Safe Access Guidelines for Public Wi-Fi

DOs

- Use a school-approved VPN to encrypt your internet traffic.
- Only access school systems through secure (HTTPS) platforms.
- Log out of systems when finished-do not just close the tab.
- Keep your device's OS and apps updated with the latest patches.
- Enable Two-Factor Authentication (2FA) for school accounts.
- Be aware of your surroundings-protect your screen and avoid discussing sensitive data aloud.
- Use school-managed devices where possible for built-in security.
- Save sensitive work offline if unsure about network safety.

DON'Ts

- Do not access sensitive data without using a VPN.
- Do not use shared or public computers to access school systems.
- Do not disable firewalls, antivirus, or security settings.
- Do not allow devices to auto-connect to public Wi-Fi networks.
- Do not download attachments from unknown sources-even within school email.
- Do not leave devices unattended in public spaces.
- Do not store passwords in plain text-use a password manager.

Pro Tip: If you're unsure whether it's safe to access a system while away from school, err on the side of caution-wait until you're on a secure network or use your mobile hotspot.