Driving data protection excellence in education

Risk List

Home Working

Risks you must consider when your staff are working offsite:

- Unencrypted devices/personal devices, make sure you are not mixing the schools files with your own.
- Others having access to the device/sharing the device. Is the Device in a secure location out of sight and reach?
- Loss of device
- Divulging Personal Data
- Paper copies being lost/printed, where possible, working from the school's cloud can help to prevent this risk.
- Any paper copies need to be locked away and not left out on the table.
- Do you use strong passwords?
- Do you have appropriate communication technology, remember unless using a business account sharing data over messaging apps like WhatsApp is a data breach.
- Locking device when walking away from it, in even in your own home.
- Teachers' mark sheets and records to be kept safe.
- SEN & FSM Data is sensitive, are you keeping it secure?
- Staff Records.
- Parents and Governor Details.
- Staff should ONLY process minimum personal data for what is needed to complete your role, if you have greater access than needed you should inform the school.
- Safeguarding information – there is a risk if this data needs to be transmitted. Staff must take extra care and think twice before transferring any data as such.
- Staff will be instructed remotely how to check that their devices are safely encrypted. Most should be in today's technology.
- Staff MUST continue to report ALL breaches.

DPO/DP Lead contact details must be given to all staff, and they must be advised to follow normal school procedures to raise any concerns they have around protecting your school's personal data and if they need to report a Data Breach.