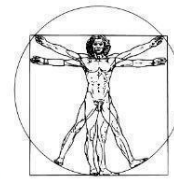




**Istituto Statale di Istruzione Superiore  
“LEONARDO DA VINCI”**



I.T.E. “G. Agnelli” 0547-673576 - Liceo “E. Ferrari” 0547-675277  
fois00400d@istruzione.it - fois00400d@pec.istruzione.it - www.isiscesenatico.edu.it  
Dirigenza e Segreteria Viale dei Mille n° 158 – 47042 Cesenatico (FC) - 0547-675277  
C. F. 90028640408 - FOIS00400D

**REGOLAMENTO INTERNO PER L'UTILIZZO DI PIATTAFORME CLOUD PER la  
DIDATTICA DIGITALE**

*(Del. Consiglio di Istituto n. 19 del 21 aprile 2023)*

**Articolo 1: Introduzione**

1. Il presente regolamento è finalizzato a fornire istruzioni al personale della scuola sull'utilizzo sicuro della 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, Accesso e Disconnessione**

1. 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.
2. 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.
3. Il personale, nel caso in cui utilizzi device condivisi con altri utenti, è tenuto a procedere alla disconnessione del proprio account al termine di ogni sessione di lavoro.

**Articolo 3: Uso di altre applicazioni**

1. 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**

1. 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

l'autorizzazione o l'incarico del titolare del trattamento dei dati personali (Dirigente scolastico).

2. 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).

#### **Articolo 5: Condivisione di contenuti**

1. 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**

1. Il personale della scuola è tenuto ad 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.
2. E' vietato accedere alle piattaforme cloud da reti pubbliche non sicure.

#### **Articolo 7: Utilizzo corretto delle risorse**

1. 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.
2. E' 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, le politiche della scuola (E-Policy d'Istituto - Del. Consiglio di Istituto n. 39/2021 del 18 ottobre 2021) o i Regolamenti di Istituto.

#### **Articolo 8: Archiviazione dei dati**

1. 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).
2. Il personale è tenuto a 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.

### **Articolo 9: Accesso ai dati**

1. Il personale è tenuto ad 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 per ottenere conferma del fatto che il trattamento di un particolare set di dati sia giustificato.

### **Articolo 10: Sicurezza delle password**

1. Il personale è tenuto ad 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.
2. Le password devono essere cambiate regolarmente per prevenire accessi non autorizzati.

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

1. 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) ovvero 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.
2. 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.

### **Articolo 12: Sicurezza del dispositivo**

1. Il personale deve utilizzare solo dispositivi sicuri e aggiornati per accedere alle piattaforme cloud di sostegno alla didattica.
2. 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**

1. 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.
2. Il personale è tenuto ad informare il dirigente scolastico di qualunque violazione di dati personali di cui sia venuto a conoscenza. Il personale è tenuto a cooperare pienamente con qualsiasi indagine interna o esterna relativa ai *data breach* o alle violazioni del presente documento.
3. Le violazioni della presente politica saranno affrontate con la massima serietà e potranno comportare le azioni disciplinari previste dalla norma.

#### **Art. 14 - Entrata in vigore e modifiche**

1. Il presente Regolamento entra in vigore dalla data di pubblicazione sull'Albo on line dell'Istituto, con valore di affissione all'albo pretorio a tutti gli effetti.
2. Eventuali modifiche e/o integrazioni al presente Regolamento devono essere deliberate dal Consiglio di istituto secondo la normativa vigente in materia.