Imperial College London

Staff and students are responsible for the security of their personal information and devices and all College information, devices, systems and networks they access, share or use.

✓ **Adhere to College policy on the use of IT facilities** by respecting equipment, access privileges, and copyright laws.

✗ **Do not ignore College policy!** Violations can result in network bans, expulsion or fines.

✓ **Use strong PIN/passwords and keep them safe.**

✗ **Do not share your password with anyone (even ICT)** or use passwords that are easy to crack.

✓ **Apply security measures to ALL computers and devices** (e.g. password protection and up-to-date security software).

✗ **Do not put your computers or devices at risk** by leaving them unattended, logged in or unlocked.

✓ **Use College's recommended file storage to save information** (e.g. H: drive, group space, OneDrive for Business)

✗ **Do not rely on removable media** (such as USB drives) to store information you can't afford to lose.

✓ **Use encryption to protect personal or sensitive information** before storing or sharing.

✗ **Do not use email to send sensitive information.**

Visit the College ICT security website for College policy and more information on encryption, device protection and tips to help spot scam emails and stay safe online.

Make sure you are protected.
Visit www.imperial.ac.uk/be-secure

Be Secure