Tai Education Centre

Senior Leadership Team Guidance – Data Security in Schools

Senior Leadership Team Guidance – Data Security in Schools

Introduction

This document has been adapted from the Becta document ‘Data Security – Dos and Don’ts’as a guide for those undertaking the role of Network Manager Administrator within schools. The aim of this guide is to raise awareness on safe handling of data, data security and roles and responsibilities. Following these principles will help you to prevent information from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation your school might suffer if you lose sensitive information about individuals.

Your roles and responsibilities

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.

Important ‘Dos’

- make sure all staff are adequately trained
- issue staff with relevant guidance documents and policies
- follow guidance
- become more security aware
    - encrypting
    - labelling
    - transmitting
- raise any security concerns with your Senior Information Risk Owner
- encourage your colleagues to follow good practice and guidance
- report incidents to your Senior Information Risk Owner
- read the School Policy for ICT Acceptable Use

Why protect information?

- Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Who is responsible and what data handling changes are required?

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they own the information risk policy (strategies in place to identify and manage risks associated with information breaches) and risk assessment
- they appoint the Information Asset Owners (IAOs)
- they act as an advocate for information risk management

SIRO = Catherine Wicks

Information Asset Owner (IAO)

Schools 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.

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 coordinator, ICT manager or information management systems manager.

Although these roles have been explicitly identified, 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.

Storing/Transferring personal, sensitive, confidential or classified information using Removable Media

Do

- ensure removable media is purchased with encryption
- store all removable media securely
- securely dispose of removable media that may hold personal data
- encrypt all files containing personal, sensitive, confidential or classified data

- ensure hard drives from machines no longer in service are removed and stored securely or wiped clean
- ensure copies of data are securely stored and disposed of after use

Servers

Do

- always keep servers in a locked and secure environment
- limit access rights
- always password protect and lock the server
- ensure existing servers have security software installed appropriate to the machine’s specification
- ensure back up tapes are encrypted by appropriate software where possible
- ensure data is backed up regularly to avoid loss of data
- ensure back up media is securely stored in a fireproof container
- take occasional copies of back up media offsite to secure storage

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school’s systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

Do

- Ensure that all user accounts are disabled once the member of the school has left
- Ensure prompt action on disabling accounts to prevent unauthorized access
- Regularly change generic passwords to avoid unauthorized access (Microsoft© advise every 42 days)
- Further advice available http://www.itgovernance.co.uk/

Data Encryption

Full guidance can be found on the Becta website. **Becta Schools - Data handling security guidance for schools** or by visting http://www.becta.org.uk *

Please ensure that all removable media (e.g. laptops) used by staff containing sensitive or personal data have True crypt or similar software installed.

The True crypt software itself can be downloaded from: http://www.truecrypt.org/downloads.php

It is recommended that all USB memory drives are purchased with an encryption chip installed.

CC3 and CC4 workstations may be encrypted but users should be aware that there maybe some loss of management functionality.

Encrypting a whole hard drive with Truecrypt

Encrypting a hard drive stops unauthorised people from accessing any data contained on it. Other passwords and security methods, such as Windows logon passwords, are easily bypassed by anyone with physical access to the hard drive but encryption cannot realistically be circumvented; without the encryption key there is no way to access the data.

Encryption is a rather arcane technology but Truecrypt makes the encryption process as transparent and painless as possible. This guide will take you through the steps needed to protect your confidential data.

1. Download True crypt from http://www.truecrypt.org/downloads and run the setup program to install it. You will need administrator access to the PC to do this and an error will be displayed if you do not have this access.
2. Run True crypt from the desktop icon or the start menu and select Encrypt System Partition/Drive from the System menu. The Truecrypt Volume Creation Wizard will be displayed.
3. Ensure Normal is selected then click Next.
4. Ensure that Encrypt the whole drive is selected then click Next. Some combinations of hard drive partitions preclude encrypting the whole drive and an error message stating this will be displayed if this is the case. If this happens click Ok to close the error message and select Encrypt the Windows system partition.
5. Select No when asked whether to encrypt the host protected area. This will ensure we don't encrypt third-party drivers that may be needed for RAID or SCSI devices.
6. Select the correct response when asked whether there is a single or multiple operating systems on the drive. Almost all PCs will only have a single operating system installed.
7. Leave all the encryption options at their defaults and click Next.
8. Type the password you want to use to access the drive.
9. Move the mouse randomly inside the window for a minute or so to generate a random number pool.
10. Click Next at the Keys Generated screen.
11. Click Next to create the rescue disk image. This image is created in your My Documents folder and should now be written to a CD as a disk image (not just writing the iso file to the disk). If you have Nero installed, you should just be able to double click on the iso file in My Computer/Windows Explorer, to launch Nero and run the Burning process. Other CD burning software should have an option to burn a disk image. This rescue disk is the only way to regain access to your data if the boot sector of the hard drive is corrupted or overwritten by another program so should be labelled and stored in a safe place. Please note that rescue disks are only valid for the PC they were created from so you will not be able to use a rescue disk from another PC.
12. Insert the rescue disk into the drive and click Next to verify it, then click Next again to continue.
13. Ensure that None is selected for Wipe mode and click Next.
14. Click Next to reboot the PC and start the pre-test. This will write the boot loader to the disk and you will need to enter the password when the system boots but no encryption has been done at this stage. This step will test that the PC will still boot with the new boot loader before encrypting your data.
15. Once the PC has rebooted Truecrypt will run automatically unless you have security software installed that stops this (if it doesn’t start automatically run the program and it should pick up where it left off). Click Next to start the encryption process. This will probably take a couple of hours to complete but the PC can be used normally during this time and even shutdown; it will continue when it is turned on again.
16. Once completed click Finish to end the encryption process.
17.
18. Your hard drive is now encrypted and cannot be accessed without the password.

CC3 and CC4 stations can be encrypted but please consult with you ICT support provider regarding a change to restore functionality.

SITSS June 2009

Information for the MIS Administrator or Manager

SIMS Master Machines

Do

ensure newly installed master machines are encrypted, therefore password protecting data (all Master and Slave machines supplied by SITSS since Easter 2009 will be encrypted)

ensure existing master machines are encrypted where possible

ensure that back up logs are checked each morning to prevent data loss

remove back up media to secure fireproof storage regularly

keep off site back up media secure

Note - remote back ups taken by SITSS will be automatically securely encrypted

Don't

share passwords without checking authorisation

Transmitting personal data securely

All schools are required by the Data Protection Act to ensure that personal data is held and transmitted securely. Personal data is data about an identifiable individual. In a school, this would be about a pupil, a member of the school staff, a governor, etc. The Unique Pupil Number (UPN) counts as personal data.

Do

When schools (including Academies) or LAs send information about identifiable pupils or staff to each other or to the DCSF, it MUST be sent by a secure method:

from one school to another not in HCC, or between LAs, or from a school or LA to the DSCF, the s2s (School to School) service should be used

between two schools in HCC or between a school and HCC, s2s can be used

from a school to HCC s2s can be used but if a local secure system such as AVCO/AnyComms or Solero is available it should be used

between Academies, and between Academies and maintained schools, or from an Academy to HCC or the DCSF, the s2s service should be used

When a school contracts a third party to provide a service on the school's behalf then you are covered under your Data Protection registration to supply the data to the contracted organisation. However the method used to provide them with the data must be secure and meet UK DP standards.

In the case of SAM Learning, which is an LA contract, the method of transmitting the pupil data is secure.

Any third party companies that schools wish to enter into contract with must meet the DP standards of the school. For example they must:

guarantee the data will not go outside the EU

provide a secure mechanism by which the school can transmit the data to them

Work has been undertaken to lock down security between Lotus Notes (HCC) and the official school email domains (of the type "@<schoolname>.herts.sch.uk"). This has now been 'signed off' and was completed during the Spring Term 2010.

Don't

send encrypted or password-protected files via open email; a misdirected or intercepted email can be decrypted or a password broken

Further help and support

Your organisation has a legal obligation to protect sensitive 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 Commissioners Office [http://www.ico.gov.uk/].

Advice on esafety - http://www.thegrid.org.uk/eservices/safety/policies.shtml

* Full Becta guidance & documents are available at the link below

Data Handling Procedures in Government

HMG Security Policy Framework

Keeping data safe, secure and legal

Dos and Don'ts

Data encryption

Information risk management and protective markings

Audit logging and incident handling

Secure remote access

http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

Further guidance - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

Test your online safety skills [http://www.getsafeonline.org].

School’s toolkit is available - Record Management Society website - http://www.rms-gb.org.uk/resources/848

Acknowledgements

SSE, CSF, ICT Team

Becta

Cabinet Office

Information Commissioners Office

LGFL

Rob Halls, Deputy Head, Thomas Coram School

Record Management Society

Appendix 1

Information Risk Actions Form

(could be included in the ‘Register of Information Assets – Appendix 3)

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Appendix 2

This Policy in Brief can be issued to visitors, laminated and posted at workstations or used as appropriate by the school. Schools will need to customised to suit local arrangements.

School Policy in Brief (amend / delete < > as necessary)

- At this school we have a Acceptable Use policy which is reviewed at least annually, which all staff sign. Copies are kept on file. We use the LA model policy.
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors. We use the LA model agreements.
- Safe Handling of Data Guidance documents are issued to all members of the school who have access to sensitive or personal data.

Protect and Restricted material must be encrypted if the material is to be removed from the school.

- At this school we ... <encrypt flash drives / use automatically encrypted flash drives> for this purpose and limit such data removal.
- At this school we use <the DCSF S2S site> to securely transfer CTF pupil data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer, using <Outlook> <secure export to Local Authority Pupil Database>.

Protect and Restricted material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At this school we store such material in <lockable storage cabinets in a lockable storage area>.
- At ths school all servers are <in lockable locations and> managed by CRB-checked staff.
- At this school we use follow LA back-up procedures and <lock the tapes in a secure cabinet>. <Back-ups are encrypted>. <No back-up tapes leave the site on mobile devices.>
- At this school we use <protocol> for disaster recovery on our admin server.

Disposal: Protect and Restricted material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At this school we use the Authority's recommended current disposal firm <other named firm> for disposal of system harddrives where any protected or restricted data has been held.
- At this school paper based sensitive information is <shredded, using cross cut shredders>.
- <At this school we are using secure file deletion software>.
- Laptops used by staff at home (loaned by the school) where used for any protected data <are brought in and disposed of through the same procedure>. <From 2009 all laptops have been set-up with laptop hardrive encryption>.

- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, SLG and Learning Platform access are controlled by <the LA processes, supported by the LA ICT Support Service> and / or by <name /role>.

- Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation.

This should be regarded as work in progress and will be amended following national / regional advice (could include Risk Assessment information if desired – see Appendix 1)

Appendix 3: Protective Marking Scheme: Information Assets: Risk Assessment Information

Senior Information Risk Owner (SIRO):

			(named person)	(delete and change as appropriate)	
Data and information assets	**Impact Level (IL)**	**Data label**	**Information Asset Owner**	**Who has access to enter information**	**Purpose**
ContactPoint	IL3	Restricted		Head / SENCO	ECM/statutory returns
Pupil data (MIS)					
Core pupil data	IL2	Protect		Senior Admin Officer/office administrators	ECM/statutory returns
Attendance	IL2	Protect		Senior Admin Officer/office administrators / class teachers	ECM/statutory returns
SEN	IL2	Protect		SENCO/ Senior Admin Officer	ECM/statutory returns
EAL	IL2	Protect		EAL Lead	ECM/statutory returns
Exclusion, behaviour	IL2	Protect		SENCO/ Senior Admin Officer/ class teachers / Deputy	ECM/statutory returns
Reports and assessments	IL2	Protect		Class teachers / Pastoral tutor / Headteacher	ECM/statutory returns
Tagged (named) student photos	IL2	Protect		Senior Admin Officer/office administrators	Safety/security
Unique Pupil Number (UPN)	IL3	Restricted		Senior Admin Officer/office administrators	ECM/statutory returns
Child protection data	IL3	Restricted			ECM/statutory returns
Staff data (MIS)					
Core staff data sets	IL2	Protect		Senior Admin Officer/Bursar	ECM/statutory returns
Training and absence data	IL2	Protect		Senior Admin Officer/Bursar / Deputy headteacher	ECM/statutory returns
Finance system					
Purchase Orders, Invoices, Payments	IL2	Protect		Senior Admin Officer/Bursar	Sound financial management
Approvals and budget setting	IL2	Protect		Head	Sound financial management
Access control / passwords					
Network password lists	IL2	Protect		Network Manager	Access to system(s)
Learning Platform password information	IL2	Protect		School LMLE SuperUser administrator	Access to system(s)
Learning Platform password information	IL2	Protect		LP administrator	Access to system(s)
Disaster recovery contact system					
Parental messaging system information	IL2	Protect		Senior Admin Officer/ Head / Deputy	Business continuity/communication
Emergency mobile phone loaded with data	IL2	Protect		Head / Deputy / Senior Admin Officer	Business continuity/communication
Other potentially sensitive material					
Tagged (named) student photos	IL2	Protect		Class teachers / Network Manager	Teaching and learning
Learning Platform	IL2	Protect		Class teachers / LP SuperUsers	Teaching and learning
School website	IL2	Protect		Office administrator / web officer / Head	Business continuity/communication
Information sent to parents	IL1	Unclassified		Head / Deputy / Class teachers	Business continuity/communication
schools' other systems - specify					

Last updated:

Updated by: