

# INFORMATION SECURITY GUIDANCE FOR SCHOOLS

The recent high-level security breaches concerning the loss of personal and sensitive information have highlighted the need for information security guidance.

Schools should review their “security policy” to ensure that it covers how personal information is stored, transmitted and protected.

**Personal data** is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. In a school context this will include eg **names, contact details, gender, dates of birth, behaviour, academic achievements** as well as other sensitive information eg religious beliefs, physical and mental conditions and racial or ethnic origins.

It is therefore important that you:

- Treat personal data with care and remember that you have a duty of confidentiality towards the Data Subject. All paper copies of personal information should be kept in a locked filing cabinet or cupboard which should only be accessed by authorised personnel on a need to know basis.
- Where personal information is requested under the Data Protection Act 1998, check the identity of the requestor before releasing such information.
- Only disclose personal information to those authorised in your Data Protection notification to the Information Commissioner.
- Ensure that personal data is not left on your desk in view of others – lock it away when not in use.
- Logoff/Lock PC's/Laptops while you are away from them for lengthy periods.
- Ensure that your PC/Laptop is “password protected”
- Do not share your Logon with any other person.
- Don't tell anyone else your “password”.
- Ensure no one else, especially pupils or members of the public, can read information from your computer screen. No one should be able to view data without authorisation.
- Do not store personal data on removable media (eg USB stick, CD ROM, unless authorised by the Principal.
- Do not remove personal data (removable media/laptop/file) from school premises unless authorised by the Principal.
- Don't use unauthorised software on your PC/Laptop.
- Ensure there is no unauthorised access to the Server Room, which should be locked.
- Back-up media should be kept in a secure storage area.
- If in doubt, seek further advice.