Data Security

Good Practice in Information Handling

This guide is provided to raise your awareness of where potential breaches of security could occur. Following this guide will help you to prevent the loss of or unauthorised access to personal or sensitive data that could cause harm or distress to students, staff or parents.

Data Security Definition

Data security legislation means that anyone who holds or has access to personal data, whether on paper or electronically must keep that data secure. Personal data is defined as any combination of data items that identify an individual and provide specific information about them, their families or circumstances. This includes names, contact details, gender, date of birth, as well as other information such as academic achievements, progress in school, behaviour and attendance records. Some data is referred to as sensitive personal data. This includes, but is not limited to, racial or ethnic origin, mental and physical health, religious beliefs, SEN details and criminal offences.

Anyone who processes personal data must comply with the eight principles of the Data Protection Act, which make sure that personal data is:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept for longer than is necessary
6. processed in line with the individual's rights
7. kept secure with appropriate technical and organisational measures taken
8. not transferred to other countries without adequate protection

What should we do?

It is a legal requirement of the Data Protection Act 1998 to secure personal data. As a member of staff you have a shared responsibility to keep secure any personal or sensitive data that you use in your day-to-day professional duties. In order to minimise the risk involved in accessing the IT systems users are required to adhere to the following:

- Staff must comply with the Data Protection Act and the Academy's Data Protection Policy and ICT Acceptable Use Policy at all times.
- Users should not remove or copy personal or sensitive data from the Academy network unless the media is encrypted, is transported securely and will be stored in a secure location.
- Master documents need to be secure and backed up – data should never be solely stored on an external device (e.g. a USB memory stick).
- Users should delete personal or sensitive data when it is no longer needed. When deleting data ensure you also empty the recycle bin.
- Where possible access data remotely rather than taking it offsite. Make sure you log out completely of any remote services once you have finished.
- If you download any personal or sensitive data to your home PC or a mobile device, remove it completely once it is no longer needed.
- Do not email sensitive information unless you know it is encrypted. Talk to IT Support for advice.
- Printed documents containing personal or sensitive data must be kept secure and disposed of correctly when no longer needed.

Passwords

- Always log out, or "lock" the screen when leaving your computer unattended.
- 'Strong' passwords should be used – don't use simple or obvious passwords.
- Never share passwords with others, never tell your password to anyone.
- Never write passwords down.
- Don't use work passwords for personal online accounts.
- Don't save passwords in web browsers.
- Never use your username as a password.

Equipment Security

- IT equipment issued to staff remains the responsibility of that individual at all times - they must never be “loaned” to another individual (including family members).
- Laptops and all other mobile devices (e.g. memory sticks) used for personal data must be encrypted and kept secure at all times.
- All staff laptops must connect to the school's network at least once each ½ term to allow for software and anti-virus updates.
- Leave school devices and school laptops behind if you travel abroad (some countries restrict or prohibit encryption technologies.)

Other Good Practice

- Beware of people watching as you enter passwords or view sensitive information.
- Always store equipment securely.
- Always keep remote access tokens/dual-factor login fob separately from your laptop.
- Don't leave equipment unattended in an unsecure location.
- Don't use public wireless hotspots to access personal or sensitive data.