LINEE GUIDA PER L'UTILIZZO SICURO DELLE PIATTAFORME CLOUD DI DIDATTICA DIGITALE

Articolo 1 – Introduzione e ambito

Le presenti linee guida forniscono al personale dell'Istituto le istruzioni per l'utilizzo sicuro delle piattaforme cloud a supporto della didattica digitale, quali Google Workspace for Education o Microsoft 365 Education. Esse costituiscono l'allegato tecnico della circolare sulle istruzioni operative per l'uso della piattaforma e integrano, per quanto compatibili, le linee guida in materia di sicurezza allegate alle determine di costituzione delle unità organizzative. L'utilizzo delle piattaforme cloud avviene nell'esecuzione di compiti di interesse pubblico e deve svolgersi in modo da prevenire ogni rischio per la sicurezza dei dati personali di studenti, famiglie e personale.

Articolo 2 – Registrazione e accesso

Al momento della registrazione, l'amministratore della piattaforma crea un profilo con il nome e cognome dell'utente, cui associa una casella di posta elettronica istituzionale. Nessun altro dato personale viene caricato sulla piattaforma e l'utente è tenuto a non aggiungere al proprio profilo ulteriori dati, quali indirizzo di residenza, numero di telefono, posta elettronica personale o fotografia.

L'accesso alle applicazioni e ai servizi avviene mediante le credenziali istituzionali, personali e non cedibili. È vietato condividere le credenziali o l'account con altre persone, compresi i colleghi, gli studenti o i familiari. In particolare:

- ove l'Istituto abbia attivato l'**autenticazione a più fattori (MFA)**, il suo utilizzo è obbligatorio e non può essere disattivato;
- è raccomandato, ove disponibile, l'accesso mediante identità digitale (**SPID o CIE**), secondo il processo di migrazione avviato dall'Istituto;
- al termine della sessione di lavoro occorre effettuare sempre la disconnessione, in particolare da dispositivi condivisi.

Articolo 3 – Uso di altre applicazioni

Il personale utilizza esclusivamente la piattaforma e le applicazioni autorizzate dall'Istituto. Le richieste di adozione di nuove applicazioni o componenti aggiuntivi vanno indirizzate all'amministratore di piattaforma, che ne valuta i profili di sicurezza e di protezione dei dati; l'attivazione è disposta previa autorizzazione del Dirigente Scolastico. È vietato proporre agli studenti l'uso di servizi o applicazioni non previamente autorizzati.

Articolo 4 – Protezione dei dati personali e minimizzazione

Il personale rispetta rigorosamente la normativa in materia di protezione dei dati personali. È vietato raccogliere, utilizzare o comunicare dati personali degli studenti al di fuori di quanto necessario alle finalità istituzionali e delle istruzioni ricevute. Nell'uso della piattaforma ciascun utente applica il principio di **minimizzazione**, in modo che i dati personali non siano presenti se non necessari.

Il principio di minimizzazione va applicato in modo particolarmente rigoroso alle **categorie particolari di dati** di cui all'art. 9 del Regolamento — dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici e biometrici, i dati relativi alla salute o alla vita sessuale. I docenti tengono presenti tali principi anche nell'assegnazione di attività e compiti agli alunni, che, ove possibile, non devono comportare la rilevazione di dati personali e in particolare di categorie particolari.

Articolo 5 – Trattamenti esclusi

Non possono essere caricati sulla piattaforma, salvo diversa e motivata disposizione del Dirigente Scolastico, i **Piani Educativi Individualizzati e la documentazione relativa alla disabilità e ai bisogni educativi speciali**, per i quali l'Istituto si avvale della partizione separata dell'Anagrafe Nazionale Studenti, che garantisce la gestione granulare degli accessi e la tracciabilità delle operazioni. Il trattamento di altre categorie particolari di dati sulla piattaforma è ammesso nei soli limiti di cui agli articoli 4 e 13.

Articolo 6 – Condivisione di contenuti

Il personale è responsabile dei contenuti condivisi sulla piattaforma. Prima della condivisione occorre verificarne la correttezza e circoscrivere i destinatari a quelli effettivamente legittimati, privilegiando la condivisione nominativa rispetto ai collegamenti aperti. È vietata la condivisione di contenuti offensivi, discriminatori o illeciti, nonché di contenuti protetti dal diritto d'autore in assenza dell'autorizzazione del titolare.

Articolo 7 – Strumenti di intelligenza artificiale

Possono essere utilizzati per il trattamento di dati personali i soli strumenti di intelligenza artificiale integrati nella piattaforma istituzionale e attivati dall'Istituto, previa integrazione della valutazione d'impatto. È vietato inserire nei prompt dati personali di studenti, famiglie o dipendenti dell'amministrazione a meno che tale attività non sia inclusa esplicitamente nei casi d'uso ammessi. I contenuti prodotti con tali strumenti sono sempre sottoposti a validazione umana prima di ogni utilizzo, restando la responsabilità dell'atto in capo a chi lo adotta.

Articolo 8 – Sicurezza

Il personale utilizza la piattaforma in modo sicuro e responsabile. A tal fine non installa né utilizza software non autorizzati o non sicuri, mantiene costantemente aggiornati i propri dispositivi con gli ultimi aggiornamenti di sicurezza ed evita l'accesso da reti pubbliche non attendibili.

Articolo 9 – Utilizzo corretto delle risorse

La piattaforma è utilizzata esclusivamente per finalità didattiche e istituzionali. Non ne è consentito l'uso per attività personali o commerciali, per la pubblicità, per la propaganda politica o per qualunque altra attività inappropriata o contraria alle leggi applicabili e ai regolamenti dell'Istituto.

Articolo 10 – Archiviazione e conservazione dei dati

I dati archiviati sulla piattaforma devono essere protetti da accessi non autorizzati, perdite o danneggiamenti. I file contenenti dati personali vanno salvati in aree ad accesso limitato ai soli soggetti autorizzati. Questo accorgimento va adottato in modo particolarmente rigoroso per le categorie particolari di dati, valutando altresì il ricorso a tecniche di pseudonimizzazione (art. 13).

Occorre tenere sotto controllo lo spazio di archiviazione e cancellare periodicamente i dati non più necessari. Al termine dell'anno scolastico sono cancellati, ed eventualmente riconsegnati agli studenti, i documenti e gli elaborati prodotti nel corso dell'anno, a eccezione di quelli soggetti a un periodo di conservazione più lungo. I tempi di conservazione sono quelli stabiliti dal piano di conservazione e dal massimario di scarto degli archivi delle istituzioni scolastiche; per gli elaborati sottoposti a valutazione resta fermo l'obbligo di conservazione secondo le regole di gestione documentale vigenti.

Articolo 11 – Accesso ai dati

L’accesso ai dati degli studenti è limitato ai soli soggetti autorizzati che ne necessitano per lo svolgimento delle proprie funzioni. In caso di dubbio sulla legittimità di un determinato trattamento, il personale contatta il Dirigente Scolastico o il Responsabile della Protezione dei Dati.

Articolo 12 – Sicurezza delle password

Le password devono essere robuste e complesse, uniche e non riutilizzate su altre piattaforme o servizi. La sostituzione della password è richiesta senza indugio in caso di sospetta compromissione; non è invece prevista una rotazione periodica obbligatoria a scadenza fissa, che le linee guida attuali sconsigliano in quanto tende a produrre password più deboli e prevedibili.

Articolo 13 – Misure di protezione rafforzata per i dati di cui all'art. 9: pseudonimizzazione e cifratura

Le categorie particolari di dati possono essere caricate sulla piattaforma solo se strettamente necessarie e in assenza di valide soluzioni alternative. Per garantire un adeguato livello di sicurezza si dovrà valutare l’adozione delle misure tecniche rafforzate di seguito indicate, secondo quanto previsto dall'art. 32 del Regolamento.

La **pseudonimizzazione** consiste nel sostituire i dati identificativi dell'interessato (quali nome e cognome) con un codice che non consente l'identificazione senza il ricorso a ulteriori informazioni, le quali vanno conservate separatamente e in modo protetto. Essa va applicata a tutte le categorie particolari di dati oggetto di trattamento, compresi i dati relativi alla salute degli studenti e del personale, ogni volta che la finalità perseguita può essere raggiunta senza il collegamento diretto ai dati identificativi.

La **cifratura** (o criptazione) rende i dati intelligibili ai soli soggetti in possesso della chiave, proteggendoli anche in caso di accesso non autorizzato o di sottrazione del supporto. I file contenenti categorie particolari di dati che debbano essere conservati sulla piattaforma o trasmessi vanno cifrati, avendo cura di custodire le chiavi separatamente dai dati e di non trasmetterle attraverso il medesimo canale. La cifratura è raccomandata in particolare per i documenti relativi alla salute e per ogni file che, per la delicatezza del contenuto, esporrebbe l'interessato a un rischio elevato in caso di violazione.

Le due misure sono complementari e, ove possibile, vanno adottate congiuntamente; la loro applicazione non esime dal rispetto del principio di minimizzazione, che resta il primo presidio: il dato particolare non necessario non va trattato affatto.

Articolo 14 – Sicurezza del dispositivo

Il personale accede alla piattaforma solo da dispositivi sicuri e aggiornati. I dispositivi personali non devono essere utilizzati per il trattamento di categorie particolari di dati degli studenti, salvo che siano adeguatamente protetti da credenziali robuste e da software di sicurezza aggiornato, secondo le eventuali indicazioni dell’Istituto in materia di uso di dispositivi personali.

Articolo 15 – Ciclo di vita dell’account

Al termine del rapporto di servizio l’account è disattivato dall’amministratore di piattaforma secondo la procedura adottata dall’Istituto. Prima della disattivazione, i documenti di rilievo istituzionale presenti negli spazi personali dell’utente devono essere trasferiti negli spazi condivisi di competenza, non potendo restare nella disponibilità personale dell’interessato né andare dispersi.

Articolo 16 – Gestione delle violazioni dei dati personali

Qualunque violazione dei dati personali — accesso non autorizzato, perdita, divulgazione accidentale, smarrimento di dispositivi, condivisione errata di documenti — o anche il semplice

sospetto di essa deve essere segnalata **senza ritardo al Dirigente Scolastico e, per il suo tramite, al Responsabile della Protezione dei Dati**, al fine di consentire gli adempimenti previsti dagli artt. 33 e 34 del Regolamento, che impongono termini stringenti. La segnalazione va effettuata anche quando l'evento appaia di modesta entità o sia stato già risolto, e non deve essere preceduta da valutazioni autonome sulla gravità. Contestualmente può essere informato l'amministratore di piattaforma per gli interventi tecnici urgenti.

Il personale coopera pienamente con ogni indagine, interna o esterna, relativa alle violazioni dei dati o del presente documento. L'inosservanza delle presenti disposizioni può dar luogo a responsabilità disciplinare secondo la normativa e la contrattazione collettiva vigenti, in proporzione alla gravità della violazione.

Il Dirigente Scolastico
Prof. Nicola Iavarone
Firma autografa sostituita a mezzo stampa
ai sensi e per gli effetti dell'art.3, C.2 D.lgs
n. 39/1993