Information Security

Following the recent security breach by HMRC the Information Commissioner has reminded us of the need to protect personal data and to be able to access risk in relation to this.

Richard Thomas stated:

"The alarm bells must now ring in every organisation about the risks of not protecting people's personal information properly. As I highlighted earlier this year (in my annual report), it is imperative that organisations earn public trust and confidence by addressing security and other data protection safeguards with the utmost vigour.

Recent research commissioned by the ICO showed that people now consider protecting their personal information as the second most socially important issue above the NHS, national security and environmental issues."

Information security is an integral part of the Data Protection Act 1998. You must take all reasonable steps to ensure that any personal information that you are processing is securely stored.

Here are some guidelines to bear in mind when considering information security:

1. Transfer of disks containing personal data – some do's & don'ts:

- Unless it is absolutely necessary, don't do it.
- Do you have the consent of the data subjects and have you informed the data subject what this data being used for?
- If personal data is to be copied to disk a senior member of staff should carry this out.
- Is the information encrypted or at least password protected?
- Ensure that the recipient will treat the information with the appropriate care once they have received it.
- Disks should not be put in the post but must either be sent by a trustworthy courier service or a member of staff should travel with them and hand them to the person they are going to.
- The envelope the disk travels in should be secured and marked confidential and this delivery should require signed proof of receipt.
- The recipient must guarantee that the information is securely disposed of at the end of its use.

2. All paper-based personal information should be kept in lockable filing cabinets, which are kept locked when the room is unattended. Personal information should not be left on your desk where anyone could see it. You might need to consider restricting access to offices in which personal information is being worked on or stored.

3. If you are "archiving" information somewhere else in your own building (or in an outbuilding) make sure that the door can be locked and that the key is kept locked away. Anyone accessing the room should sign for the key. Where possible, there should be a file tracking system where anyone borrowing items from the "archive" room must make a note of what they have taken.

4. Personal information held on computer systems should be adequately password protected. Information should never be left up on a screen if the computer is unattended. Make sure that you don't have shared passwords to systems (or share personal passwords with other members of staff) and that all members of staff log off the computer when it is left unattended.

5. Where possible personal information should not be sent by e-mail, as its security cannot be guaranteed. Never send personal information in the text of an e-mail; if necessary make sure that the information is in a MS Word document attached to the e-mail.

6. When sending personal information by fax ensure the fax machine you are sending it to is a "safe haven" one (a fax machine in a secure or constantly manned area). If it isn't the personal data must be removed before sending.

7. When sending land-mail through either the internal or external postal system make sure that the information is in a sealed envelope. If sending personal data externally it should be sent using the registered postal service, which means it must be signed for and that there is an audit trail to trace its whereabouts.

8. When using children or other members of staff to transport personal information around the school make sure that the information is in a sealed envelope or file.

9. If files need to be taken off the premises they should be secured in a lockable box or briefcase and put in the boot of the car. Any items containing personal information (e.g. laptops, PDAs, briefcases etc) should not be left in a car on open view.

   Records should not be left in the boot of a car overnight or for any extended period of time. Once you have taken the records from the car please make sure that they are not left on general access in your home. Put them out of sight in a secure environment.

10. If using a home computer (or laptop) to process personal information ensure you have up-to-date virus protection software installed. 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 disk and not to the hard drive.

11. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing. If the request is urgent take the callers name and switchboard telephone number and verify their details before responding.

12. Do not discuss other people's personal business in public areas where conversations can be overheard by people with no right to know the details of the information.

13. Document how any transfer of personal data is made and where applicable obtain a signature upon dispatch and receipt.

If there was a breach of the legislation and the data holder was found to be negligent the Information Commissioner has the power to impose fines or enforcement action on the school.