



06 Dicembre 2025

Circolare numero 111

Circolare 111 - Policy di Uso Accettabile (AUP) delle Risorse Informatiche e Norme di Cyber-Igiene per la Tutela della Privacy di Studenti e Personale

Al Personale Scolastico (Docente e ATA), Ai Genitori/Tutori, Studenti.

Oggetto: Policy di Uso Accettabile (AUP) delle Risorse Informatiche e Norme di Cyber-Igiene per la Tutela della Privacy di Studenti e Personale

Premessa

Al fine di garantire un ambiente digitale di apprendimento e lavoro sicuro, etico e rispettoso della privacy (in conformità con il Regolamento Generale sulla Protezione dei Dati – GDPR), si rende necessaria la rigorosa osservanza delle seguenti regole relative all'uso dei dispositivi (computer, tablet, ecc.), delle reti, degli account email e delle piattaforme digitali messe a disposizione dall'Istituto.

Principi Fondamentali di Utilizzo

Area Indicazione Esempio Specifico Obiettivo Principale Le risorse (dispositivi e rete) devono essere utilizzate esclusivamente per scopi didattici, amministrativi o lavorativi. **L'uso personale** è tollerato solo se strettamente limitato e a condizione che non interferisca con il lavoro/studio o la larghezza di banda della rete. **Account e Password** Ogni utente è l'unico responsabile della segretezza e della protezione del proprio account. **È vietato condividere la propria password.** È obbligatorio effettuare il **logout** al termine di ogni sessione. **Proprietà Intellettuale** È fondamentale rispettare i diritti d'autore e le licenze del software. È severamente **vietato scaricare, distribuire o utilizzare** materiale protetto da copyright (musica, film, software pirata) sui dispositivi e sulla rete dell'Istituto. **Privacy Altrui** È necessario rispettare la privacy, la dignità e l'immagine degli altri utenti (studenti e colleghi). **Non è consentito** accedere o tentare di accedere ai file, agli account o alle cartelle di altri utenti senza esplicita autorizzazione.

II. Uso Non Consentito (Divieti Espliciti)

L'Istituto condanna e sanziona le seguenti attività:

Installazione di Software Non Autorizzato: È **vietato** installare qualsiasi software, applicazione o estensione sui dispositivi dell'Istituto senza la preventiva e formale approvazione..... Ciò previene l'introduzione di malware e software con licenze non conformi. **Accesso a Contenuti Inappropriati o Illegali:** È **vietato** accedere, visualizzare, scaricare o distribuire materiale esplicitamente sessuale, violento, discriminatorio, offensivo o illegale. **Attività Illecite e Danni alla Rete:** È **vietato** tentare di aggirare le misure di sicurezza, i filtri di rete o i controlli implementati. È **vietato** distribuire malware, virus o partecipare a qualsiasi forma di attacco informatico. **Violazione della Privacy:** È **vietato** registrare, fotografare o condividere immagini, video o informazioni di altri utenti (studenti, colleghi) senza il loro esplicito consenso e, nel caso di minori, senza il consenso dei genitori. **III. Norme di Cyber-Igiene e Buone Pratiche Dopo l'Uso**

Queste azioni sono cruciali per proteggere la privacy quando si utilizzano dispositivi o postazioni condivise (laboratori, aule multimediali, uffici).

Azione Importanza per la Sicurezza Effettuare Sempre il Logout Regola Fondamentale: Dimenticare di uscire dall'email, dai servizi cloud (Drive, Teams) o dalle piattaforme consente all'utente successivo di accedere a tutti i dati e file sensibili dell'account. **Cancellare la Cronologia** La cronologia di navigazione, i cookie e le password salvate possono esporre le attività e le credenziali. Si suggerisce l'uso della **modalità di navigazione in incognito/privata** per le sessioni rapide. **Scollegare i Dispositivi Personali** Se sono state utilizzate chiavette USB, hard disk esterni o smartphone, assicurarsi che siano stati **scollegati in sicurezza** (rimozione sicura) e che siano stati portati via dall'utente. **Verificare la Stampa** Assicurarsi che documenti contenenti informazioni sensibili non siano rimasti sul vassoio della stampante o nella coda di stampa del dispositivo condiviso.

Conclusione e Sanzioni

Tutti gli utenti (Personale, Studenti, Genitori per delega) sono tenuti a leggere e rispettare questa Policy. La mancata osservanza delle regole sopra elencate costituisce una violazione delle norme di sicurezza e privacy dell'Istituto e comporterà l'applicazione di sanzioni disciplinari che possono includere la revoca dei privilegi di accesso e, nei casi più gravi, l'avvio di procedimenti legali.

Si confida nella collaborazione di tutti per mantenere un ambiente digitale sicuro.

Il Dirigente Scolastico

Margherita Silvestre