Homeworking Security Guide

Computer Screens

Position your screen away from windows and accidental viewing by family and visitors.

Lock your screen when leaving your desk by pressing the Windows key (⊞) + L or hold down Ctrl+ Alt+ Delete

Passwords

Use strong passwords. These should be memorable to you, but not easy to guess!

Don't write them down or share them with other people.

Personal Accounts

Don't use personal email or personal file storage to receive, send or store confidential school data.

Keep school data within the school's systems.

Listening Devices

Turn off all listening devices (e.g. Alexa) during conference calls.

Discussions should not be overheard by other people at home.

Paper Security

Lock away confidential paperwork when not in use. Do not leave them in your car overnight or look at them in public places.

Dispose of unwanted paperwork securely. Use a 'cross cut' shredder.

Encryption

Portable IT equipment such as laptops, USBs, pen drives etc. must be encrypted if they hold personal data.

Seek authorisation before downloading any school data and taking it off site.

Phishing Emails

Watch out for suspicious emails. Don't give out private information (such as bank details or passwords) and be careful about clicking on links or downloading attachments.

Equipment

If you've been provided with school IT equipment, you must keep this secure. Do not leave it on public display or in your car overnight.

Report Breaches

Report personal data security breaches to your line manager quickly. If they are not available, contact the Data Protection Officer directly, who will advise on the next steps.

Contact Your Data Protection Officer:

Amber Badley
DPO@firebirdltd.co.uk

Firebird
Data Protection Consultancy Ltd