Security of Computerised Personal Information

The GDPR and Data Protection Act 2018 requires Data Controllers (the people or organisations who hold and use personal information) to have in place adequate security measures to prevent unauthorised access, alteration or disclosure of personal information and to guard against its deliberate or accidental loss or destruction.

The responsibility for personal data held by schools extends to all work undertaken on behalf of the school by employees whether office based, mobile or home based.

Here are some good practice guidelines:

Passwords

- Your computer should be password protected to ensure that only those with authorisation can gain access to the system. If the system does not prompt the user to change their password on a regular basis then staff should be reminded and trained to change their own.
- To minimise security risks do not share your password with colleagues or members of your household.
- Passwords should be alpha numeric (use a combination of letters and numbers).

Access Levels

- Access to computer facilities must be controlled. Such access must be restricted to authorised users only.
- Levels of access should be assessed on a 'need to know' basis.
- Regularly review the levels of access of authorised users to ensure that they only have access to the correct / necessary information to enable them to carry out their duties.
- All users are expected to take necessary precautions to prevent unauthorised access to their accounts.

Log-out / shut down

- In order to prevent unauthorised access to school systems, a computer should be shut down when the work area is to be left unattended for any length of time.
- When a computer or information is left unattended, doors / windows must be secured.
- After use completely close the Internet Explorer and any additional open screens.

Records Management

- All users must ensure that the information they hold is kept up-to-date and is accurate. There should be a process in place to regularly review the details that they hold, perhaps annually.
- Do not keep the records for longer than is necessary. Please refer to the Information Management Toolkit for Schools.

Personal computers

- Personal computers (or laptops) should only be used to process personal data, if they have up to date virus protection software installed.
- Do not store your automated password on the computer and do not tick the 'remember my password' prompt.

- No other members of your household should have access to the computer or the information contained on it.
- Any documents produced should be stored onto disc or memory sticks and not to the hard drive.

Old computer accounts

- Any computers or laptops that are returned should be cleaned of old data prior to disposal or re-use. Here are some suggestions based on the perceived security risk if the data on the disk was compromised:

  High Risk - Remove Hard Drive (HD) and Destroy; replace with new disk reinstall OS and Applications
  Medium Risk - Format HD reinstall OS and Applications
  Low Risk - Delete Files and remove from Recycle Bin.

- When a user leaves, their account should be deleted to prevent a breach of confidentiality. If the data is stored on a secure server then folders can either be archived or deleted depending on relevant data retention policies. If on a mobile device then follow the process referred to above.

Servers

- You must ensure the physical security of the servers from any outside interference, by locating the server in a secure area with restricted access.

For more information on data protection, please contact the KCC Information Resilience & Transparency Team at the following email address: informationgovernance@kent.gov.uk