativa del Regolamento Europeo 2016-679 per il trattamento dei dati personali degli alunni e delle famiglie – prot. n. 8583 del 01/10/2025 e relativa informativa ex art. 13 e 14 del Regolamento Europeo 2016/679 per il trattamento dei dati personali degli alunni e delle famiglie, prot. n. 8572 del 01/10/2025). Per quanto riguarda gli alunni, i docenti sono stati invitati a valutare attentamente l'opportunità di proporre ad essi attività che prevedono il trattamento di dati ed informazioni sensibili e di valutare possibili alternative all'uso della piattaforma. **In considerazione dell'assenza della funzionalità Data Residency, per la documentazione contenente dati particolari (quali ad esempio il Piano Educativo Individualizzato - PEI o il Piano Didattico Personalizzato - PDP), la scuola valuterà l'adozione di tecniche di criptaggio o di pseudonimizzazione.**

Con la tecnica di criptaggio si rende accessibile l'informazione solo a coloro che sono in possesso di una chiave di decodifica.

Con la tecnica di pseudonimizzazione, in luogo del nome e cognome del soggetto si mette nel documento un codice univoco ad esso riconducibile attraverso una chiave che associa nome a codice.

Nelle more dell'adozione di eventuali tecniche di criptaggio e/o pseudonimizzazione non si prevede di utilizzare la piattaforma Microsoft 365 for Education per il trattamento di dati sensibili inerenti PEI e PDP.

Nello specifico, dovrà, comunque, essere effettuata una valutazione caso per caso che tenga conto della natura del dato, delle finalità del trattamento, del contesto e delle misure di sicurezza applicabili, al fine di verificare se il livello di protezione offerto dalla piattaforma sia adeguato al

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

rischio specifico (riferimento Circolare n. 121 del 20/11/2025 - Linee guida per il corretto trattamento dei dati personali particolari (ex dati sensibili), Prot. n.10259 del 20/11/2025).

Il principio di stretta necessità del dato sensibile dovrà anche essere utilizzato da tutto il personale nella redazione della documentazione di propria competenza. Per il trattamento dei dati sensibili si valuterà la necessità di adottare tecniche di cifratura o pseudonimizzazione a seconda della rilevanza dei dati trattati.

E' stato applicato un principio di minimizzazione anche in relazione alle applicazioni utilizzate?

Sì. Anche nella scelta dei servizi e delle applicazioni utilizzate si sono tenuti presenti i principi di necessità e di minimizzazione per ridurre i possibili rischi associati al loro uso. Al termine di tale valutazione si è deciso di attivare le seguenti applicazioni:

- Caselle di posta elettronica
- Sistema di videoconferenza
- App di terze parti necessarie allo svolgimento dell'attività didattico/formativa o a condurre l'attività scolastica in genere

Come ulteriore misura di contenimento dei rischi si è limitata la comunicazione con le caselle di posta elettronica a quelle realizzate nel dominio associato alla scuola.

Sono state adottate tecniche di anonimizzazione, pseudonimizzazione e cifratura per la protezione dei dati personali?

Come detto più sopra nella relativa sezione, saranno adottate tecniche di cifratura e di pseudonimizzazione per la tutela di documenti contenenti dati particolarmente sensibili (come, ad esempio, i PEI).

Si è anche presa in considerazione l'opportunità di procedere alla pseudonimizzazione dei dati personali identificativi caricati sulla piattaforma. In particolare si è valutata la possibilità di caricare nella piattaforma non il nome e cognome dell'utente ma il codice di pseudonimizzazione ad esso associato. Adottando tale soluzione la casella associata all'utente non sarà più nome.cognome@dominio.scuola ma codice-utente@dominio.scuola. In tal modo, tuttavia, si complica notevolmente la gestione della piattaforma e diventa complessa la comunicazione email, fatto che comporta un sensibile aumento del rischio di errori che possono condurre anche a

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

rilevati violazioni dei dati personali (si pensi ai problemi che possono nascere da errori nella digitazione del destinatario di una comunicazione o alla perdita della chiave che associa un codice ad un determinato utente). **Al termine della valutazione del rischio condotta si ritiene che adottare tecniche di pseudonimizzazione del nome e cognome degli utenti e delle caselle email ad esse associate comporti non una diminuzione ma un sensibile aumento del rischio associato.**

E' stata fornita agli utenti idonea informativa e sono state portate a conoscenza di essi le procedure di utilizzo della piattaforma?

Sì. Tutti gli utenti registrati sulla piattaforma hanno ricevuto specifica informativa privacy per i trattamenti di dati personali operati sulla piattaforma cloud adottata dalla scuola. In essa gli interessati sono stati informati della nomina di Google a responsabile del trattamento e dei trasferimenti all'estero operati dei dati personali. Sono state fornite a tutti gli utenti disposizioni specifiche per l'uso corretto della piattaforma e tali da garantire la sicurezza e la protezione dei dati personali in essa trattati (riferimento Circolare n.14 del 12/09/2025 - Procedura comunicazioni interne SCUOLA -FAMIGLIA e Circolare n. 43 del 01/10/2025 - Informativa del Regolamento Europeo 2016-679 per il trattamento dei dati personali degli alunni e delle famiglie – prot. n. 8583 del 01/10/2025 e relativa informativa ex art. 13 e 14 del Regolamento Europeo 2016/679 per il trattamento dei dati personali degli alunni e delle famiglie, prot. n. 8572 del 01/10/2025).

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento prevede l'utilizzo di tecniche didattiche innovative atte allo svolgimento dell'insegnamento scolastico in modalità digitale e a sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione degli studenti.

Lo scopo ultimo è quello di formare gli studenti all'utilizzo di piattaforme e servizi digitali, con l'effetto collaterale di aumentarne la consapevolezza nell'uso dell'ambito tecnologico, lato fruizione e lato produzione. Tale consapevolezza è utile fin dalle classi di ordine inferiore e diventa necessaria a orientarsi nella scelta del futuro percorso di studio e/o professionale da intraprendere per gli studenti degli istituti superiori. In questo processo è importante l'utilizzo di software e attrezzature dedicati fra i quali abbiamo deciso di puntare su strumenti molto diffusi e spesso già

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

utilizzati dagli studenti e dal personale scolastico. I dati personali relativi alle attività didattiche possono portare ad una valutazione degli studenti stessi da parte dei docenti, e sono suscettibili di diventare atti amministrativi scolastici.

Gli stessi strumenti adottati per condurre l'attività didattico/formativa devono essere utilizzati anche per favorire la comunicazione fra le varie componenti scolastiche per finalità organizzative ed amministrative. Da qui l'uso di sistemi di videocomunicazione, email e di condivisione documenti e risorse anche nello svolgimento delle attività dei vari organi collegiali, delle commissioni e più in generale del personale scolastico che allo scopo è stato dotato dall'amministrazione scolastica di una casella email istituzionale.

Quali sono le basi legali che rendono lecito il trattamento?

La base legale del trattamento è l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; In particolare il trattamento viene effettuato sulla base del Piano Triennale dell'Offerta Formativa dell'Istituto che prevede l'utilizzo di sistemi digitali di supporto alla didattica per il conseguimento delle proprie finalità istituzionali.

L'utilizzo degli strumenti di formazione a distanza ha fondamento anche nei seguenti riferimenti normativi:

- D. Lgs 82/2005 (Codice che traccia il quadro legislativo entro cui deve attuarsi la digitalizzazione della pubblica amministrazione)
- Legge 13 Luglio 2015, n. 107 (Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti – PNSD).
- D. L. 179/2012 convertito con L. 221/2012
- D.L. n. 95/2012 (che ha introdotto per le istituzioni scolastiche l'uso del registro elettronico)
- D. Lgs 297/1994 (Approvazione del testo unico delle disposizioni legislative vigenti in materia di istruzione, relative alle scuole di ogni ordine e grado) che all'art. 1 stabilisce la libertà di insegnamento.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Il personale è invitato a raccogliere (e archiviare) la quantità minima di informazioni necessaria al corretto svolgimento delle loro funzioni. I principi di adeguatezza, pertinenza e minimizzazione dovranno essere applicati in modo stringente per i dati particolari di cui all'art. 9 del GDPR (dati

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

sensibili) che dovranno essere trattati solo se strettamente necessari, e comunque utilizzando degli strumenti di minimizzazione e protezione dei dati (ad es. pseudonimizzazione).

I medesimi principi dovranno anche essere presi in considerazione nel valutare i dati ed i documenti che gli alunni, ma anche i docenti, potranno in modo autonomo caricare sulla piattaforma in cloud.

E' peraltro importante fornire adeguate informazioni agli utenti e vigilare affinché i dati trattati non esulino dalle esigenze formative connesse all'ambito didattico o, più genericamente, istituzionale.

I dati sono esatti e aggiornati?

Si. Tuttavia la procedura di raccolta e conservazione dei dati prevede la creazione spesso cooperativa di contenuti, perciò potrebbe presentarsi il caso in cui un elaborato venga deliberatamente modificato da eventuali collaboratori durante il suo processo di creazione. In tal caso, è preferibile utilizzare uno strumento che tenga traccia delle modifiche apportate alla documentazione, tramite soluzioni di backup e di cronologia delle modifiche (versioning).

Qual è il periodo di conservazione dei dati?

La conservazione dei dati è necessaria per un periodo strettamente necessario allo svolgimento dell'attività formativa o amministrativa prevista. Successivamente ad essa, i dati verranno archiviati dal docente (anche attraverso una apposita funzionalità proposta dal servizio, ove presente), e la documentazione prodotta verrà resa inaccessibile agli interessati, salvo richiesta scritta di accesso o cancellazione degli interessati.

Nel caso in cui gli elaborati debbano essere oggetto di valutazione, l'archiviazione deve essere mantenuta per almeno un anno dalla produzione, a meno che non ci si trovi nei casi particolari previsti dalla Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" che prescrive la conservazione di documentazione campione un anno ogni dieci. In tal caso, bisogna distinguere i due casi:

- **dati ed elaborati non soggetti a valutazione:** non hanno necessità di essere conservati per eventuali verifiche o controlli per cui devono essere cancellati nel momento in cui termina l'attività formativa svolta. Di norma tali dati vanno cancellati alla fine dell'anno scolastico a meno che l'attività programmata si svolga su più anni scolastici ed è necessario per essa operare qualche forma di trattamento anche sui dati raccolti gli anni precedenti;

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

- **dati ed elaborati soggetti a valutazione:** il periodo di conservazione deve rispettare le disposizioni previste dalla legge fra cui la citata circolare n°44 del 19/12/2005 della Direzione Generale degli archivi-.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati vengono informati del trattamento precedentemente all'inizio dello stesso, tramite somministrazione di informativa ex Art. 13 del Reg. UE 2016/679. L'informativa viene somministrata a personale, alunni e genitori degli stessi tramite una combinazione più completa possibile dei canali disponibili alla scuola, che includono, a titolo esemplificativo e non esaustivo:

- L'utilizzo delle modalità di comunicazione scuola famiglia messe a disposizione dal registro elettronico.
- La pubblicazione nella sezione privacy del sito web istituzionale;
- L'invio della stessa agli indirizzi mail indicati da genitori, alunni e dipendenti (si sottolinea anche qui l'importanza di utilizzare il campo ccn per l'invio, che a differenza del campo "a" e "cc" consente l'invio a più destinatari senza dividerne gli indirizzi);

Gli interessati sono stati informati sulle modalità di trattamento e sui possibili rischi associati anche in relazione al possibile trasferimento dei dati personali al di fuori dell'UE. Durante il processo didattico stesso verranno forniti agli studenti le conoscenze necessarie ad un utilizzo consapevole della piattaforma anche per garantire la protezione dei dati personali propri e altrui (riferimento Circolare n. 43 del 01/10/2025 - Informativa del Regolamento Europeo 2016-679 per il trattamento dei dati personali degli alunni e delle famiglie – prot. n. 8583 del 01/10/2025 e relativa informativa ex art. 13 e 14 del Regolamento Europeo 2016/679 per il trattamento dei dati personali degli alunni e delle famiglie, prot. n. 8572 del 01/10/2025).

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso non costituisce base legale del trattamento e non viene richiesto agli interessati.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati possono sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

l'esercizio degli stessi (Circolare n.221 del 09/02/2026 - Rettifica Circolare n.217 - Regolamento UE 2016-679 per il trattamento dei dati personali - Diritto degli interessati, prot. 1200 del 10/02/2026).

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati possono sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi (Circolare n. 43 del 01/10/2025 - Informativa del Regolamento Europeo 2016-679 per il trattamento dei dati personali degli alunni e delle famiglie – prot. n. 8583 del 01/10/2025 e relativa informativa ex art. 13 e 14 del Regolamento Europeo 2016/679 per il trattamento dei dati personali degli alunni e delle famiglie, prot. n. 8572 del 01/10/2025 e Riferimento Circolare n.221 del 09/02/2026 - Rettifica Circolare n.217 - Regolamento UE 2016-679 per il trattamento dei dati personali - Diritto degli interessati, prot. 10/02/2026).

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati possono sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi (Riferimento Circolare n.221 del 09/02/2026 - Rettifica Circolare n.217 - Regolamento UE 2016-679 per il trattamento dei dati personali - Diritto degli interessati, prot. 1200 del 10/02/2026).

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

I trattamenti operati da Microsoft sono regolamentati dal Data Processing Agreement (DPA) dove vengono specificati gli obblighi del fornitore individuato responsabile del trattamento. E' tuttavia da rilevare lo scarso potere contrattuale detenuto dalla scuola nei confronti del fornitore e l'importanza che potrebbe avere il coinvolgimento diretto del Responsabile della Transizione Digitale delle istituzioni scolastiche, ruolo assunto dal Direttore Generale dei sistemi informativi del Ministero dell'Istruzione, che potrebbe avviare le interlocuzioni eventualmente necessarie con i fornitori al fine di chiarire alcuni aspetti dei trattamenti operati sulle piattaforme

Per quanto riguarda la valutazione dell'affidabilità dei servizi presi in esame, si è provveduto a verificare che il fornitore è inserito nel c.d. Cloud Marketplace gestito dall'agenzia all'**Agenzia per**

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

la **Cybersicurezza nazionale** nell'elenco SaaS (Software as a Service) con codice **SA-90** (Microsoft OFFICE 365).

Rischi

Misure esistenti o pianificate

Crittografia

Il fornitore cripta i dati per impostazione predefinita. I dati sono protetti con più livelli di sicurezza che includono tecnologie di crittografia all'avanguardia, come i protocolli HTTPS e Transport Layer Security. Non si è ritenuto opportuno adottare tecniche di cifrature client side.

Controllo degli accessi logici

L'accesso alle funzionalità delle piattaforme utilizzate deve essere regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software (il D.S. o un suo delegato).

Archiviazione

Tutta la documentazione relativa all'attività Istituzionale dell'Amministrazione è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.

Minimizzazione dei dati

I dati vengono trattati e archiviati in forma minima, per quanto previsto dalla normativa vigente. I dati sensibili sono limitati a quelli strettamente necessari.

Lotta contro il malware

I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus). È inoltre opportuno fornire agli utilizzatori delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali, che includano le istruzioni per una efficace lotta al malware.

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Backup

Sebbene il fornitore debba predisporre le soluzioni tecniche atte a garantire la reperibilità e l'integrità dei dati caricati sulla piattaforma è opportuno che la scuola valuti ulteriori misure di salvaguardia dei dati e dei documenti.

Manutenzione

Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware e software scolastici. Il fornitore della piattaforma cloud garantisce il corretto funzionamento e la sicurezza dei propri sistemi.

Contratto con il responsabile del trattamento

I trattamenti operati da Microsoft sono regolamentati dal Data Processing Agreement (DPA) dove vengono specificati gli obblighi del fornitore individuato responsabile del trattamento.

Politica di tutela della privacy

L'amministrazione ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente. I dipendenti sono stati nominati incaricati al trattamento ai sensi dell'Art. 2- quaterdecies del D.Lgs. 196/2003, per l'esercizio delle loro funzioni. Specifiche istruzioni e regolamenti sono stati emessi dall'istituto per la tutela dei dati personali nell'uso della piattaforma cloud.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L'amministrazione ha emesso un regolamento interno per la gestione dei data breach, al cui interno sono specificate le modalità di gestione degli incidenti che coinvolgono dati personali. Emessa anche una circolare per il personale che deve essere in grado di riconoscere un data breach quando interviene e che deve sapere cosa fare all'occorrenza (Circolare n.225 del 11/02/2026 - Procedura gestione violazione dati personali (data breach), prot. n. 1224 del 11/02/2026)

Valutazione del rischio

Riportiamo di seguito la valutazione della gravità dei seguenti rischi associati all'uso della piattaforma:

- Accesso illegittimo ai dati
- Modifiche indesiderate ai dati

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

- Perdita di dati

Prima di valutare la misura del rischio procederemo alla stima dei seguenti fattori:

entità del danno: 1. Trascurabile, 2. Limitata, 3. Importante, 4. massima

probabilità del rischio: 1. Trascurabile, 2. Limitata, 3. Importante, 4. Massima

L'**entità del rischio** sarà quindi un valore compreso fra 1 e 16 determinato come il prodotto fra **entità del danno** e la **probabilità del rischio**.

Accesso illegittimo ai dati

Il rischio: Il primo rischio che andiamo a valutare è l'accesso illegittimo ai dati che può intervenire a seguito di azioni accidentali o dolose. Le fonti del rischio sono le seguenti:

- errori nell'indicazione dell'indirizzo del destinatario di una comunicazione
- errato uso del campo CC al posto di quello CCN
- errori nella concessione dei permessi di accesso ai documenti al momento del caricamento sulla piattaforma
- azioni dolose da parti di utenti della piattaforma o di estranei per accedere a dati ed informazioni di terze persone

Misure atte a mitigare il rischio: tutte le misure adottate e citate al punto precedente sono atte a mitigare il rischio. Fra le più pertinenti citiamo:

- controllo degli accessi logici
- archiviazione
- minimizzazione dei dati
- pseudonimizzazione e anonimizzazione
- manutenzione
- politiche di tutela della privacy
- formazione
- procedure per la gestione degli incidenti

Stima gravità del danno: La gravità del danno per l'accesso illegittimo ai dati personali comuni possiamo ritenerla **limitata** (livello 2 su una scala di 4). Più grave l'accesso illegittimo ai dati di natura sensibile quando questo, ad esempio, coinvolge documenti di programmazione dell'attività didattica/educativa (PDP/PEI) legati a particolari condizioni dell'alunno. In tal caso la

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

venuta a conoscenza di tutti gli alunni della classe di situazioni personali e di salute particolari di un proprio compagno può comportare in questo e nella sua famiglia un notevole disagio. In questo caso la gravità del rischio può essere stimata come **importante** (livello 3 su una scala di 4).

Stima probabilità del rischio: A seguito delle misure di sicurezza già adottate la probabilità del rischio può essere valutata come **limitata** (livello 2 su una scala di 4). Per mantenere la probabilità di rischio ad un livello contenuto la scuola si impegna a portare avanti attività formative e di sensibilizzazione di tutti gli utenti della piattaforma.

Stima gravità del rischio:

Gravità del rischio = Danno x Probabilità

Gravità del rischio accesso illegittimo ai dati: $3 \times 2 = 6$ (valore massimo 16)

Modifiche indesiderate dei dati

Il rischio: Il secondo rischio che andiamo a valutare è la modifica indesiderata di dati. Le fonti del rischio sono le seguenti:

- errore umano
- azione volontaria di un utente della piattaforma o di un soggetto esterno

Misure atte a mitigare il rischio: tutte le misure adottate e citate al punto precedente sono atte a mitigare il rischio. Fra le più pertinenti citiamo:

- controllo degli accessi logici
- archiviazione e backup
- manutenzione
- politiche di tutela della privacy
- lotta contro i malware
- formazione
- procedure per la gestione degli incidenti

Stima gravità del danno: La gravità del rischio per modifiche indesiderate ai dati personali comuni possiamo ritenerla **limitata** (livello 2 su una scala di 4). Fra le eventualità più gravi da considerare è che la violazione potrebbe portare ad una errata valutazione dell'alunno. Tuttavia le misure di backup e controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.

Stima probabilità del rischio: A seguito delle misure di sicurezza già adottate la probabilità del rischio può essere valutata come **trascurabile** (livello 1 su una scala di 4). Per mantenere la

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

probabilità di rischio ad un tale livello la scuola si impegna a portare avanti attività formative e di sensibilizzazione di tutti gli utenti e dei docenti in particolare che devono vigilare sul corretto uso della piattaforma. Gli utenti, ed il personale scolastico in particolare, devono anche essere sensibilizzati sulle misure di sicurezza da adottare per tenere riservate le proprie credenziali ed evitare così un accesso indebito ai sistemi da parte di terzi.

Stima gravità del rischio:

Gravità del rischio = Danno x Probabilità

Gravità del rischio “modifiche indesiderate dei dati”: $2 \times 1 = 2$ (valore massimo 16)

Perdita di dati

Il rischio: Il terzo rischio che andiamo a valutare è la perdita di dati. Le fonti del rischio sono le seguenti:

- errore umano
- azione volontaria di un utente della piattaforma o di un soggetto esterno
- guasti ed altre cause accidentali

Misure atte a mitigare il rischio: tutte le misure adottate e citate al punto precedente sono atte a mitigare il rischio. Fra le più pertinenti citiamo:

- controllo degli accessi logici
- archiviazione e backup
- manutenzione
- politiche di tutela della privacy
- lotta contro i malware
- formazione
- procedure per la gestione degli incidenti

Stima gravità del danno: La gravità del rischio per modifiche indesiderate ai dati personali comuni possiamo ritenerla **limitata** (livello 2 su una scala di 4). Fra le eventualità più gravi da considerare è la perdita di documenti soggetti a valutazione da parte del docente o quella di documenti redatti dal personale scolastico.

Stima probabilità del rischio: A seguito delle misure di sicurezza già adottate la probabilità del rischio può essere valutata come **trascurabile** (livello 1 su una scala di 4). Per mantenere la

Liceo Statale "C. Lorenzini"

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

probabilità di rischio ad un tale livello la scuola si impegna a portare avanti attività formative e di sensibilizzazione di tutti gli utenti della piattaforma.

Stima gravità del rischio:

Gravità del rischio = Danno x Probabilità

Gravità del rischio "perdita dei dati": $2 \times 1 = 2$ (valore massimo 16)

Valutazione gravità del rischio

A seguito dell'analisi condotta abbiamo quindi ricavato le seguenti valutazioni:

Rischio	Entità del danno	probabilità	Gravità del rischio
Accesso illegittimo ai dati	3	2	6
Modifiche indesiderate ai dati	2	1	2
Perdita di dati	2	1	2

Quelle condotte sono delle valutazioni sommarie volte a stimare l'entità dei rischi connessi all'uso della piattaforma cloud. L'analisi condotta evidenzia come i rischi, valutati in relazione alla probabilità ed alla entità del danno, sono al di sotto di una soglia accettabile considerate le misure di contenimento del rischio già adottate. Non si ritiene quindi di dover fare analisi più approfondite sui rischi volte a stimare questi in modo più puntuale e alla ulteriore riduzione del rischio residuo.

Conclusioni

Al termine dell'analisi condotta nel presente documento, l'istituto conferma l'adozione della piattaforma Microsoft 365 for Education per lo svolgimento delle attività didattiche e amministrative, nel rispetto delle condizioni e delle cautele di seguito riepilogate.

La scuola, ove possibile, privilegia l'uso delle piattaforme ministeriali e di quelle messe a disposizione dal fornitore di segreteria digitale, che garantiscono la collocazione dei dati sul territorio nazionale. Tuttavia, tali piattaforme non offrono funzionalità essenziali per lo svolgimento dell'attività didattica moderna, quali gli strumenti di lavoro collaborativo in tempo

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

reale, la videocomunicazione integrata e la gestione delle classi virtuali. Per tali esigenze si rende necessario l'utilizzo della piattaforma Microsoft 365 for Education.

Si è valutato che i dati trattati dalle istituzioni scolastiche sono classificati come dati ordinari ai fini della normativa sulla qualificazione dei servizi cloud per la pubblica amministrazione. La piattaforma Microsoft 365 for Education risulta certificata dall'Agenzia per la Cybersicurezza Nazionale e, a differenza di altre soluzioni presenti sul mercato, garantisce attraverso il progetto EU Data Boundary la collocazione dei dati sul territorio dell'Unione Europea. Tale garanzia, unitamente all'adeguatezza riconosciuta dal Data Privacy Framework per eventuali trasferimenti residuali verso gli Stati Uniti, consente di ritenere pienamente conforme al GDPR l'utilizzo della piattaforma per il trattamento dei dati personali, sia comuni che particolari, in ambito didattico e amministrativo.

La garanzia della residenza dei dati in Europa costituisce un elemento di particolare rilevanza ai fini della presente valutazione, in quanto assicura un livello di protezione adeguato anche per il trattamento dei dati particolari ai sensi dell'art. 9 del GDPR. Ciò nonostante, nel rispetto dei principi di minimizzazione e di necessità, la scuola raccomanda comunque l'adozione di tecniche di pseudonimizzazione per la documentazione contenente dati sensibili, quale ulteriore misura di cautela.

L'analisi dei rischi condotta ha evidenziato che, a fronte delle misure tecniche e organizzative adottate e delle garanzie fornite dal fornitore in merito alla localizzazione dei dati, i rischi residui associati all'uso della piattaforma si collocano al di sotto di una soglia accettabile. La scuola si impegna a monitorare costantemente l'evoluzione normativa e tecnologica, nonché a rivedere periodicamente la presente valutazione al fine di garantire nel tempo l'adeguatezza delle misure adottate.

In conclusione, si ritiene che l'uso della piattaforma Microsoft 365 for Education da parte dell'istituto sia conforme alla normativa vigente in materia di protezione dei dati personali e garantisca un livello di sicurezza adeguato ai rischi connessi ai trattamenti operati.

Uso di Copilot (solo casi d'uso senza trattamento di dati personali)

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Contesto e finalità

La presente integrazione valuta l'impatto dell'introduzione di **Microsoft Copilot** nella piattaforma **Microsoft 365 Education** già adottata dall'Istituto.

L'analisi riguarda esclusivamente i casi d'uso che **non comportano il trattamento di dati personali**, come la generazione di materiali didattici generici, la revisione di testi anonimi o la creazione di documenti e presentazioni privi di riferimenti a persone fisiche identificate o identificabili.

Dati, Processi e Risorse di Supporto

- **Dati Trattati:** In questi specifici casi d'uso, i dati trattati **non sono dati personali**. Vengono trattate esclusivamente **informazioni generiche, prompt** (istruzioni di testo) per la generazione di contenuti, o documenti e materiali già pseudonimizzati/anonimizzati.
Esempio: Generazione di un piano di lezione su "L'Impero Romano", creazione di un quiz su "La fotosintesi clorofilliana".
- **Finalità del Trattamento:** Supporto alla didattica e alla pianificazione organizzativa ed amministrativa, riassunto e analisi di testi anonimi o di dominio pubblico. La base giuridica rimane l'esecuzione di un compito di interesse pubblico (supporto all'autonomia didattica e organizzativa).

Inquadramento dei servizi

Copilot è integrato in **Microsoft 365 Education**, piattaforma **qualificata ACN** per i servizi cloud SaaS e disciplinata dal *Data Protection Addendum* di Microsoft, che garantisce la conformità al GDPR e la localizzazione dei dati nell'Unione Europea.

I dati trattati da Copilot restano all'interno dei confini di Microsoft 365 Education: non vengono utilizzati per l'addestramento dei modelli di IA e non vengono condivisi con sistemi esterni o con l'ambiente consumer di Microsoft.

Copilot può pertanto essere utilizzato **in ambito scolastico e amministrativo**.

Ambito di utilizzo

L'ambito di utilizzo analizzato in questo documento è per finalità didattiche ed amministrative in assenza di dati personali (impiego di documenti anonimizzati o pseudonimizzati). Sono esclusi da tale analisi i casi d'uso che prevedono il caricamento e quindi il trattamento di dati personali e

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

quindi di documenti riferibili a studenti, genitori o personale scolastico, nonché file contenenti informazioni riservate o identificative.

Misure di sicurezza applicabili

Nella DPIA fatta per l'utilizzo della piattaforma Microsoft 365 for Education sono state individuate le seguenti **misure tecniche ed organizzative atte a garantire la sicurezza dei trattamenti operati**:

- nomina di Microsoft a responsabile del trattamento
- nomina di un amministratore della piattaforma
- autenticazione con credenziali istituzionali
- logging degli accessi
- informativa aggiornata
- formazione del personale e degli alunni
- regolamento per l'uso della piattaforma

Di seguito si valuta l'idoneità di tali misure a soddisfare i requisiti di sicurezza necessari per l'utilizzo controllato di Copilot e la necessità di adottarne di nuove.

Valutazione dei Rischi per l'Uso "Data-Free"

La valutazione del rischio si concentra sul pericolo residuo legato all'uso di questi strumenti, anche in assenza di dati personali.

Rischio 1: Accesso Illegittimo o Modifica Indesiderata dei Dati Personali

- **Fonte del Rischio:** L'unico rischio è che l'utente (docente o studente) carichi accidentalmente dati personali, anche di natura sensibile, su Copilot contravvenendo alle disposizioni impartite dall'istituto.
- **Misure di Mitigazione Adottate:**
 - **Formazione del Personale:** Il personale deve essere formato sul principio di minimizzazione dei dati e sull'uso corretto della piattaforma.
 - **Autorizzazione dei Docenti:** Verrà emessa una circolare specifica che **proibirà** l'uso di Copilot per documenti contenenti dati personali.
 - **Minimizzazione dei Dati Personali:** ove fosse necessario riportare riferimenti a dati personali dovranno essere adottate tecniche di pseudonimizzazione.

Liceo Statale "C. Lorenzini"

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

- **Stima Gravità del Danno (Danno residuo, in caso di errore umano): Importante (Livello 3).** L'errore umano che porta a caricare dati sensibili è grave.
- **Stima Probabilità del Rischio: Trascurabile (Livello 1).** Data l'adozione di un robusto corpo documentale, informative e formazione, la probabilità di uso non conforme è ridotta al minimo.
- **Gravità del Rischio Residuale:** $3 \times 1 = 3$ (Valore Massimo 16).

Rischio 2: Perdita di Dati (Contenuti Generati/Analizzati)

- **Fonte del Rischio:** Il contenuto generato dall'IA (es. un riassunto di un testo didattico) non è un atto amministrativo essenziale e non è coperto dalle politiche di conservazione del fornitore alla pari dei documenti istituzionali.
- **Misure di Mitigazione Adottate:** La DPIA stabilisce che la documentazione ottenuta dall'attività didattica verrà archiviata dal docente al termine dell'attività.
- **Stima Gravità del Danno: Limitata (Livello 2).** La perdita di un *prompt*, di una bozza di riassunto o del materiale didattico sviluppato da un docente non compromette la missione istituzionale.
- **Stima Probabilità del Rischio: Trascurabile (Livello 1).**
- **Gravità del Rischio Residuale:** $2 \times 1 = 2$ (Valore Massimo 16).

3. Conclusioni e Mitigazione Aggiuntiva

Rischio	Entità del Danno	Probabilità	Gravità del Rischio	Rischio Accettabile?
Accesso Illegittimo/Modifica Dati Personali (Errore d'Uso)	3 (Importante)	1 (Trascurabile)	3	Sì
Perdita di Dati Generati	2 (Limitata)	1 (Trascurabile)	2	Sì

Liceo Statale “C. Lorenzini”

Classico, Linguistico, Scientifico Ord. e Opz. Scienze Applicate, Scienze Umane

Conclusione

L'uso di **Copilot** all'interno della piattaforma **Microsoft 365 Education** non modifica in modo significativo l'impatto complessivo sul rischio già valutato nella DPIA principale.

L'adozione dello strumento è **ammissibile** nei casi d'uso che non prevedono trattamento di dati personali, a condizione che:

- l'utilizzo avvenga esclusivamente tramite **account istituzionali Microsoft 365 Education**;
- siano rispettate le **configurazioni di sicurezza standard Education** (no training sui dati);
- venga ribadito il **divieto di uso per atti amministrativi o documenti contenenti dati personali**;
- si effettui un **monitoraggio periodico** e si aggiorni la formazione del personale.

In conclusione, il livello di rischio residuo associato all'impiego di **Copilot** in casi d'uso che escludono il trattamento di dati personali è **trascurabile** e al di sotto della soglia di accettabilità. L'uso è dunque ammesso per scopi didattici e di supporto organizzativo privi di dati personali, all'interno dell'ambiente **Microsoft 365 Education qualificato ACN**.

Autore: Ing. Raffaella Mambrini – DS IM Lorenzini di Pescia (PT)

Validatore: Ing. Antonio Vargiu - DPO IM Lorenzini di Pescia (PT)

La Dirigente Scolastica

Dott.ssa Raffaella Mambrini

Documento firmato digitalmente ai sensi del Codice
dell'Amministrazione digitale e norme ad esso connesse