SCUOLA EUROPEA di VARESE

indirizzo: via Montello, 118
21100 Varese (VA)
ITALIA

telefono: +39 0332 806111
fax: +39 0332 806202
sito web: www.eursc.org
codice fiscale: 80009540123

Digital Good Practices

for Students

The European School of Varese, through the Central Office in Brussels, provides every student with access credentials for the institutional email and the Microsoft Teams platform — essential tools for teaching, communication, and study.

The security of our digital space, however, does not depend solely on central systems. It also depends on the responsible use each person makes of their own devices. Recent cybersecurity incidents at various schools have shown how malicious actors often exploit open sessions or personal computers to access school data and send inappropriate messages under compromised accounts.

To protect everyone's privacy and maintain the integrity of our learning environment, we strongly encourage all students to follow the guidelines below.

Your Six Commitments to Digital Safety

1

🔐 Session Management

When using Microsoft Teams or your school email on a personal or shared computer, always log out at the end of your session. Never leave your device unattended with school applications open.

2

🔑 Password Management

Choose a strong password (combining uppercase and lowercase letters, numbers, and special characters). It is strictly forbidden to reuse your school account password for private services such as social networks, personal email, or online gaming platforms.

3

🎯 Phishing Awareness

Never click on links or download attachments from unknown senders or suspicious emails (e.g. urgent messages requesting password changes you did not initiate, or notifications claiming you have won a prize).

4

Separating School and Personal Life

Be cautious if unknown individuals try to contact you on your personal social platforms (Discord, TikTok, Instagram, Snapchat) and make reference to your class, your school, or student lists. This may be a social engineering attempt to manipulate you or extract information from you.

5

No Sharing of Credentials

Your institutional email is strictly personal. Do not share your credentials with classmates, friends, or third parties for any reason whatsoever. Each student is responsible for all actions carried out using their own account.

6

Immediate Reporting

If you notice unusual activity on your account (e.g. messages sent without your knowledge, logins from unexpected locations, or changes to your settings), or if you receive threatening or harassing emails, inform your parents and the School Administration immediately. Acting quickly stops risks before they escalate.