

Working from Home

Do...

- Ensure you follow your school's policy that sets out expectations for home working and any permitted use of personal devices.
- Keep information in a secure place within your home.
- Only use cloud storage and applications that have been authorised by the school's IT service.
- If permitted to use school USB memory sticks, ensure these are encrypted.
- Be aware of your surroundings - consider if your screen can be seen through a window or if you can be heard on sensitive calls or in meetings.

Don't...

- Email work to your personal account or download school-related personal information to your own personal laptop or device.
- Allow family or friends to have access to school information.
- Leave paper files or devices in your car overnight.
- Use public Wi-Fi. You should use a home network or hotspot instead.
- Leave food or drink on or near paperwork or devices, as spills could destroy information and equipment.

Data Breaches

Do...

- Follow your school's procedure for information security incidents.
- Report any incidents to the appropriate member of staff straight away.
- Assist with reporting any serious incidents to your Data Protection Officer.
- Work with your DPO to ensure serious, high risk breaches are reported to the Information Commissioner's Office (ICO) within 72 hours.
- Log all breaches and near-misses in the school's Information Security Incident Log.
- Carry out refresher training if you have been involved in a breach.

Don't...

- Keep a breach or incident to yourself, even if you think it's only minor.
- Delay when reporting a breach to the DPO.
- Allow the same breach to occur twice. Ensure you carry out any preventative measures following a breach, to prevent a re-occurrence.

Information Security

Do...

- Lock your device if you are away from your device or workstation, i.e. using ctrl + alt + delete.
- Store paper files containing sensitive personal information securely in locked cabinets in lockable rooms within school.
- Use the 'BCC' email function when appropriate.

Don't...

- Leave personal information out overnight or if you are away from your workstation.
- Forget about private documents you are printing and leave them on the printer where they could be viewed by others.
- Deliberately access information you are not authorised to view.

Special Category Data

Details about:

- Sex life
- Race or ethnicity
- Religion and philosophical beliefs
- Mental or physical health
- Political views
- Trade union membership
- Biometric and genetic info

Please note that criminal history information is covered under separate legislation but should be treated in the same way as special category data.

Do...

- Take extra care when sending special category information externally.
- Send emails containing sensitive information securely, e.g. via Egress.
- Post sensitive information securely, e.g. via special or recorded delivery.
- Ensure contact details for your data subjects are accurate and up-to-date, to ensure information is not sent to the wrong person.

Don't...

- Accidentally send additional sensitive files, which are not intended for that recipient. Please double check before sending.
- Share special category data externally, unless you have a clear purpose such as safeguarding.
- Display anything containing sensitive data on the whiteboard or a shared area of the school's IT systems.

Password Security

Do...

- Comply with your school's password policy to ensure a complex, unique password.
- Where possible, use passwords made up of three random words strung together, e.g. 'coffeetrainfish' or 'eaglecrumpetsdiary'.
- Store passwords securely and away from your device, if you struggle to remember them without writing them down.

Don't...

- Use easy to guess words, such as 'password' or 'qwerty', pet names or favourite sports teams.
- Use the same password for different accounts.
- Share your password with anyone else – including your manager or ICT.
- Use shared school passwords, which multiple staff use to access the same account

Cyber Security

Do...

- Make sure devices have anti-virus software installed, and that all apps and software are up to date.
- Contact an organisation directly, using their official contact details, if you receive a suspicious message claiming to be from them.
- Ask for advice if you are not sure if a link or message is legitimate.

Don't...

- Click on links in emails, especially if something doesn't seem right.
- Use unencrypted, personal USB drives.
- Keep quiet if you think you have been caught out by a scam. Instead, report it to your Headteacher or IT team.

Training and Awareness

Do...

- Carry out data protection training at least every two years.
- Consider taking additional training relevant to your role.

Don't...

- Put into place new apps, projects, or systems involving personal data without informing the relevant staff member, so they can carry out the necessary contract checks and complete a Data Protection Impact Assessment (DPIA) if required.

Lancaster Christ Church C of E Primary
School



GDPR / Data Protection
Handbook



September 2023