LICEO ARTISTICO STATALE FAUSTO MELOTTI
**SEDE CENTRALE:** Via Andina 8 – 22063 Cantù (CO) Tel. 031.714100 Fax. 031704747
**SEDE STACCATA:** Via Pitagora 15 –22074 Lomazzo (CO) tel. 02.96779256 Fax 02.96779572
**C.F.** 81003890134 – **Cod. Univoco Fatt. Elettr.** UFXGI6 –**COD. MIN.** COSD02000R
**SITO INTERNET:** www.liceoartisticomelotti.edu.it
**E- MAIL:** cosd02000r@istruzione.it - cosd02000r@pec.istruzione.it

# DPIA/TIA per l'adozione della piattaforma Google Workspace for Education nello svolgimento delle attività didattiche ed amministrative

**Autore:** Arch. Anna Proserpio **Validatore:** Ing. Antonio Vargiu

**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 Google Workspace for Education nello svolgimento delle attività svolte dall'amministrazione scolastica. Il documento analizza in modo distinto 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 le seguenti attività: scambio di informazioni fra gli studenti ed i docenti mediante caselle email istituzionali realizzate nel dominio della scuola; scambio di documenti e materiale didattico fra studenti e docenti con Google Drive; videocomunicazioni mediante Google Meet per lezioni a distanza e attività di recupero; gestione delle classi virtuali attraverso Google Classroom; produzione collaborativa di documenti, presentazioni e fogli di calcolo. Tali attività possono essere svolte sia da scuola che da casa, garantendo continuità didattica in qualsiasi circostanza.

### Ambito amministrativo e organizzativo

La medesima piattaforma Google Workspace for Education viene utilizzata per favorire la comunicazione e la collaborazione fra le varie componenti scolastiche per finalità organizzative ed amministrative. In particolare, si fa uso di sistemi di videocomunicazione per le riunioni degli organi collegiali (Collegio Docenti, Consigli di Classe, Consiglio d'Istituto), per le commissioni di lavoro e per i gruppi operativi. La posta elettronica istituzionale viene

utilizzata per le comunicazioni interne e per lo scambio di documentazione amministrativa. Gli strumenti di condivisione documenti e risorse vengono impiegati per la redazione collaborativa di verbali, relazioni e altri atti amministrativi.

**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, nonché 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 contenuti o gratuità per le istituzioni scolastiche.

**Perché questa DPIA?**

A seguito delle disposizioni contenute nei decreti che hanno disposto, per tutta la durata della sospensione delle attività didattiche "in presenza" nelle scuole a causa della diffusione di Covid 19, l'attivazione di modalità di didattica a distanza, la scuola ha approvato l'uso della piattaforma Google Workspace for Education.

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 - ACN), condizione prevista come necessaria all'adozione di piattaforme cloud da parte della pubblica amministrazione.

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 è anni che 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 ed il passaggio al cloud è 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 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 "Learn 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.

L'uso di ambienti digitali è oggi richiesto anche per l'adozione dei nuovi strumenti di intelligenza artificiale finalizzata a garantire l'efficacia e l'efficienza delle attività istituzionali delle pubbliche amministrazioni.

**È 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 2020, 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 (EDPB)** 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'EDPB 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** che dispone che le Pubbliche Amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati da AGID (oggi attività demandata all'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.

## Dati, processi e risorse di supporto

### Quali sono i dati trattati?

#### Dati trattati in ambito didattico

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.

### 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 e per il personale delle utenze istituzionali sulla piattaforma cloud che dovranno essere utilizzate, con dispositivi di proprietà della scuola o personali, per lo svolgimento delle attività istituzionali.

Durante le attività didattiche tali servizi saranno utilizzati per affidare agli studenti dei compiti, da svolgere in classe o da casa, che prevedono la comunicazione e la produzione di materiale. Tale materiale verrà conservato in cloud sulla piattaforma Google Workspace e condiviso secondo le regole stabilite dal docente. 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.

Per quanto riguarda le attività amministrative, la documentazione prodotta (verbali, relazioni, comunicazioni) seguirà un ciclo di vita che prevede la creazione, eventualmente collaborativa, la condivisione con i soggetti interessati, l'approvazione e l'archiviazione secondo le procedure previste dalla normativa vigente in materia di conservazione documentale.

Per quanto riguarda lo scarto dei documenti dalla piattaforma Google Workspace, questo dovrà rispettare le disposizioni presenti nel massimario di classificazione e scarto approvato dall'istituto. Si evidenzia che per quanto riguarda la conservazione di elaborati delle prove scritte, grafiche e pratiche il massimario di scarto, in conformità con la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi, dispone 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 Google Workspace 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.

Tuttavia, in ottemperanza alle direttive del Ministero dell'Istruzione e del Merito sul divieto di utilizzo dei telefoni cellulari a scuola (con particolare riferimento alla Circolare Ministeriale prot. n. 5274 dell'11 luglio 2024 e alle relative disposizioni applicative estese al secondo ciclo di istruzione), l'accesso alla piattaforma Google Workspace tramite dispositivi mobili personali (*smartphone*) è severamente vietato a tutti gli studenti durante l'orario scolastico nei locali dell'Istituto. Di conseguenza, nell'ambito delle attività didattiche in aula o nei laboratori del Liceo, la fruizione dei servizi della suite (es. Google Classroom, Google Drive, Documenti, Fogli, Presentazioni) avviene esclusivamente mediante l'impiego di dispositivi informatici idonei forniti dall'Istituto (quali PC di aula/laboratorio, tablet d'Istituto) sottoposti alla supervisione del docente. L'uso di dispositivi mobili personali resta consentito esclusivamente nei casi inderogabili previsti dalla normativa vigente (supporto ad alunni con disabilità o DSA formalizzato nei rispettivi PEI/PDP). L'accesso alla piattaforma tramite *smartphone* da parte degli studenti è pertanto confinato all'ambito domestico, per lo svolgimento di compiti a casa, la consultazione di materiali didattici e lo studio asincrono. Tale vincolo organizzativo rappresenta una formale misura di mitigazione del rischio per la protezione dei dati personali, riducendo l'esposizione del sistema scolastico a vulnerabilità derivanti dall'uso in rete di dispositivi *BYOD* non gestiti e non monitorabili.

# Trasferimento dati extra UE

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

Sì. Google Workspace for Education, nella versione Fundamentals adottata dalla scuola, non prevede la funzionalità di Data Residency (disponibile solo nella versione Education Plus a pagamento). Questo significa che, sebbene Google abbia datacenter collocati in Europa dove normalmente risiedono i dati per i clienti europei, non si può escludere che dati e documenti possano essere trasferiti o archiviati in datacenter al di fuori dell'UE. Si rileva inoltre che dati personali sono comunque trasferiti fuori dall'UE per la fornitura dei servizi in transito nei sistemi o in forma di dati di telemetria.

**Quale è la classificazione dei dati trattati dall'istituzione scolastica ai fini della normativa cloud?**

È fondamentale premettere che, ai sensi della normativa vigente in materia di qualificazione dei servizi cloud per la pubblica amministrazione, i dati trattati dalle istituzioni scolastiche sono classificati come **dati ordinari**. Tale classificazione è rilevante ai fini della presente valutazione poiché i dati delle pubbliche amministrazioni, ai fini dell'adozione di servizi cloud, sono distinti in tre categorie: dati ordinari, dati critici e dati strategici.

I dati delle istituzioni scolastiche, non rientrando tra quelli la cui compromissione può determinare un pregiudizio per la sicurezza nazionale o per il mantenimento delle funzioni essenziali dello Stato, né tra quelli la cui compromissione può determinare un pregiudizio per la sicurezza pubblica o per la continuità di servizi essenziali, sono correttamente classificati come ordinari.

**Conseguenza di tale classificazione è che l'assenza della funzionalità Data Residency sulla piattaforma Google Workspace for Education non costituisce, di per sé, un impedimento assoluto all'uso della piattaforma da parte dell'istituzione scolastica.** La piattaforma, infatti, risulta regolarmente certificata dall'Agenzia per la Cybersicurezza Nazionale (ACN) e inserita nel Cloud Marketplace, attestazione che ne conferma l'idoneità all'utilizzo da parte delle pubbliche amministrazioni per il trattamento di dati ordinari.

**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 Google, 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 Google avviene sulla base di una dichiarazione di adeguatezza (art. 45 GDPR). Ciò detto, anche le condizioni contrattuali prevedono delle specifiche condizioni di sicurezza. In particolare i trattamenti operati da Google sono regolamentati dal Cloud Data Processing Addendum (CDPA) dove, oltre ad attestare la conformità ed il rispetto delle disposizioni del GDPR, viene dichiarato all'articolo 10 che nel caso in cui il trasferimento di dati personali avvenga verso un paese non coperto da una decisione di adeguatezza, allo stesso si applicano le clausole contrattuali tipo, previste dall'articolo 46 GDPR.

La valutazione concreta dell'effettivo rispetto del GDPR nei trattamenti operati sulla piattaforma Google 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 Google.

**Quali sono le implicazioni dell'assenza di Data Residency per i diversi tipi di dati?**

**Dati personali comuni**

Per quanto riguarda i **dati personali comuni** (dati identificativi, dati di contatto, dati relativi all'attività didattica ordinaria, comunicazioni istituzionali, documenti amministrativi privi di dati particolari), l'uso delle applicazioni principali e dei servizi aggiuntivi di Google Workspace for Education è **pienamente consentito**, sia in ambito didattico che amministrativo. La certificazione ACN della piattaforma, unitamente all'adeguatezza riconosciuta dal Data Privacy Framework per i trasferimenti verso gli Stati Uniti, garantisce un livello di protezione adeguato per questa tipologia di dati, conforme ai requisiti del GDPR.

**Dati particolari (ex dati sensibili)**

Per quanto riguarda i **dati particolari** ai sensi dell'art. 9 del GDPR (dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale), l'assenza di Data Residency richiede una valutazione più attenta.

Il GDPR impone infatti che il trattamento dei dati personali garantisca un livello di sicurezza adeguato al rischio, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Nel caso dei dati particolari, il rischio intrinseco è maggiore e pertanto il livello di sicurezza richiesto è proporzionalmente più elevato.

L'impossibilità di garantire con certezza che i dati particolari restino archiviati esclusivamente su datacenter situati nel territorio dell'Unione Europea introduce un elemento di incertezza che deve essere valutato caso per caso. È necessario infatti bilanciare: la natura e la sensibilità dei dati trattati; il contesto del trattamento e le finalità perseguite; le misure di sicurezza tecniche e organizzative adottate; il rischio residuo per i diritti e le libertà degli interessati.

**In considerazione di quanto sopra esposto, il trattamento di dati particolari sulla piattaforma Google Workspace for Education non viene proibito in modo assoluto, ma viene subordinato a valutazioni specifiche caso per caso.** In particolare, per ogni trattamento di dati particolari sulla piattaforma, dovrà essere verificata: la stretta necessità del dato particolare per il conseguimento della finalità; l'impossibilità o l'eccessiva onerosità di utilizzare strumenti alternativi che garantiscano la residenza dei dati in Europa; l'adozione di misure supplementari di protezione (quali la pseudonimizzazione); l'adeguatezza delle misure rispetto al rischio specifico.

**Il trasferimento è necessario per importanti motivi di interesse pubblico?**

Sì. La base giuridica del trasferimento dei dati all'estero è 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 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.

**È 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 Google Workspace for Education 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.

**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).

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;
- corretta attribuzione dei ruoli con adozione di misure organizzative tali da garantire concretamente la gestione del rischio attraverso l'individuazione di specifici ruoli e responsabilità;
- valutazione dei dati da trattare 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 limitando l'uso delle applicazioni;
- tecniche di anonimizzazione e pseudonimizzazione per garantire adeguati livelli di protezione;
- definizione di regolamenti e disposizioni specifiche per l'uso delle piattaforme formando un coerente corpo documentale con informative, disciplinari e regolamenti.

**È 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 risvolti in termini di violazione dei Dati Personali implica 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. Google è stata verificata come inserita nel Cloud Marketplace gestito dall'Agenzia per la Cybersicurezza Nazionale nell'elenco SaaS.
- **Amministratore della piattaforma Google**: 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 Google.

**È 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

- cognome.nome@liceoartisticomelotti.edu.it per studenti e personale ATA
- nome.cognome@liceoartisticomelotti.edu.it per docenti

È stata disabilitata la possibilità di aggiungere ulteriori informazioni da parte dell'utente proprietario del profilo quali telefono, email alternative e foto.

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. 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. Per ogni specifico trattamento di dati particolari che non possa essere effettuato in forma criptata o pseudonimizzata, dovrà 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 rischio specifico.

**È stato applicato un principio di minimizzazione anche in relazione alle applicazioni utilizzate?**

Sì. Nella scelta dei servizi e delle applicazioni da utilizzare si sono tenuti presenti i principi di necessità e di minimizzazione per ridurre i possibili rischi associati al loro uso. La scuola ha attivato i servizi principali di Google Workspace for Education, ossia: caselle di posta elettronica (Gmail); sistema di videoconferenza (Meet); Documenti, Fogli di calcolo e Presentazioni; Classroom per la gestione delle lezioni e dei compiti; spazio di archiviazione condivisa (Drive); Calendar per la condivisione di impegni e appuntamenti. Per quanto riguarda le applicazioni di terze parti disponibili nel marketplace di Google, la loro attivazione sarà valutata caso per caso, tenendo conto dell'effettiva necessità per il conseguimento delle finalità didattiche o amministrative e dei rischi associati al loro uso, con particolare riferimento ai trattamenti di dati personali operati da tali applicazioni. All'esito positivo di tali valutazioni, l'uso delle applicazioni di terze parti avrà ancora come base legale l'esecuzione di un compito di interesse pubblico di cui è investita la scuola ai sensi dell'art. 6 comma 1 lettera e del GDPR.

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

Come detto più sopra, sono state adottate tecniche di pseudonimizzazione per la protezione dei dati sensibili, in particolare per la redazione dei PEI e PDP. Si è anche presa in considerazione l'opportunità di procedere alla pseudonimizzazione dei dati personali identificativi caricati sulla piattaforma, valutando la possibilità di caricare nella piattaforma non il nome e cognome dell'utente ma il codice di pseudonimizzazione ad esso associato, individuato nel codice SIDI (identificativo unico assegnato dal Sistema Informativo dell'Istruzione del Ministero dell'Istruzione e del Merito (MIM) a ciascun studente iscritto nell'Anagrafe Nazionale degli Alunni). Tuttavia, adottando tale soluzione la casella associata all'utente non sarebbe più cognome.nome@liceoartisticomelotti.edu.it ma codiceSIDI@liceoartisticomelotti.edu.it . In tal modo si complicherebbe notevolmente la gestione della piattaforma e diventerebbe complessa la comunicazione email, fatto che comporta un sensibile aumento del rischio di errori che possono condurre anche a rilevanti violazioni dei dati personali. **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.**

**È 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.

# 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.

Gli stessi strumenti adottati per condurre l'attività didattico/formativa vengono 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. 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 sensibili) che dovranno essere trattati solo se strettamente necessari, e comunque utilizzando degli strumenti di minimizzazione e protezione dei dati (ad es. pseudonimizzazione).

**I dati sono esatti e aggiornati?**

Sì. 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.

## 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.

Per i dati ed elaborati non soggetti a valutazione, la cancellazione avviene di norma alla fine dell'anno scolastico. Per i dati ed elaborati soggetti a valutazione, il periodo di conservazione deve rispettare le disposizioni previste dalla legge fra cui la Circolare n°44 del 19/12/2005 della Direzione Generale degli archivi.

**Politica di sospensione, archiviazione e cancellazione degli account utente**

Al fine di garantire la corretta gestione del ciclo di vita delle identità digitali create sulla piattaforma Google Workspace for Education (relative a docenti, studenti e personale ATA), l'istituto applica la seguente politica:

- Sospensione dell'account: al termine del ciclo delle attività didattiche, lavorative o del percorso di studi presso l'istituto, l'account dell'utente viene tempestivamente disattivato/sospeso, inibendo l'accesso ai servizi e alla casella di posta elettronica.

- Archiviazione dei dati: decorsi due anni dalla data di sospensione dell'account, l'account e tutti i dati ad esso associati vengono messi in stato di archiviazione.

Eliminazione definitiva: trascorsi cinque anni dalla sospensione, l'account e tutti i contenuti digitali correlati inseriti nell'ambiente cloud vengono eliminati in modo definitivo ed irreversibile.

- Trasferimento dati a un account personale: al termine del ciclo delle attività didattiche, lavorative o del percorso di studi presso l'istituto, l'utente (docente, studente, personale ATA) ha la possibilità di richiedere il trasferimento dei propri dati dall'account istituzionale a un account personale. Per formalizzare tale richiesta è stato predisposto un documento specifico allegato alla presente DPIA.

**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 206/679. 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 condividerne 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.

**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 l'esercizio degli stessi.

## 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.

## 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.

In merito, si rimanda all'allegato del presente documento.

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

I trattamenti operati da Google sono regolamentati dal Cloud Data Processing Addendum (CDPA) dove sono specificati gli obblighi del fornitore individuato responsabile del trattamento. 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 per la Cybersicurezza Nazionale nell'elenco SaaS.

# 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. Cifratura client side potrà essere adottata per la protezione di documenti sensibili.

### Controllo degli accessi logici

L'accesso alle funzionalità delle piattaforme utilizzate è regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software.

### 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 e, in considerazione dell'assenza di Data Residency, vengono preferibilmente trattati in forma cifrata o pseudonimizzata.

### Lotta contro il malware

I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus). Sono state fornite agli utilizzatori delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali.

### Backup

Sebbene il fornitore debba predisporre le soluzioni tecniche atte a garantire la reperibilità e l'integrità dei dati caricati sulla piattaforma, la scuola valuta ulteriori misure di salvaguardia dei dati e dei documenti più importanti.

### Manutenzione

Viene effettuata regolarmente un'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 Google sono regolamentati dal Cloud Data Processing Addendum (CDPA) 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.

**Gestione degli incidenti di sicurezza e delle 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. È stata 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.

In merito, si rimanda all'allegato del presente documento.

**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
- Perdita di dati

Prima di valutare l'entità 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 **Importante** (livello 3 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 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 **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: 3x2=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 sono:

- 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 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: 2x1=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:

- 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 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 di dati: 2x1=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, il Liceo Fausto Melotti conferma l'adozione della piattaforma Google Workspace 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 reale, la videocomunicazione integrata e la gestione delle classi virtuali. Per tali esigenze si rende necessario l'utilizzo della piattaforma Google Workspace 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. Tale classificazione, unitamente alla certificazione ACN della piattaforma Google Workspace e all'adeguatezza riconosciuta dal Data Privacy Framework per i trasferimenti di dati verso gli Stati Uniti, consente di ritenere che l'assenza della funzionalità Data Residency non costituisca un impedimento all'utilizzo della piattaforma per il trattamento dei dati personali comuni, sia in ambito didattico che amministrativo.

Per quanto riguarda i dati particolari ai sensi dell'art. 9 del GDPR, il loro trattamento sulla piattaforma non è proibito in modo assoluto ma è subordinato a valutazioni specifiche caso per caso. In tali circostanze dovrà essere prioritariamente valutata l’adozione di tecniche di cifratura o pseudonimizzazione, se possibile, e dovrà essere verificata l'adeguatezza delle misure di protezione rispetto al rischio specifico connesso alla natura dei dati trattati.

L'analisi dei rischi condotta ha evidenziato che, a fronte delle misure tecniche e organizzative adottate, 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 Google Workspace 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.

Il Dirigente Scolastico

Arch. Anna Proserpio