Information and Data Security in Schools

Guidance for all school staff and governors

Revision	Date	Author	Approved by
V1.0	19th November 2008	L Hornsby	
V2.0	18 February 2010.	Maria Bannister	
V3.0	18th March 2010	Maria Bannister	

1.0 INTRODUCTION

Recent losses of personal and sensitive information have highlighted an urgent need to improve existing security practices. The Cabinet Office report, Data Handling Procedures in Government, published in June 2008, stipulates in detail the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that these procedures are adopted by educational institutions too.

Data protection legislation requires personal data, whether on paper or electronically, to be kept secure. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth and so on, as well as other sensitive information such as academic achievements, other skills and abilities, and progress in school. It may also include behaviour and attendance records.

2.0 SCOPE OF THE POLICY

2.1 The objectives of this policy are to ensure:

- the protection of confidentiality, integrity and availability of school information and assets.
- that users are aware of and fully comply with all relevant legislation.
- all staff understand the need for information and ICT security and their responsibilities in this respect.

2.2 The policy applies to all schools within the borough of Knowsley. Head Teachers and Governors are responsible for implementing the policy and ensuring compliance.

3.0 DEFINITION OF INFORMATION AND DATA

This covers any information and/or data, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created. Organisations hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this data 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 reputational damage and potentially legal action and sanction. This can make it

more difficult for your organisation to use technology to benefit learners. Each member of your organisation has a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

It is important that,

- guidance is followed
- staff become aware of the need for vigilance and security
- concerns are raised, discussed and addressed
- good practice is common place
- incidents are reported, recorded and acted upon.

3.1 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 organisation. Your organisation should have someone who is responsible for working out exactly what information needs to be secured. This person is your Information Asset Owner. They should understand what information you need to handle, how the information changes over time, who else is able to use it and why. Several people may share this role if you work in a large organisation.

Make sure that you follow policy on keeping your computers up to date with the latest security updates. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). It is also important that only authorised software is installed on devices. Get advice from your IT team if you need help – never turn off or bypass security systems installed on devices.

3.2 Passwords

Passwords are important in protecting information. Knowsley has implemented a complex password process which supports improved security. However, it is important that passwords are easy to remember but hard to guess. It is good practice to have a password that has eight characters or more and contain upper and lower case letters, as well as numbers. Never share your passwords with anyone else, write it down, use work passwords for personal on line accounts or save passwords in web browers. Never email as password.

3.3 Laptops

Laptops are increasingly becoming a part of working toolkits. It is essential that the devices and the information they contain are adequately protected. It is always good practise to store information on a secure central server rather than locally. This provides security and also provides protection in the case of device failure. Laptops and other devices which provide similar functionality (i.e. notebooks, UMPCs etc) are by design portable and in some cases easy to conceal increasing the risk of theft. It is therefore important that the hard drives are encrypted and additionally that are secured using a visible security lock when they are in use.

Always:

- 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
- turn off and store your laptop securely (if travelling, use your hotel's safe)
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop unattended
- make sure your laptop is protected with encryption software.

It is important that when working on sensitive data take precautions that other people cannot see the screen.

Never:

- store remote access tokens with your laptop
- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots – 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.

3.4 Sharing Information

Be aware and follow guidance on who you are allowed to share information with and how you can do it securely.

Never:

- 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 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.

3.5 Working on-site

Always:

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

Never

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

3.6 Working off-site

- 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
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used
- try to reduce the risk of people looking at what you are working with

3.7 Information Asset Owner (IAO)

Organisations 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.

3.8 Recommended considerations and changes:

To adequately protect data, organisations may need to make operational and technological changes. Some can be accomplished quickly with existing resources; others will require extra investment and the help of ICT and managed service suppliers. In any given organisation, Information Asset Owners will need to work out the level of change required by carrying out a thorough information risk assessment. Organisations may also need to make staff more aware of data security with training. They may also need to put in place systems and procedures for:

- protectively marking data
- encryption
- responding to security incidents
- secure remote access (using two-factor authentication where needed)

Further information can be found in the ICT Usage Policy, eMail Policy and Acceptable Use Policy.

3.9 Device Configuration

All devices connected to the network must be configured in accordance with technical standards discussed at the Operations Board and approved by LTSB.

3.10 Email as records

Where staff are provided with an approved email address in the format of "@knowsley.gov.uk" or "@staff.klear.org.uk" these must be used to conduct official business.

Non approved email accounts must not be used to conduct official business. All emails that represent aspects of official business are the property of the business and not the individual.

Don't make the mistake of thinking your emails are private – they are not. You should never include any information in an email that you wouldn't want published on the front page of your local newspaper! In other words, never send confidential, proprietary, sensitive, personal or classified information through email unless the email has appropriate security in place, such as encryption software. If you need to use encryption software contact the IT Service Desk.

Link to the KMBC policy:
KMBC Email Policy

4.0 DATA ENCRYPTION

To comply with the intent of data handling procedures and practice in Government:

- Users should not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely for storage in a secure location.
- Authorised users accessing data from outside the school premises must do so by secure access
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

For schools, this means that they must encrypt any data that is classified as Impact Level 2 (IL2–Protect) or higher if this data is removed or accessed from outside any approved secure space.

In order to comply with the intent of Data Handling Procedures in Government, it is essential that a holistic approach is taken to security. Encryption does not work in isolation, awareness of the sensitivity of data, whether electronic or on paper, must be part of every school's duty of care to staff and pupils.

Data should, by default, be stored on a networked or shared disk drive or portal where it will be backed up and covered by disaster recovery processes. If there is a need for offline access to any data containing personal, confidential and/or sensitive data and it is to be held on the local disk drive (C:/) of a PC or tablet PC, permission from the Headteacher must be obtained and the data **must** be stored in an encrypted folder. Instructions on how to create an encrypted folder are available here.

Portable storage devices (such as USB disks, pen drives, CDs, etc) **must not** be used for the storage of personal, confidential and/or sensitive data.

4.1 USB Portable Drives:

The recommended approach for encryption on USB portable drives is to purchase drives that are FIPS 140-2 certified. The following are widely available:

- Eclypt PICO Freedom (FIPS 140-2 Validated)
- IronKey (all variants)
- KanguruMicro Drive
- Kingston DataTraveler BlackBox
- SanDisk Cruzer (Enterprise FIPS edition)
- Stealth MXP.

It is also necessary to support this with policies or tools to prevent users from using other (unencrypted) USB portable drives.

5.0 DATA DESTRUCTION

When the need arises to destroy any printed or written documents containing personal, confidential and/or sensitive data, measures must be taken to ensure that the information cannot be accessed by unauthorised parties in the future. Under no circumstances should

personal, confidential and/or sensitive data be placed in general waste or recycling bins, cross-cut shredders or confidential waste bins must be used for this type of data.

A process has been agreed for the disposal of ICT equipment which covers the secure removal of personal, confidential and/or sensitive data. The details of this process are available here.

6.0 LEGISLATION

Data Protection Act - regulates the storage of personal information (i.e. any information that can be identified as relating to a particular person or person(s) on computer systems. Before storing any such information on the School computer system, you must notify the School Data Protection Officer in writing. It is everyone's responsibility to ensure that any such information complies with the law. For more information regarding Data Protection see http://www.dataprotection.gov.uk.

Freedom of Information Act - The Freedom of Information Act deals with access to official information. In addition there are also regulations which provide access to environmental information. These are known as the Environmental Information Regulations.

The Freedom of Information Act applies to most public authorities. It also applies to companies which are wholly owned by public authorities.

The Act gives the public a general right of access to information held by public authorities. Further details can be found at: http://www.ico.gov.uk/Home/what_we_cover/freedom_of_information/guidance.aspx#proguidance.

7.0 SECURITY AND DISCLOSURE TO THIRD PARTIES

Before sharing any personal, confidential and/or sensitive data with partner agencies care needs to be taken to ensure that the sharing is covered by the data protection registration for the data and that an information sharing agreement is in place between the Council and the partner agency.

If a request is received to transfer personal, confidential and/or sensitive data via any electronic means (including email, FTP and CD) the necessary encryption protocols need to be verified as in place. If in doubt contact the Schools Support helpdesk.

If a request is received to transfer printed or written personal, confidential and/or sensitive data ensure that appropriate security procedures are in place, ideally a point-to-point courier with tracking and a signed receipt by the intended recipient.

8.0 SECURITY INCIDENTS

All suspected or actual breaches of data security, must be reported to the Schools Information Officer and LA Information Manager.

9.0 REFERENCES

Becta Data protection and Security and Information Guidance for Schools – a summary for schools

http://publications.becta.org.uk/display.cfm (search on data protection)

DCSF Data processing and Sharing Guidance –

http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/

Knowsley MBC Data Security Guidance – http://knowit.kmbc/C3/C0/CORPORATE%20POLICIES%20AND%20PROCEDU/default.aspx

KMBC Email Policy – http://bertha.knowsley.gov.uk/Staff_Stuff/Your_job/HR%20Policies%20and%20Procedures/Section%203%20-%20Employment%20practices/Use%20of%20email%20guidance%20-%20employees.doc

10.0 FURTHER INFORMATION

Further information relating to the Data Protection Act and Freedom of Information Act can be obtained from:

The Information Commissioner: Web: www.ico.gov.uk