Istituto Superiore majorana Palermo
tecnico liceo professionale serale

Palermo, 15 Settembre 2025

A tutti i Docenti
al personale ATA

CIRCOLARE N. 1035

Oggetto: Password Policy – gestione sicura delle credenziali di accesso per il personale docente e ATA incaricato al trattamento di dati personali

PREMESSA
La protezione delle credenziali di accesso è uno degli elementi fondamentali per garantire la sicurezza dei dati e delle informazioni trattate dall'Istituto, in particolare tramite la creazione, gestione e conservazione delle password, che costituiscono la principale barriera contro accessi non autorizzati.

Visto il D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, e le disposizioni del Regolamento (UE) 2016/679 (GDPR), nonché la Nota MIM del 13/12/2023 con cui è stata diffusa la comunicazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) e del Garante per la Protezione dei Dati Personali sulle Linee guida per la conservazione sicura delle password, la presente circolare fornisce indicazioni operative per il personale scolastico incaricato al trattamento di dati personali.

Riferimenti normativi:
- Regolamento (UE) 2016/679 (GDPR)
- D.Lgs. 196/2003 (Codice Privacy), come modificato dal D.Lgs. 101/2018
- Nota MIM del 13/12/2023 - Linee guida ACN e Garante Privacy
- Art. 615-quater Codice Penale (accesso abusivo a sistemi informatici)

1. CAMPO DI APPLICAZIONE
La presente policy si applica obbligatoriamente a:

1.1 Sistemi e Servizi:
- registro elettronico e piattaforme didattiche
- posta elettronica istituzionale
- sistemi gestionali (segreteria, amministrazione)
- postazioni di lavoro (pc, tablet, lim)
- dispositivi mobili
- rete wi-fi dell'istituto
- servizi cloud autorizzati
- piattaforme e-learning e videoconferenza

1.2 Autenticazione a due fattori (2FA)
Obbligatoria per:
- amministratori di sistema

2. OBBLIGHI E RESPONSABILITÀ DEGLI UTENTI
Il personale incaricato si impegna a:
- cambiare la password al primo accesso, rispettando i criteri indicati nel paragrafo 3;
- mantenere le credenziali strettamente personali e non condivisibili;

- non fornire mai le proprie credenziali via e-mail, messaggistica o altri canali non sicuri;
- prestare attenzione a e-mail o link sospetti per evitare frodi informatiche;
- segnalare immediatamente anomalie o sospetti di violazione al team digitale o animatore digitale;
- utilizzare preferibilmente un password manager sicuro (es. keepass, lastpass) evitando la conservazione su supporto cartaceo o in file non protetti.

Divieti Assoluti:

→ condivisione di credenziali via email, chat o telefono
→ annotazione di password su supporti cartacei accessibili
→ salvataggio in chiaro su dispositivi non protetti
→ utilizzo di pc pubblici per accedere a servizi dell'istituto
→ lasciare incustodite postazioni con sessioni attive

3. REQUISITI TECNICI PER LA CREAZIONE DELLE PASSWORD

Le password devono:

- essere lunghe almeno 8 caratteri;
- contenere almeno 4 tipologie di caratteri tra maiuscole, minuscole, numeri e simboli;
- non includere riferimenti personali (nome, cognome, data di nascita) né il nome utente;
- non essere parole di dizionario comuni;
- essere create con parole di fantasia o camuffate con caratteri speciali;
- essere diverse per ogni servizio e non riutilizzare password già usate in passato;
- essere cambiate periodicamente o in caso di sospetta violazione.

4. CONSERVAZIONE DELLE CREDENZIALI

Per una corretta gestione e conservazione delle password:

- non conservare mai le password su biglietti o documenti facilmente accessibili;
- non memorizzarle in chiaro su dispositivi non protetti;
- non salvarle automaticamente su pc o smartphone pubblici o condivisi.

5. USO DELL'E-MAIL ISTITUZIONALE

L'e-mail fornita dall'Istituto deve essere utilizzata esclusivamente per finalità istituzionali legate alle mansioni assegnate. È vietato l'uso promiscuo, la registrazione a servizi non autorizzati o l'iscrizione a newsletter estranee, al fine di ridurre il rischio di violazioni e uso improprio dei dati.

6. GESTIONE DEGLI INCIDENTI

6.1 Segnalazione immediata in caso di:

- sospetto accesso non autorizzato
- perdita o furto di dispositivi
- email di phishing
- malfunzionamenti anomali

6.2 Procedura di emergenza:

- cambiare tutte le password compromesse
- disconnettere il dispositivo dalla rete

- documentare l'incidente (data, ora, descrizione)
- attendere istruzioni dal team digitale

7. RIFERIMENTI NORMATIVI PENALI

La detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici costituisce reato ai sensi dell'art. 615-quater c.p., anche quando ottenuti mediante inganni o osservazione della digitazione.

8. INCARICO AL TRATTAMENTO DEI DATI PERSONALI

Ogni dipendente è incaricato del trattamento dei dati personali limitatamente alle proprie mansioni, con obbligo di attenersi scrupolosamente alle istruzioni del Titolare. L'accesso è consentito esclusivamente ai dati strettamente necessari.
Per approfondimenti sulle regole di creazione e gestione delle password, si rinvia alla guida del Garante: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4248578

9. CONTATTI E RIFERIMENTI

Ruolo	Nome	Email
Dirigente Scolastico	Giovanna De Pietro	giovanna.depietro@majoranapa.edu.it
Animatore digitale	Baldassare Profeta	animatoredigitale@majoranapa.edu.it
DPO	Mario Grimaldi	dpo.grimaldi@gmail.com
DSGA	Paola Zangari	paola.zangari@majoranapa.edu.it

10. ENTRATA IN VIGORE E AGGIORNAMENTI

Entrata in vigore: 01/10/2025
Prossima revisione: [01/10/2025 + 12 mesi]
Versione: 1.1 - [01/10/2025]

La presente circolare sostituisce ogni precedente disposizione in materia di gestione password e sicurezza informatica.

La Dirigente Scolastica
Prof.ssa G. De Pietro
(Firma autografa omessa ai sensi dell'art.3, comma 2 del D.lgs. 39/1993)