

Information Security

Policy and Guidance for Schools

Helping you safeguard Council, School and Pupil
information and ICT equipment

Rationale

Several high profile instances of data loss have been reported in the press recently and as a result organisations are tightening up their procedures for handling personal and confidential data to prevent any further occurrences.

Most recently Leicester City Council was found to be in breach of the Data Protection Act by the Information Commissioner's Office (ICO) after staff downloaded personal information onto an unencrypted memory stick. The sensitive personal information relating to 80 children was subsequently lost from a council-run nursery.

This applies equally to schools and school staff with access to such data – indeed, it is currently common practice for school staff to have personal and confidential information about pupils, staff or parents on their personal laptops, home computers, USB memory sticks and other media. Generally, that data is not held securely and these guidelines are provided to help schools tighten up their own procedures.

In September 2008 Becta produced a substantial guidance document; [Good Practice in information handling in schools; Keeping data secure, safe and legal](#) The underlying principle of the guidance is that schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

Introduction

This document summarises what is expected of all school staff in the course of their duties in relation to information security and computer equipment. It is the first in a series of guidance documents.

Its aim is to protect:

- staff, pupils, parents and visitors;
- assets, including information assets;
- the school's finances and reputation

by reducing the risk of:

- harm to individuals
- accidental loss or damage to assets
- unintended change to, or disclosure of, personal and confidential information
- deliberate and harmful acts carried out through lack of awareness of their consequences.

It applies to:

- all services in the school
- all employees of the school, both permanent and temporary
- pupils
- any other person working for the school or on school premises.

Roles and Responsibilities

All members of the school community have a shared responsibility to secure any sensitive or personal data used in day-to-day professional duties.

Important 'dos'

- make sure you and your colleagues are adequately trained
- follow guidance
- become more security aware
- raise any security concerns
- encourage your colleagues to follow good practice and guidance
- report incidents.

Why protect information?

The Data Protection Act 1998 places a duty on organisations (including schools) to protect the personal data they hold on individuals. Further guidance can be found on the GoWild website in the (click here) [Data Protection guidance](#) area :

www.gowild.org.uk/ManagementAdviceAndGuidance/OrganisationAndManagement/DataProtectionAct/default.htm

Schools are required to hold personal data on learners, staff and other people to help them conduct their day-to-day activities. If this data is not held securely and falls into the wrong hands it could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data could result in adverse media coverage, and potentially damage the reputation of your school. This can make it more difficult for your school to use technology to benefit learners.

What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your school. Under the Data Protection Act the Head Teacher (referred to as Data Controller) is ultimately responsible for ensuring that the requirements of the Act are applied within their school, but all staff share responsibility for the protection of that data.

What is sensitive data?

Information relating to an individual's:

- Safeguarding information
- Special education needs
- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade Union membership
- Physical, mental health or condition
- Sexual life
- Criminal record

Two roles have been highlighted that have responsibility for information Security. Schools should look to appoint a senior member of staff to take the role of Senior Information Risk Owner.

Senior Information Risk Owner (SIRO)

Although the Head Teacher is responsible as the Data Controller they may wish to nominate a member of the senior leadership team to act as Senior Information Risk Owner (SIRO) Typically, the SIRO should have the following responsibilities:

:

- They own the information risk policy and risk Assessment
- They appoint the Information Assess Owners (IAOs)
- They act as an advocate for information risk management.

The Office of Public Sector Information has produced Managing Information Risk (<http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf>) to support SIROs in their role.

Information Asset Owner

Organisation should identify their information assets. These will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Information assets also include non-personal data that could be considered sensitive if lost or corrupted, such as financial data, commercial data, research data, organisational and operational data, and correspondence.

The 'value' of an asset is determined by considering the consequences likely to occur if it is lost or compromised in anyway, such as identity theft, adverse publicity or breaches of statutory/legal obligations.

An information asset is regarded as the collection of data or an entire data set. It is important to distinguish between an information asset and the information (usually a subset of the asset) that needs protecting. For example, reports run from a core information asset, such as a management information system, are not information assets themselves.

Organisations should then identify an Information Asset Owner (IAO) for each asset or group of assets as appropriate. For example, the organisation's management information system should be identified as an asset and should have an IAO.

The role of an IAO is to understand:

- what information is held, and for what purposes
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. Typically, there may be several IAOs within an institution, whose roles may currently be those of e-safety co-ordinator, ICT manager or information management systems manager.

Although we have explicitly identified these roles, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Protective Marking

The Government recommends that the “Protective Marking Scheme” is used to indicate the sensitivity of data.

Most learner or staff personal data that is used within educational institutions will come under the PROTECT classification.

Becta are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and are working with suppliers to find ways of automatically marking reports and printouts. **Further guidance will be published when available.**

Steps you can take to help prevent security problems

There are many steps that you should take (or not take) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these 'dos and don'ts' will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

Working online

Do

- make sure that you follow your organisation's policies on keeping your computers up to date with the latest security updates. You should also keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (eg anti-virus, anti-spyware and Microsoft security updates). Get advice from your ICT support service if you need help.
- only visit websites that are appropriate to access within organisation. Remember your organisation may monitor and record the websites you visit.
- check that your organisation has an acceptable-use policy for the internet use and ensure that you follow it.
- turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)
- make sure that you only install software that your ICT support service has checked and approved
- be wary of links to websites in emails, especially if the email is unsolicited
- only download files or programs from sources you trust. If in doubt, talk to your ICT support service.

Email and messaging

Do

- read your organisation's email policy
- ensure that all staff only use an official school email account for any work purpose
- report any spam or phishing¹ emails to your ICT support service that are not blocked or filtered
- report phishing emails to the organisation they are supposedly from
- use your contacts or address book. This helps to stop email being sent to the wrong address.

Don't

- click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on. Never reveal your password to anyone not even official bank or credit card employees.
- turn off any email security measures that your ICT support service has put in place or recommended
- email sensitive information unless you know it is encrypted². Talk to your ICT support service for advice.
- try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account)
- reply to chain emails or pass on.

¹ Phishing is an attempt to obtain your personal information (for example, account details) by sending you an email that appears to be from a trusted source (for example, your bank)

² Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it. There are many different types of encryption software and devices; you should consult your ICT support provider before purchase or use.

Passwords

Do

- follow your organisation's password policy (you should also have a separate policy on pupil/student passwords)
- use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- make your password easy to remember, but hard to guess
- choose a password that is quick to type
- use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password.
- change your password(s) if you think someone may have found out what they are.

Don't

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message.

Laptops

Do

- shut down your laptop using the 'Shut Down' or 'Turn Off' option
- try to prevent people from watching you enter passwords or view sensitive information
- lock your desktop when leaving your laptop unattended.
- turn off and store your laptop securely (eg if travelling, use your hotel's safe)
- if you are in a vulnerable location use a physical laptop lock to prevent theft
- Avoid having sensitive data on a laptop, if you need to transport it use an encrypted pen drive (memory stick). Encryption of laptops is not recommended at this time and further work is being done on this. If travelling abroad seek further guidance from your SIRO or ICT support service.

Don't

- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots to access sensitive data – they are not secure
- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- let unauthorised people use your laptop
- use hibernate or standby.
- store remote access tokens (eg for secure access to your schools network) with your laptop

Sending and sharing

Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure.
- ask third parties how they will protect sensitive information once it has been passed to them and seek a signed agreement from them.
- encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier. See your ICT support service for advice. Encrypted USB Pen drives can be purchased through EdIT.

Don't

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- send sensitive information by email unless it is encrypted
- place protective labels (ie CONFIDENTIAL,) on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.
- assume that third-party organisations know how your information should be protected.

Working in school

Do

- lock sensitive information away when left unattended
- use a lock for your laptop to help prevent opportunistic theft.

Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read by others in the room or from outside the room.

Working outside school

Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- wherever possible access data remotely instead of taking it off-site
- Use your personal files storage area on the Learning Platform (only you have access to this) to reduce risk associated with loss of pen drives.
- be aware of your location and take appropriate action to reduce the risk of theft
- if you use WiFi or public internet PCs make sure you sign out / log out completely from any services you have used and make sure the internet browser is closed down – don't rely on just switching off the PC
- try to reduce the risk of people looking at what you are working with
- be aware of greater security risks on foreign travel – if you don't really need your laptop then don't take it with you

If data or equipment is lost or stolen

Do

- Report the incident immediately to your SIRO
- If theft has occurred report this to the local police.
- Complete a theft or data loss advice form (see example)

Further help and support

Your organisation has a legal obligation to protect personal information. Your senior management should be aware of their legal obligations under the Data Protection Act 1998. For more information, visit the website of the Information Commissioner's Office <http://www.ico.gov.uk>.

More detailed guidance for organisations can be found on the Becta website

Plan for sustainable success <http://www.becta.org.uk/plansustainableuccess>

e-Safety <http://schools.becta.org.uk/index.php?section=is>

Data handling security guidance for schools
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

Test your online safety skills at the Get Safe Online website

<http://www.getsafeonline.org>

More information on roles and responsibilities will be published at

<http://www.gowild.org.uk/ManagementAdviceAndGuidance/OrganisationAndManagement/default.htm>

For further information on securing your computer or safe guarding your data you may need to contact your ICT support support service.

Appendix A – Security Incident Reporting

Details of Person Reporting: Name _____
Contact Number _____
Date of Report _____
Signature _____

Type of Occurrence:

- a) An issue that could occur in the future which needs to be highlighted as a possible security problem. a)
- b) An incident (breach of security), which has actually occurred. b)
- (Please mark relevant box)

Details of Issue/Incident

Details of Action Taken

To be completed by SIRO:

Incident/Issue No:

Date updated by SIRO: _____

Appendix B – Report of Loss or Theft

Removable Device Loss Security Incident Form

Please record the loss of any device (ie laptop, USB memory stick, cd etc) which potentially holds sensitive or personal information.

Date lost or stolen

Type of device lost

(e.g. laptop, phone, USB drive).

Please include as much detail as possible, e.g. make and model, serial number.

Circumstances of loss/theft

Date/Time loss reported

Who was it reported to

(if reported to the police include crime reference number)

Was the device or data encrypted

Details of types of information stored on the device

This should include office files (such as Word/Excel), databases, phone numbers or e-mails. Individual files, emails etc need not be mentioned at this stage unless they are particularly sensitive (eg safeguarding information).

Is there any information on the device that could be considered as confidential, that could cause embarrassment to the school, aid criminal activity or lead to individuals or other bodies taking legal action against the school? Detail any information of this kind.

What actions have been taken at this point to attempt to recover the device

Have the police or any other external bodies been informed of this loss

Please provide any other information which may be relevant