LICEO SCIENTIFICO STATALE "FRANCESCO SEVERI"
Liceo Scientifico di Ordinamento - Liceo Scientifico Scienze Applicate- Liceo Linguistico – Liceo Musicale
Viale L. D'Orsi, 5 – 80053 Castellammare di Stabia (NA)
PBX 4 linee Tel –0818717605- 0818739745 – 0818713148 – 0818739752
CF 82011770631 - IBAN IT 15 T 01030 22100 000000723277
CONTO UNICO TESORERIA IT29K0100003245425300314138
NAPS110002@ISTRUZIONE.IT – NAPS110002@PEC.ISTRUZIONE.IT
Fatturazione elettronica: Codice Univoco Ufficio UFQ3HR

L.S.S. - "F. SEVERI" - C.MMARE
Prot. 0018796 del 12/11/2026
II-5 (Uscita)

Agli Alunni
Ai genitori/esercenti la responsabilità genitoriale
Ai docenti
AL DSGA
Sito Web-Albo-Atti
Bacheca registro Argo

Circolare n.100

Oggetto: istruzioni operative per la protezione degli account e delle credenziali di accesso alle piattaforme scolastiche

Care studentesse, cari studenti,

ogni giorno utilizzate account personali per accedere ai servizi della scuola: il Registro Elettronico, la posta istituzionale e le piattaforme didattiche in uso nel Liceo. Le vostre credenziali (nome utente e password) sono la chiave che protegge i vostri dati e quelli dei vostri compagni e docenti: se finiscono nelle mani sbagliate, qualcuno può entrare al posto vostro, leggere informazioni riservate, inviare messaggi a vostro nome o diffondere contenuti.

Per prevenire la sottrazione delle credenziali da parte di terzi, è importante ricordare a tutti le regole per proteggere i propri account.

Il furto di credenziali avviene quasi sempre con trucchi semplici: un messaggio falso che invita a "verificare l'account", una password troppo facile o usata ovunque, un dispositivo lasciato aperto. Per questo vi chiediamo di seguire con attenzione le istruzioni che seguono, che fanno parte delle regole di utilizzo delle piattaforme scolastiche.

1. Le vostre credenziali sono personali

- Non comunicate a nessuno la vostra password: né ai compagni, né agli amici, né a chi si presenta come tecnico, docente o personale della scuola. **La scuola non vi chiederà mai la password**, né per e-mail, né per telefono, né in chat.
- Non comunicate mai i codici di verifica (OTP) che ricevete via SMS, e-mail o app: servono solo a voi, nel momento in cui accedete.
- Non usate l'account di un'altra persona, nemmeno con il suo permesso.
- Non scrivete la password su fogli, diario, note del telefono o post-it.

2. Scegliete una password robusta

- Almeno **12 caratteri**, con lettere maiuscole e minuscole, numeri e simboli. Un buon metodo è una frase facile da ricordare per voi ma difficile da indovinare (es. tre o quattro parole non collegate tra loro, con numeri e simboli).

- Evitate nome, cognome, data di nascita, nome dell'animale domestico, della squadra del cuore o sequenze come "123456" e "password".
- **Usate una password diversa per ogni servizio**: la password della scuola non deve essere la stessa dei social, dei giochi o della posta personale. Se un sito viene violato, i malintenzionati provano la stessa password ovunque.
- Cambiate subito la password provvisoria ricevuta dalla scuola al primo accesso e cambiatela immediatamente se sospettate che qualcuno l'abbia scoperta.
- Se possibile, usate un gestore di password (password manager) affidabile, invece di salvare le password nel browser di dispositivi condivisi.

3. Attivate la verifica in due passaggi

Dove la piattaforma lo consente, attivate la **verifica in due passaggi** (codice via app o SMS oltre alla password): anche se qualcuno scopre la vostra password, non potrà entrare senza il vostro telefono.

4. Riconoscete i messaggi truffa (phishing)

Diffidate di e-mail, SMS, chat o messaggi sui social che:

- vi chiedono password, codici, dati personali o pagamenti;
- vi mettono fretta ("il tuo account sarà bloccato entro 24 ore", "verifica subito");
- contengono link o allegati inattesi, anche se sembrano arrivare da un docente, da un compagno o dalla scuola;
- hanno un mittente o un indirizzo web strano, con errori di ortografia o lettere scambiate.

Prima di cliccare, fermatevi: passate il mouse sul link per vedere l'indirizzo reale, non aprite allegati sospetti e, nel dubbio, chiedete conferma al docente **di persona** o tramite un canale che conoscete già. Accedete alle piattaforme digitando voi l'indirizzo o usando l'app ufficiale, mai da link ricevuti.

5. Proteggete i dispositivi

- Bloccate smartphone, tablet e computer con PIN, password o impronta.
- Mantenete aggiornati sistema operativo, browser e app; installate app solo dagli store ufficiali.
- Sui dispositivi condivisi o della scuola (laboratori, LIM, computer di classe) **non salvate le password**, usate se possibile la navigazione in incognito e **fate sempre il logout** a fine utilizzo.
- Non lasciate il dispositivo sbloccato e incustodito.
- Evitate di accedere agli account scolastici da reti Wi-Fi pubbliche non protette.

6. Usate gli account scolastici solo per la scuola

- Usate l'account istituzionale solo per le attività scolastiche e non per iscrivervi a social, giochi o altri servizi.
- Non scaricate, non inoltrate e non pubblicate dati, voti, immagini o contenuti di compagni e docenti visti sulle piattaforme: la loro diffusione è una violazione della privacy che può comportare conseguenze disciplinari e, nei casi più gravi, anche penali.

7. Comportamenti vietati e conseguenze

È severamente vietato tentare di scoprire, sottrarre, farsi consegnare o utilizzare le credenziali di altre persone, accedere ad account che non sono i propri (di compagni, docenti o personale della scuola) o fingersi un'altra persona sulle piattaforme. Non si tratta di uno scherzo: questi comportamenti possono costituire reati, come l'accesso abusivo a un sistema informatico (art. 615-ter del Codice penale), la detenzione e diffusione abusiva di codici di accesso (art. 615-quater c.p.) e la sostituzione di persona (art. 494 c.p.).

Chiunque venga sorpreso a sottrarre credenziali o ad accedere con account non suoi sarà soggetto ai **provvedimenti disciplinari** previsti dal Regolamento di disciplina d'istituto e dallo Statuto delle studentesse e degli studenti (D.P.R. 249/1998). La famiglia sarà informata e la scuola attiverà le procedure per la **segnalazione dei fatti alle autorità competenti** (Polizia Postale e delle Comunicazioni, Autorità giudiziaria) e, ove previsto, per la comunicazione al Garante per la protezione dei dati personali, ferma restando la possibilità di chiedere il risarcimento degli eventuali danni.

8. Cosa fare se qualcosa non va

Se pensate che il vostro account sia stato violato, o notate qualcosa di strano (accessi che non riconoscete, messaggi inviati che non avete scritto, password che non funziona più, impostazioni modificate):

1. cambiate subito la password, se riuscite ancora ad accedere;
2. **avvisate immediatamente** il coordinatore di classe o la segreteria: NAPS110002@istruzione.it;
3. non cancellate i messaggi sospetti: possono servire per le verifiche;
4. se avete usato la stessa password altrove, cambiatela anche lì.

Segnalare subito non è una colpa: permette alla scuola di intervenire in tempo e di proteggere anche gli altri.

9. Riferimenti

Per chiarimenti potete rivolgervi alla segreteria o al Responsabile della protezione dei dati (DPO): PHOR S.R.L. – info@phorsrl.it – phor@pec.it.

Vi chiediamo di leggere queste istruzioni insieme ai vostri genitori. I docenti coordinatori sono invitati a illustrarle in classe.

Grazie per la collaborazione.

Il Dirigente Scolastico

prof.ssa Elena Cavaliere

Firmato digitalmente ai sensi del D.Lgs. 82/2005 s.m.i. e norme collegate.