Guidelines

This guideline offers an overview of what the Data Protection Act requires in terms of information security and aims to help you decide how to manage the security of the personal data you hold. It cannot provide a complete guide to all aspects of security but can help identify the main points. **There is no “one size fits all” solution to information security. The security measures that are appropriate for your school will depend on its circumstances, so you should adopt a risk-based approach to deciding what level of security you need.**

The Data Protection Act says that:

“Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.” This is the seventh data protection principle.

In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:

- Organize your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- Be clear about who in your school is responsible for ensuring information security.
- Make sure you have the right physical and technical security, backed up by robust policies and procedures.
- Be ready to respond to any breach of security swiftly and effectively. Schools should check that any existing measures or controls they have in place are actually working. Failing measures or controls do not reduce risk.

Advances in technology have enabled schools to process more and more personal data, and to share information more easily. This has obvious benefits if schools collect and share personal data in accordance with the data protection principles, but it also gives rise to equally obvious security risks.

The more databases that are set up and the more information exchanged, the greater the risk that the information will be lost, corrupted or misused. If personal data is not properly safeguarded, this can seriously damage a school’s reputation and can compromise the safety of individuals. The school must understand what information it needs to handle, how the information changes over time, who else is able to use it and why.

It is important to understand that the requirements of the Data Protection Act go beyond the way information is stored or transmitted. The seventh data protection principle relates to the security of every aspect of your processing of personal data.

So the security measures you put in place should seek to ensure that:

- Only authorized people can access, alter, disclose or destroy personal information;
- People only act within the scope of their authority; and
- If personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any
damage or distress to the individuals concerned.

- Information is not kept for longer than necessary. Refer to the School Disposal and Record Retention Schedule, published by DE  [http://www.deni.gov.uk](http://www.deni.gov.uk)

The Data Protection Act says you should have security that is appropriate to:

- the nature of the information in question; and
- the harm that might result from its improper use, or from its accidental loss or destruction.

The DPA does not define “appropriate”. But it does say that an assessment of the appropriate security measures in a particular case should consider technological developments and the costs involved. The Act does not require you to have state-of-the-art security technology to protect the personal data you hold, but you should regularly review your security arrangements as technology advances. Again there is no “one size fits all” solution to information security, and the level of security you choose should depend on the risks to your school.

So, before deciding what information security measures you need to take, you should assess your information risk: you should review the personal data you hold and the way you use it to assess how valuable, sensitive or confidential it is, and what damage or distress could be caused to individuals if there were a security breach.

**Example**

A school holds highly sensitive or confidential personal data (such as information about pupils and their family circumstances) which could cause damage or distress to those individuals if it fell into the hands of others. The school’s information security measures should focus on any potential threat to the information.

This risk assessment should take account of factors such as:

- Nature of the school premises and computer systems;
- Number of staff;
- Extent of their access to personal data; and
- Personal data held or used by a third party on your behalf. (You are responsible for ensuring that any data processor you employ also has appropriate security).

Unless there is clear accountability in your school for handling and safeguarding information security will probably be overlooked and your procedures will quickly become out of date.

**Carrying out an Information Risk Assessment**

Schools should carry out an information risk assessment to help them to manage information risks effectively. A good risk assessment will establish what security measures they already have in place and whether they are the most appropriate (and cost effective) available.

Conducting an information risk assessment is broadly similar to any other kinds of risk assessment. In general carrying out any risk assessment involves:
• recognising which risks are present
• judging the size of the risks
• prioritising the risks

Once the school has assessed the risks, they can decide how to reduce them or accept them as they stand. Risk assessment is an ongoing process, particularly as risks change as threats evolve over time.

Staff
It is vital that all staff understand the importance of protecting personal data; that they are familiar with your schools procedures on handling information and that they put it into practice. You need to provide appropriate initial and refresher training, and this should cover:

• How to handle requests for information e.g. Freedom of Information, Data Protection and educational records under the control of the Head Teacher.
• Compliance under DPA and restrictions on the use of personal data;
• Responsibilities of individual staff members for protecting personal data, including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority;
• Procedures to use to identify callers;
• The dangers of people trying to obtain personal data by deception (for example, by pretending to be the person whom the information is about or by making *phishing attacks) or by persuading you to alter information when you should not do so;
• Any restrictions you places on the personal use of computers by staff (to avoid, for example, virus infection or spam).

*Phishing is a way of attempting to acquire information by pretending to be a trustworthy source in an electronic communication.

Physical Security

Technical security measures to protect computerized information are of obvious importance. However, many security incidents relate to the theft or loss of equipment, or to old computers or hard-copy records being abandoned.

Physical security includes things like the quality of doors and locks, and whether premises are protected by alarms, security lighting or CCTV. However, it also includes how you control access to premises, supervise visitors, dispose of paper waste, and keep portable equipment secure. If you have staff who work from home, you should put measures in place to ensure that this does not compromise security.

Important ‘Dos’

• Make sure staff are aware of the legislation and understand their obligations under the law.
• Encourage your colleagues to follow good practice and guidance.
• Issue staff with relevant guidance documents and policies. You can use information published on Teachers section of belb web site [http://www.belb.org.uk/](http://www.belb.org.uk/)
• Remember, requests must be made in writing.
• If a request for personal information is received from a police officer, unless it is an emergency situation, you should ask for the request to be made on a Form 81, (See the DPA guidance for schools published on the teachers section of the board’s web site)
• Become more security aware- report and evaluate any incidents.
• Keep a record of all information you disclose (e.g. responding to subject access requests) - Good idea to have an audit trail of disclosures.
• Be aware of obligations in respect of the common law duty of confidentiality.
• Be especially aware of the implications of the Human Rights Act and how this may limit a schools ability to disclose personal information. Seek advice.
• If you use another organisation (third party) to do something with personal information for which the school is the data controller, consider getting assurances in writing on how they will handle the information. Remember, the school principal and the board of governors are accountable for any breach of the DPA by a third party where the school is not able to demonstrate that proper assurances were obtained at the beginning and managed throughout. Example- using an external text messaging system to contact patents. (guidance available belb)
• The same principle applies if you are asked to provide personal information to an organisation or academic researcher. You should consider some sort of “Agreement to Conduct Research” where both sides are clear on what the information will be used for and how it will be handled etc.

**Example**

As part of its security measures, a school ensures that the information on laptop computers issued to staff is protected by encryption, and that desk-top computer screens in its offices are positioned so that they cannot be viewed by casual passers-by. Paper waste is collected in secure bins and is shredded/ disposed of securely.

If, despite the security measures you take to protect the personal data you hold, a breach of security occurs, it is important that you deal with the security breach effectively. The breach may arise from a theft, a deliberate attack on your systems, from the unauthorized use of personal data by a member of staff, or from accidental loss or equipment failure. However the breach occurs, you must respond to and manage the incident appropriately.

There are four important elements to any breach-management plan:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.

2. Assessing the risks – you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.
3. Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. You should be clear about who needs to be notified and why.

4. Evaluation and response – it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it.

Additional Points

Personal information 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 e.g. names, contact details, gender, dates of birth, behaviour, academic achievements as well as other sensitive information e.g. religious beliefs, physical and mental conditions and racial or ethnic origins.

It is therefore important that you:

• Treat personal data with care; remember that you have a duty of confidentiality.

• 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, (subject access request) 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 desks etc 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. (Unless required for work purposes)

• 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 (e.g. 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.
• Try to prevent people from watching you enter passwords or view sensitive information

• Do not leave your laptop unattended unless you trust the physical security in place.

• Do not let strangers or unauthorised people into staff areas unless supervised.

• Position screens where they can be read from outside the room (window)

• Ensure only authorised staff are allowed to remove data from the school’s premises.

• **Posting** sensitive information, Check the quality of the envelope. Use an inner envelope if necessary. This means that people can’t see from the outside that the envelope contains sensitive information

• Be aware of who you are allowed to share information with. Ask third parties how they will protect sensitive information once it has been passed to them

**E- Mail**

• Don’t send sensitive information by email unless it is encrypted.

• Use your school’s contacts or address book. This helps to stop email being sent to the wrong address

• Only use your school email account for any school business (this is secure), not a personal account such as Yahoo or Hotmail. Remember an e mail is like a post card, any one can read it.

• When sending an email put a security classification in the first line of the email. For emails to do with information about a pupil, e.g. you should put in **PROTECT – PERSONAL** on the first line of the email. The name of the individual is not to be included in the subject line and the document containing the information is encrypted. This provides additional security.

• Be wary of links to websites in emails, especially if the email is unsolicited.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. The ICO's new powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner’s office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The DPA laws can be complex and until they are tested in Courts there is a need to make judgements on the best course of action in any particular case. If in any doubt, please seek advice.

I hope this is useful. Liz Johnston BELB December 2011.