REGOLAMENTO INTERNO PER L'UTILIZZO SICURO DI PIATTAFORME CLOUD DI DIDATTICA DIGITALE

Regolamento adottato dal Consiglio di Istituto del 03-07- 2023 con delibera n 59

Articolo 1: Introduzione

Il presente regolamento è finalizzato a fornire istruzioni al personale della scuola sull'utilizzo sicuro della piattaforma cloud didattica digitale, come Google Workspace for 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.
L'appartenenza al dominio non comprende il servizio di posta elettronica g.mail per gli studenti.
La posta dei docenti è invece aperta anche all'esterno del dominio.
Gli account creati devono essere usati esclusivamente per le finalità didattiche.
Tutto il personale in servizio e gli studenti regolarmente iscritti o che hanno frequentato il nostro istituto, in temporanea istruzione parentale e in attesa dell'esame di idoneità, possiedono un account. Altre categorie di utenti (collaboratori, esperti impegnati in progetti della scuola) possono richiedere la creazione di un account, sempre in relazione alle necessità didattiche e di comunicazione; in questo caso l'accoglimento della domanda indirizzata al Dirigente è a suo insindacabile giudizio.

Articolo 3: Uso di altre applicazioni

Il personale è tenuto ad utilizzare esclusivamente le piattaforme cloud autorizzate dalla scuola, essendo vietato l'utilizzo di piattaforme cloud o di applicazioni non autorizzate o non sicure. 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 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. Per nessun motivo, l'account e la mail ad esso associato possono essere utilizzati per acquisti e transazioni. Inoltre, è vietato utilizzare le piattaforme cloud per la pubblicità, la propaganda politica e sindacale 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. Informare il Dirigente scolastico nel caso in cui siano archiviati documenti ed elaborati tipo compiti in classe, sottoposti a valutazione, quindi.

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 è tenuto ad utilizzare 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. In linea generale, comunque si raccomanda di non utilizzare le piattaforme per l'elaborazione di PEI e PdP. Confrontarsi sempre con il Dirigente scolastico su questo aspetto.

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 contatterà il DPO per 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. 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.

ART. 14 Cessazione del servizio Google WORKSPACE

Il servizio viene reso disponibile agli studenti per tutto il periodo di iscrizione presso l'Istituto e cessa al termine del percorso didattico all'interno dello Stesso o nel caso lo studente cambi scuola. Sarà possibile per l'alunno recuperare i propri materiali archiviati entro 30 giorni dalla cessazione del rapporto trascorsi i quali ogni dato e file archiviato nel Drive dell'account verrà eliminato.
Per i docenti/personale ATA: il servizio viene reso disponibile ai docenti e personale ATA
per tutto il periodo di permanenza presso l'Istituto e cessa con il termine del contratto, oppure qualora il docente sia trasferito ad altro Istituto. Sarà possibile recuperare i propri dati personali entro 3 mesi dalla cessazione del servizio. Successivamente l'indirizzo verrà sospeso per 3 mesi, quindi eliminato.

ART.15 Limiti di responsabilità dell'Istituto

L'istituto si avvale del servizio offerto dal fornitore Google Inc. con sede in 1600 Amphitheatre Parkway Mountain View, CA 94043, denominato "Google WORKSPACE" (ex "Google Gsuite for Education"). Pertanto l'istituto non ha alcun potere per quanto concerne le misure necessarie a minimizzare il rischio di perdita d'informazioni e a garantire la riservatezza dei dati. Le politiche di gestione dei dati operate dal fornitore sono descritte nel sito ufficiale dello stesso. L'utente solleva l'istituto da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, o alla mancata conservazione dei contenuti nonché al mancato invio/ricezione di messaggi di posta (email). Non sono previste attività di backup e di ripristino da parte dell'istituto dato che i server sono gestiti dal fornitore. L'utente provvederà per proprio conto alla realizzazione delle copie di sicurezza che ritenesse necessarie. L'istituto si riserva la possibilità di sospendere temporaneamente o disattivare definitivamente il servizio.

ART.16 Definizioni

Il presente Regolamento contiene i seguenti termini sotto elencati con il seguente significato:
a. Istituto: I. C. " G. Ferraris" Spello
b. Amministratore di dominio: Animatore Digitale e Assistente Tecnico incaricati dal Dirigente Scolastico per l'amministrazione del servizio
c. Servizio: Google Workspace (ex Google GSuite for Education) messo a disposizione dall'Istituto
d. Fornitore: Google Inc., con sede 1600 Amphitheatre Parkway Mountain View, CA 94043 Stati Uniti.
e. Utente: colui che utilizza un account del cui uso è pienamente responsabile
f. Account: insieme di funzionalità, applicativi, strumenti e contenuti attribuiti ad un nome utente con le credenziali di accesso.

g. data breach: violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.

Il Presidente del Consiglio di Istituto Gianluca Masciolini
Il Dirigente scolastico Prof.ssa Maria Grazia Giampè