10 Golden Rules for cybersecurity

Protect your accounts with strong authentication!

- Use **multifactor authentication** (MFA) whenever possible!
- Use **long passwords (15 characters, at least),** containing uppercase, lowercase, numeric characters, special characters (&,$,%,!,=,+...).
- Do **NOT share** them
- Rely on a **password manager** (not the same as saving your password on briwsers! to be avoided)

Create multiple accounts

- Use **different passwords** for professional and personal accounts
- **Protect** your **school e-mail**: do NOT use it to register on websites, platforms that are not school-related !
- Regularly check **which apps and services have access to your accounts**. Remove any that you no longer use or don't trust.

Have backups

- Store all your data in a system where backups are made regularly and centrally.
- Staff is required to save their work related documents in their 0365 school account.

Security updates

- Regularly **update all software and applications** to close potential security gaps.
- Make it a habit to **restart your devices** regularly, as some updates require a reboot to take effect.
- **Pay attention to notifications about updates,** and take action promptly to maintain device security.

Secure your workspace

- **Never** leave physical documents (e.g., papers) or devices **unattended** on your desk.
- **Lock your computer** if you leave it unattended.
- Ensure you **collect all your printed materials** from the printer promptly.

SCHOLA EUROPAEA
Brussels III

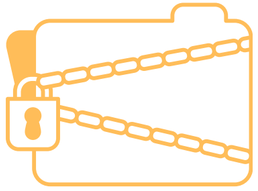
10 Golden Rules for cybersecurity

Avoid public WiFi - Use VPN

- **Avoid** public Wi-Fi.
- Use the **school's Wi-Fi** network instead and only for pedagogical related purposes.
- Staff is invited to always connect to the **Virtual Private Network (VPN)** when working remotely.

Beware of phishing

- **Read** carefully the school guidelines regarding phishing.
- **Never respond** and provide your or others' personal information.
- **Train** in detecting phishing attempts.
- **Report** phishing attempts to IXL-ICT@eursc.eu and and delete the email/text.



Handling of sensitive information

- **Never dispose of sensitive information** (e.g., medical records, financial data, or ID copies) in regular yellow bins.
- **SHRED** all confidential or sensitive materials.
- Avoid consulting or discussing confidential information in public places within the school. Always try to isolate yourself wherever possible to prevent anyone overhearing a conversation.

Careful when dowloading

- Use only **official websites and platforms** to download applications and software.
- Be cautious of **unfamiliar file types**; avoid downloading executable files (.exe) unless you're sure of their safety.
- Always **run antivirus** scans on downloaded files before opening them.
- On school devices, downloading software should be avoided. Software is installed by the IT team

Report to ICT

Report all information security incidents to our school IT team when you notice:

- anything contrary to this document;
- a suspected or confirmed incident, such as phishing, occurs.

Contact : IXL-ICT@eursc.eu

SCHOLA EUROPAEA
Brussels III