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

Articolo 1: Introduzione

Le presenti linee guida sono finalizzate a fornire istruzioni al personale della scuola sull'utilizzo sicuro delle piattaforme cloud didattica digitale, come Google Workspace for Education o Office 365 Education. L'utilizzo delle piattaforme cloud è essenziale per garantire un'esperienza di apprendimento online e digitale, ma è altrettanto importante prevenire qualsiasi rischio per la sicurezza dei dati personali degli studenti.

Articolo 2: Registrazione e Accesso

Al momento della registrazione l'amministratore della piattaforma cloud aprirà un profilo con il nome e cognome dell'utente cui verrà associato una casella email istituzionale. Nessun altro dato personale verrà caricato sulla piattaforma e l'utente stesso è invitato a non aggiungere nel proprio profilo altri dati personali quali indirizzo di residenza, numero di telefono, email personale o foto. L'accesso alle applicazioni ed ai servizi della piattaforma avverrà per mezzo dell'indirizzo email istituzionale e la digitazione della relativa password di accesso. È vietato condividere le credenziali di accesso o l'account con altre persone, incluso il personale della scuola o gli studenti.

Articolo 3: Uso di altre applicazioni

Il personale è tenuto ad utilizzare esclusivamente la piattaforma cloud e le applicazioni autorizzate dalla scuola. Ove i docenti volessero adottare nuove applicazioni dovranno sottoporle all'approvazione del dirigente scolastico che dovrà valutarne il grado di sicurezza.

Articolo 4: Protezione dei Dati Personali

Il personale della scuola è tenuto a rispettare rigorosamente la normativa sulla privacy e sulla protezione dei dati personali degli studenti, in linea con la base legale del trattamento prevista per l'esecuzione del pubblico servizio. Pertanto, è vietato raccogliere, utilizzare o divulgare qualsiasi informazione personale degli studenti senza il rispetto delle norme di legge e senza la supervisione del responsabile della privacy della scuola. Nell'uso della piattaforma ciascun utente deve adottare un principio di minimizzazione dei dati personali in modo che questi non siano presenti se non necessari. Tale principio di minimizzazione deve essere adottato in modo particolarmente stringente e rigoroso per i dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale (dati sensibili). I docenti dovranno tenere presenti tali principi anche nell'assegnazione delle attività e dei compiti agli alunni che, ove possibile, non dovranno rilevare dati personali ed in particolare sensibili.

Articolo 5: Condivisione di contenuti

Il personale della scuola è responsabile dei contenuti condivisi su piattaforme cloud di supporto alla didattica. Pertanto, si richiede al personale di verificare accuratamente la correttezza e l'accuratezza dei contenuti prima di condividerli e di evitare la condivisione di contenuti offensivi, discriminatori o illegali. Inoltre, è vietato utilizzare le piattaforme cloud per la condivisione di contenuti protetti da copyright o di proprietà intellettuale senza l'autorizzazione esplicita del proprietario.

Articolo 6: Sicurezza

Il personale della scuola deve utilizzare le applicazioni e le piattaforme cloud di supporto alla didattica in modo sicuro e responsabile, garantendo la protezione dei dati personali propri e degli studenti che dovranno essere quelli minimi necessari per lo svolgimento delle attività programmate. Pertanto, si richiede al personale di non installare o utilizzare software non autorizzati o non sicuri e di mantenere costantemente aggiornati i propri dispositivi con gli ultimi aggiornamenti di sicurezza. Inoltre, è vietato accedere alle piattaforme cloud da reti pubbliche non sicure.

Articolo 7: Utilizzo corretto delle risorse

Il personale della scuola è tenuto a utilizzare le piattaforme cloud di supporto alla didattica solo per scopi accademici e didattici. L'uso delle piattaforme cloud per attività personali o commerciali non è consentito. Inoltre, è vietato utilizzare le piattaforme cloud per la pubblicità, la propaganda politica o qualsiasi altra attività che possa essere considerata inappropriata o che possa violare le leggi applicabili o le politiche della scuola.

Articolo 8: Archiviazione dei dati

Tutti i dati archiviati nelle piattaforme cloud di supporto alla didattica devono essere adeguatamente protetti da accessi non autorizzati, perdite o danneggiamenti. Il personale deve quindi assicurarsi che i file contenenti dati personali siano salvati in aree sicure delle piattaforme, con accesso limitato solo ai membri del personale o agli studenti o ai genitori autorizzati. Tale accorgimento deve essere adottato in modo particolarmente rigoroso nel caso in cui si debbano archiviare nella piattaforma dati sensibili valutando l'opportunità di adottare anche tecniche di pseudonimizzazione (vedi art. 11).
Inoltre, è importante tenere sotto controllo lo spazio di archiviazione e assicurarsi di cancellare periodicamente i dati non più necessari, al fine di mantenere la sicurezza e la privacy delle informazioni degli studenti. In particolare a fine anno scolastico dovranno essere cancellati, ed eventualmente riconsegnati, tutti i documenti ed elaborati prodotti dagli studenti nel corso dell'anno ad eccezione. Per gli elaborati sottoposti a valutazione si ricorda la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" che prescrive la conservazione per almeno un anno, e la conservazione di documentazione a campione un anno ogni dieci.

Articolo 9: Accesso ai dati

Il personale deve assicurarsi che l'accesso ai dati degli studenti sia limitato solo ai membri del personale autorizzati che necessitano di tali informazioni per svolgere il loro lavoro. In caso di dubbio, il personale deve contattare il Dirigente o il Responsabile della Protezione dei Dati per ottenere conferma del fatto che il trattamento di un particolare set di dati sia giustificato.

Articolo 10: Sicurezza delle password

Il personale deve utilizzare password robuste e complesse per accedere alle piattaforme cloud di sostegno alla didattica. Le password devono essere uniche e non utilizzate in altre piattaforme o servizi. Inoltre, le password devono essere cambiate regolarmente per prevenire accessi non autorizzati.

Articolo 11 – uso di tecniche di pseudonimizzazione per dati ex Art. 9 GDPR

Ai fini della presente sezione, per "dati sensibili" si intendono le categorie di dati personali di cui all'articolo 9 del Regolamento generale sulla protezione dei dati (GDPR) ovverosia dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Per queste categorie di Dati Personali, il personale della scuola deve garantire la massima sicurezza e riservatezza in conformità con quanto previsto dal GDPR e dal Codice della privacy. I dati personali di natura sensibile potranno essere caricati sulla piattaforma cloud **solo se strettamente necessari ed in assenza di valide soluzioni alternative**. In questo caso il personale della scuola dovrà valutare la necessità di adottare tecniche di pseudonimizzazione che prevedono la sostituzione dei dati personali identificativi dell'interessato (come il nome ed il cognome) con un codice che non consente l'identificazione dell'interessato senza l'utilizzo di ulteriori informazioni. La pseudonimizzazione deve essere applicata a tutti i dati sensibili, compresi quelli relativi alla salute degli studenti e del personale della scuola, qualora questi siano oggetto di trattamento.

Articolo 12: Sicurezza del dispositivo

Il personale deve utilizzare solo dispositivi sicuri e aggiornati per accedere alle piattaforme cloud di sostegno alla didattica. I dispositivi personali non devono essere utilizzati per accedere a dati sensibili degli studenti, a meno che non siano adeguatamente protetti da password robuste e software di sicurezza aggiornato.

Articolo 13: Gestione delle violazioni dei dati personali

Per la gestione delle violazioni di dati personali (data breach) l'istituto ha definito specifiche linee guida e ha emesso una circolare per il personale in modo che questo sia in grado di riconoscere l'occorrenza di qualunque violazione, anche solo potenziale o sospetta, e di adottare comportamenti conseguenti. Ricordiamo in questa sede le disposizioni che impongono di informare l'amministratore della piattaforma cloud ed il dirigente scolastico di qualunque violazione di dati personali di cui si venga a conoscenza. Per informazioni o richieste di chiarimenti può essere contattato anche il responsabile protezione dati nominato dal dirigente scolastico. Il personale deve cooperare pienamente con qualsiasi indagine interna o esterna relative ai data breach o alle violazioni del presente documento. Le violazioni della presente politica saranno affrontate con la massima serietà e potranno comportare azioni disciplinari fino al licenziamento.