Istituto Comprensivo
**Velletri Sud Ovest**
Velletri (RM)

28 Febbraio 2025

**Circolare numero 177**

# Misure di sicurezza informatica

## Premessa

Si è riscontrato che, al termine dell'utilizzo delle postazioni informatiche condivise presenti nell'Istituto, gli utenti non sempre effettuano la disconnessione dai propri account personali (posta elettronica, registro elettronico, ecc.). Tale comportamento costituisce una grave violazione delle norme sulla protezione dei dati personali e può comportare accessi non autorizzati a informazioni riservate e dati sensibili.

## Obblighi normativi

Si ricorda che il Regolamento UE 2016/679 (GDPR) e il D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali), come modificato dal D.Lgs. 101/2018, prevedono l'adozione di misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali trattati. In particolare, l'art. 32 del GDPR impone l'adozione di misure volte a garantire la riservatezza, l'integrità e la disponibilità dei dati personali, nonché la resilienza dei sistemi e dei servizi di trattamento.

## Disposizioni operative

Alla luce di quanto sopra, si dispone che tutto il personale scolastico osservi scrupolosamente le seguenti procedure:

**Effettuare SEMPRE la disconnessione** (logout) da tutti gli account personali al termine dell'utilizzo delle postazioni informatiche condivise, in particolare da:  Casella di posta elettronica istituzionale e personale Registro elettronico Account Google Workspace for Education Qualsiasi altra piattaforma o servizio che richiede autenticazione **NON memorizzare credenziali di accesso** (username e password) sui browser delle postazioni condivise. **NON selezionare l'opzione "Ricorda password"** o "Resta connesso" quando si accede a qualsiasi account da postazioni condivise. **VERIFICARE sempre**, prima di allontanarsi dalla postazione, di aver chiuso tutte le sessioni attive. Nei casi in cui si riscontrino postazioni con account di altri utenti ancora attivi, provvedere alla disconnessione immediata e segnalare l'accaduto al Dirigente Scolastico.

## Responsabilità

Si ricorda che la mancata osservanza delle presenti disposizioni può comportare:

Accesso non autorizzato a dati personali, anche di natura sensibile Violazione delle norme sul trattamento dei dati personali Potenziali responsabilità personali
Ogni utente è responsabile della protezione dei dati a cui ha accesso e del corretto utilizzo delle risorse informatiche dell'Istituto.

## Entrata in vigore e diffusione

La presente circolare entra in vigore immediatamente e sarà pubblicata sul sito web dell'Istituto.

Si invitano i docenti a discutere con gli studenti l'importanza della sicurezza informatica e della protezione dei dati personali e ad accertarsi sempre, quando utilizzano i device in dotazione alla scuola effettuando

l’accesso con il loro account personale, che provvedano ad effettuare sempre la disconnessione al termine del lavoro.