CUSTOMER SERVICE EXCELLENCE

January 2010

DATA SECURITY SPECIAL

ScoMIS
Great Moor House
Bittern Road
Sowton
Exeter
EX2 7NL

Helpline and General Enquiries: 01392 385300

Course Enquiries: 01392 385301 or bookings@devon.gov.uk

Full Training Directory: www.devon.gov.uk/scomis-training

Fax: 01392 385302
Email: ScoMIS@devon.gov.uk
www.devon.gov.uk/scomis/

INVESTOR IN PEOPLE

SIMS Accredited Support

Devon County Council

Password Extra

The ScoMIS ICT Magazine

Last year I drew your attention to the work that was taking place in response to the Becta Data Security guidelines, “Good practice in information handling in schools - Keeping data secure, safe and legal” This work involved the production of :

- Electronic edition of Password
- Delivery of Security Workshops for schools
- Development of a Laptop Encryption Service
- Process for the disposal of ICT equipment.

I hoped to get this to you during the autumn term. However, we did decide that documentation, services and processes should not be finalised until after the Security Workshop sessions so that we could encompass concerns, comments and suggestions. It was also important that we spent time testing the Laptop Encryption Services in a number of different school situations with different computer operating systems.

The Security Workshops, jointly funded by ScoMIS and Children and Young Peoples’ Services took place in three venues around the County. They were well attended and the positive feedback indicates that the sessions dealt with the issues and proposed solutions in a very effective way. We have run further sessions in response to a continuing demand.

This edition of password is perhaps more lengthy than I would have wished although somewhat shorter than the Becta guidelines. It has been designed to highlight specific security concerns for schools and to offer advice as well as services to provide solutions for the security issues we face. An Executive Summary is included to give an overview of the document. We have also produced information that is available on the ScoMIS website that provides more detail particularly about the solutions that have been developed.

Steve Salway

Head of ScoMIS

Password Security Special – Executive Summary

We have produced a Password Security Special which deals in some detail with the various issues Schools need to address. It has been impossible to condense this into a smaller document without missing out key areas. This document is aimed at providing schools with a Summary of the key issues in our main document.

Data Protection and BECTA guidelines

Schools need to be aware of their obligations under the Data Protection Act 1998 and the Freedom of Information Act 2000. They should also understand the eight data protection principles which govern the use of personal information. They should have a good idea of the BECTA Good Practice in Data Handling guides, which provide a pragmatic approach to the issues in Schools.

Organisational Change

Schools should be prepared to identify key roles in protecting data and have a hierarchy of responsibilities.

Issues for consideration include:-

- Conducting an Information Risk Assessment
- What Data needs protecting?
- Who is responsible for that data?
- Impact levels and labelling of data.

Technological Change

Schools should make arrangements to secure data electronically, whether it be on site, in transit or when accessed remotely.

Issues for consideration include:-

- Network Security
- Physical Security
- Password Policies
- Encryption of personal data which is being accessed remotely
- Encrypt media that contains personal data that is to be removed from the organization
- Securely delete and overwrite to government standards all files that contain personal data when no longer required and ensure that equipment is disposed of in a secure manner.

Next Steps

Schools should provide awareness sessions on Good Practice in Data Handling and ensure that their staff are aware of their duties under the Data Protection Act 1998.

Further information on all these topics can be found in this Password Extra – Data Security Special.

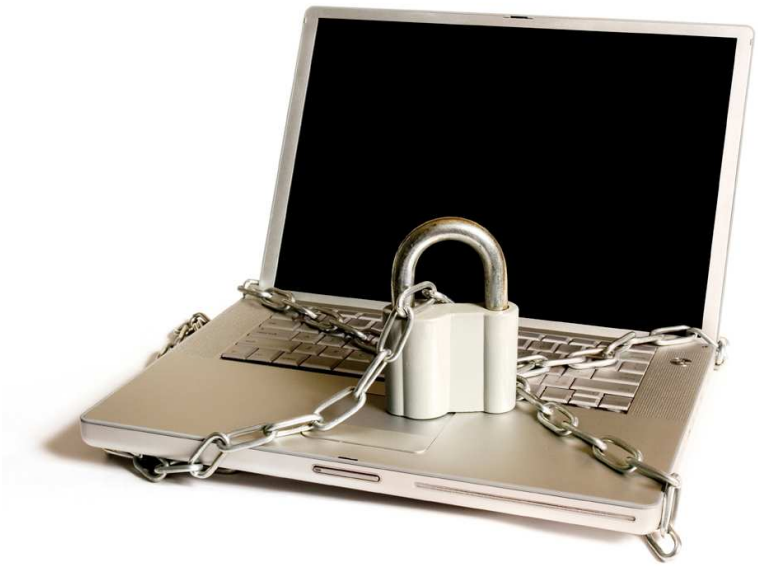
Introduction

Never have Schools held more data about their pupils, students and staff, and at no time has this data been more in demand by Teachers, Governors and Parents. Schools will need to develop appropriate processes to ensure they are compliant with data protection legislation and security guidance.

ScoMIS have been working over the past few months with Children and Young Peoples' Services, Devon Audit Partnership, and Strategic Intelligence to develop a strategic approach to Data Security, in response to the BECTA Guidelines and central and local government concern over the protection of data in schools.

The BECTA Data Security guidelines, summarised as "Good practice in information handling in schools - Keeping data secure, safe and legal", provide detailed guidance in key areas relating to school's data. To enable schools to be able to comply with these guidelines, ScoMIS aim to provide information encompassing strategic advice, workshops for schools and a range of security services.

This Special edition of Password pulls together the information School Leaders require to take the necessary steps in Data protection.



Contents (Hyperlinks to relevant sections)

Background Information on Data Protection

Legislation

In order to look at all the issues involving protecting the data we hold about the children in our schools, we need to remind ourselves of the following Acts of law:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Human Rights Act 1998/European Convention on Human Rights
- Freedom of Information (FoI) Act 2000
- Common law duty of confidentiality

Key amongst the messages is the definition of Personal data and the manner in which it may be processed:

Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. Personal data includes names, contact details, gender, dates of birth, unique pupil number (UPN). Personal data may also contain other information such as academic achievements, other skills and abilities, progress in school, and behavior and attendance records.

The Eight Data Protection Principles

There are 8 Principles which define the role of organisations in Data Protection. They define how individuals in organisations should process personal data. The following summary is provided by the Devon County Council Corporate Information Governance team:

Principle 1 – Personal data shall be processed fairly and lawfully

Principle 1 is the most important principle. If you don't comply with this anything else you do with someone's information will be unlawful.

Fairly – you need to make it clear to all individuals who you obtain personal information about, who you are, what you want to do with their information and who you might disclose their information to.

Lawfully – any information obtained, used, disclosed or destroyed (processed) must be done so lawfully. This means that you need to have a legal power enabling you to process personal information e.g. this could be if someone gives you permission to use their information.

Principle 2 – Personal data shall be processed for specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes.

This means you can only use someone's information for the purpose(s) outlined in your School's 'Notification' and for the purpose(s) you stipulated at the time of collecting the information.

You cannot re-use personal information for unrelated purposes without obtaining further consent from the data subject, unless you have another legal power enabling you to use the information for a different purpose e.g. you need to give the information to the Police to assist in the prevention or detection of a crime.

Principle 3 – Personal data shall be adequate relevant & not excessive

When collecting and inputting data, you must ensure that the information is adequate, relevant and not excessive for the purpose for which it was obtained.

All computer and written entries must be clear in meaning and be easily understood by others. Opinions should be clearly distinguishable from fact.

Remember, individual's have a right of access to information held about them (whether held in a handwritten note, in an email or in a formal document) so all comments must be professionally worded.

Principle 4 – Personal data shall be accurate and where possible kept up to date

This places an obligation on schools to ensure that the personal information you hold is accurate and up to date. This means you need to review the information you hold about people regularly and change any out of date or inaccurate information.

Data is inaccurate for the purpose of the Data Protection Act if it is incorrect or misleading.

Principle 5 – Personal data must not be kept for longer than necessary

Personal information must be reviewed on a regular basis and out-of-date or irrelevant information should be deleted or destroyed.

Principle 6 – Personal data shall be processed in accordance with the rights of data subjects

One of the rights under the Data Protection Act is 'Subject Access'. This gives everyone the right to obtain a copy of personal information held about them (including opinions), subject to certain exemptions.

Your school should have a procedure in place for handling Subject Access requests. Guidance on what should and shouldn't be disclosed can be obtained from Devon County Council's Corporate Information Governance team at dpoffice@devon.gov.uk or on 01392 384678.

In addition, individuals have the right to have inaccurate data held about them rectified, blocked, erased or destroyed and can claim compensation for any damage or distress that has been caused by any contravention of the Data Protection Act.

Principle 7 – Personal data shall be kept secure

Employees, contractors and agents must keep all personal information secure.

A common sense approach should be taken:

- Keep desks clear of paperwork containing personal information.
- File information in lockable cabinets.
- Devise difficult computer passwords and do not disclose them to anyone.
- Lock unattended offices.
- Wear identification badges at all times and challenge those who aren't.
- Only disclose personal information to people who have a legal right to know.
- Take care to ensure that confidentiality is maintained in verbal discussions especially

if you may be overheard by those who do not need to know.
- When sending confidential information by post, mark it 'personal & confidential – to be opened by addressee only' and clearly state the name and full address of the intended recipient.
- Make sure envelopes and packages are effectively sealed and have the correct postage on them (when posted externally).

This is not an exhaustive list.

Principle 8 – Personal data must not be transferred to countries without adequate security

Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory can ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

BECTA were then commissioned to look at security issues in school, particularly involving the use and management of data. There are two key sets of documents – the Information Management Strategy Framework and the set of 6 guides in Good Practice in Data Handling. Here we will briefly look at each set of documents.

Information Management Strategy Framework

Effective use of data is a key issue for school management, as system integration enhances the smooth running of the school, with not only improved efficiencies but also possible cost savings.

BECTA has published an Information Management Strategy framework guide to help schools make more effective and secure use of their data and improve the quality of data that they hold.

The Information Management Strategy framework is designed to help schools to review their current position on data management and provides helpful tips and hints on how to plan further actions.

The Framework is divided into four key strands: Leading an information management strategy; Developing capacity and capability; Gaining effectiveness and efficiency and Improving Data Management. The latter concerns us most in this context and is divided into 4 areas:

- Data quality
- Data processing and interoperability
- Data security
- Data sharing

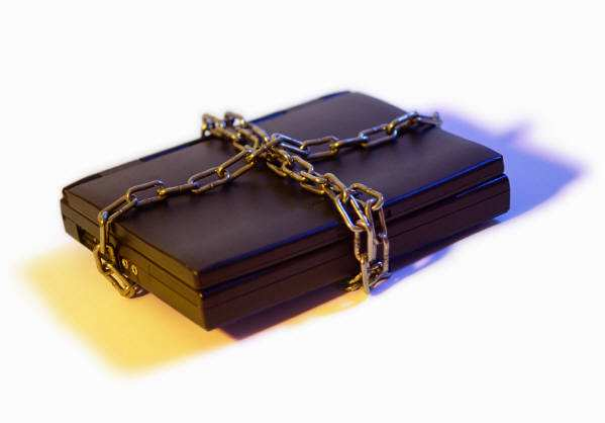
If we focus on the Data Security area, the Framework immediately provides schools with the type of questions that need to be asked:

- Who in school is aware of the legal requirements of the Data Protection Act and the Freedom of Information Act?
- Who is the school's Data Protection Officer?
- Who is the Senior Information Risk Owner (SIRO)?
- How does the school ensure compliance with legal requirements for encryption, controlled access to sensitive data, and storage and destruction of sensitive data?

We will attempt to answer these and more questions in the rest of this Security issue.

BECTA Guidelines

The BECTA Guidelines were written to provide a pragmatic approach that will enable schools, colleges and universities to follow the spirit of the government legislation in a way that is proportionate and appropriate for them.



Six separate, but linked, documents make up the Good practice in information handling Guides:

- Keeping data secure, safe and legal http://schools.becta.org.uk/upload-dir/downloads/information_handling.doc
- Audit logging and incident handling http://schools.becta.org.uk/upload-dir/downloads/audit_logging.doc
- Data encryption http://schools.becta.org.uk/upload-dir/downloads/data_encryption.doc
- Secure remote access http://schools.becta.org.uk/upload-dir/downloads/remote_access.doc
- Information risk management and protective marking http://schools.becta.org.uk/upload-dir/downloads/page_documents/information_risk_management.doc
- Data security dos and don'ts http://schools.becta.org.uk/upload-dir/downloads/data_security_dos_and_donts.doc

The key messages are explored in more detail in some of the following sections. However there are two key messages on types of change which might be needed:

Organisational Change and Technological Change

Organisational Change – issues for consideration include:-

- Appointing a Senior Risk Information Officer (SIRO)
- Identify information assets and for each one, identify an Information Asset Owner (IAO)
- Conducting an Information risk assessment
- Impact levels and labelling of data
- Conduct data-handling awareness training for all users
- Implement a policy for reporting, managing and recovering from information risk incidents
- Paper containing protected data must be shredded, pulped or incinerated when no longer required.

Technological change – issues for consideration include:-

- Implement and/or require suppliers or hosting partners to implement SSL or IPSec encryption for remote access to sensitive data contained in school information management systems, learning platforms and portals
- Encrypt all media that contains protected data that is to be removed from the school premises
- Securely delete and overwrite to government standards all files that contain protected data when no longer required.

Organisational Change

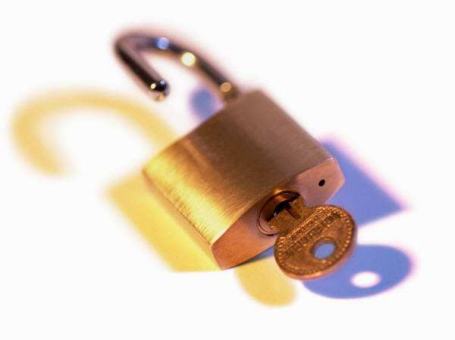
Roles and Responsibilities

The Good Handling Guides detail roles and responsibilities which people in schools need to undertake to begin the Data Security trail.

Senior Information Risk Owner (SIRO)

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

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



The Information Asset Owner(s) (IAO)

Schools must identify their information assets – including personal data for pupils and staff, assessment records, medical information and special educational needs data, for example – and for each one, identify an 'information asset owner'. The role of an IAO is to understand:

- what information is held, and for what purposes
- how information has been amended or added to over time
- who has access to protected data and why

Our Data Security pages have a proforma, School Hierarchy of Responsibilities which schools may wish to use:
http://www.scomis.org/go/ds-hierarchy

Risk Assessment

As part of your Data Security programme Schools need to work through a risk assessment to identify areas and scenarios where the safety of data might be put at risk. This may involve looking at scenarios and deciding whether they are high or low risk, and looking at suitable controls on these activities. The following questions may be useful:

Establishing risk:

- Is there a culture of valuing information as an asset in your school?
- Do senior managers lead by example and talk about the importance of information management?
- Are staff at all levels given personal accountability and held accountable for their actions when dealing with key information?

Is the risk to information seen as a serious risk, and treated with the same importance as other serious risks?

Are the procedures in plain English and understood by all staff?

Are there safeguards (e.g. IT security, physical checks, personnel security, escalation procedures) to minimise the risk of errors, or someone just not obeying the rules, or even reckless damage

Do you manage access to key data sufficiently (e.g. security clearance for people dealing with

sensitive data, tracking systems for seeing who has accessed what, removing access rights as soon as they are not needed)?

- Do you have systems which monitor what is happening locally?

Is the message consistently reinforced through induction events and training?

- Is good information management valued in staff appraisals? Is poor information management addressed?

Are staff at all levels given personal accountability and held accountable for their actions when dealing with key information?

ScoMIS have made some proformas available on our Merlin Data Security site.

http://www.scomis.org/go/ds-documents

Incident Handling and Reporting

Devon County Council has a responsibility to monitor all incidents in schools which may breach security and/or confidentiality of information. All incidents need to be identified, reported, investigated and monitored so that incidents of a particular nature do not keep re-occurring. It is not the intention to apply or apportion any blame to members of staff. Schools need to ensure that they have a clear understanding of these issues and staff understand what they need to do if loss of data or IT equipment should occur.

All breaches of security and/or confidentiality are events that could compromise business operations, result in embarrassment to either the Council or loss of trust in the organisation by a client or the public as a whole. Each could be a threat to the personal safety or privacy of an individual(s) and/or lead to legal or penalty issues. Every breach must be taken seriously and reported using the following link: http://www.devon.gov.uk/index/councildemocracy/improving_our_services/access-to-information/data_protection/incidentreporting.htm.

If there is any doubt about what constitutes a security incident, staff should contact the Corporate Information Governance Manager or a member of the Information Compliance Team, using the corporate mailbox: keepdevonsdatasafe@devon.gov.uk

All incidents relating to breaches of security and confidentiality where there has been a theft/loss of IT equipment must also be reported using the incident theft form: http://staff.devon.gov.uk/fit/dfs/audit/fitdfsauditgenstaffinfo/theft/fitdfsauditittheftreport.htm

Protective Marking

Protected documents must be marked with the risk level in the header and footer. This will serve to identify Documents which contain Personal and Sensitive Data. The BECTA Guidelines state that this should be the Government Protective Marking Scheme. The scheme is made up of five markings, which in descending order of sensitivity are:-

1. Top Secret
2. Secret
3. Confidential
4. Restricted
5. Protect

Most learner or staff personal data that is used within Schools will come under the **PROTECT** classification. This has been reproduced below:-

Criteria for assessing PROTECT (Sub-national security marking) assets:

- cause distress to individuals;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- breach statutory restrictions on the disclosure of information
- cause financial loss or loss of earning potential, or to facilitate improper gain;
- unfair advantage for individuals or companies;
- prejudice the investigation or facilitate the commission of crime;
- disadvantage government in commercial or policy negotiations with others.

The full table may be found on the Cabinet Office website: http://www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx#18

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.

ScoMIS will also be working towards ensuring that any reports that they produce on behalf of schools are appropriately marked.

Shredding paper waste

All personal or sensitive pupil information held in paper form should be destroyed securely when it is no longer needed. If the school shreds its own documents, please make sure that these are securely shredded using a good cross-cut shredder, so that documents cannot possibly be reconstructed.

Technological Change

BECTA outline technological changes which are needed to take place in terms of Data Security. The agency is aware that this may require more long term planning and assistance from bodies out of school that provide IT support. In this section we will try to outline some of these changes and highlight areas where ScoMIS solutions can help schools meet these criteria.

The BECTA Guidelines specifically look at the technical aspects of:-

- Audit Logging
- Secure Remote Access
- Encryption of media that contains personal data that is to be removed from the school premises
- The secure deletion of personal data when no longer required
- The safe disposal of redundant IT equipment.

Further advice on these items can be found below as well as details of solutions that ScoMIS has put in place to enable schools to meet these requirements.

Audit

Educational organisations must keep audit logs to help detect and respond to security incidents, and to provide evidence of accidental or deliberate security breaches, for example, loss of personal data or breach of an acceptable-use policy.

ScoMIS are required therefore to keep full logs of access to all our systems, in order that patterns of unexpected logons may be monitored and reported.

Secure Remote Access

BECTA recognise that teachers require access to data about children when outside of School in order to carry out their primary function, that of providing high quality, informed teaching. BECTA outline that where Remote Access is required, the following parameters must be observed:

- **authentication** – who or what system is trying to connect, ensuring that the users and the computers at each end are who they say they are
- **authorisation** – ensuring that the users at the remote end are authorised to access the data
- **geographical restrictions** – personal data may not be accessed remotely unless encrypted, and access may require specific network connections
- **encryption** – to secure personal data in transit, and file or full disk encryption for any storage media that holds personal data
- **Audit** – logs of access to secured data.

ScoMIS Solutions

SIMS Terminal Server Service

ScoMIS offer a service to all schools to host the school's SIMS data on powerful servers held at a secure location. School's have full access to SIMS, but are spared the issues of upgrades and back-up of this data. It has proved to be an effective way of allowing more staff access to SIMS. In terms of security and protecting pupil data, the following points are relevant:

- Password Security – ScoMIS enforce a complex password, with an enforced change every 42 days
- Audit logs/trails - ScoMIS keep logs of all logons with details as set out in the BECTA guidance
- Encryption - SIMS is accessed via Terminal Services and is encrypted to 128bit
- Schools control creation of user accounts
- Security Screen Saver - there is an enforced Password – protected screen saver which will apply when a period of inactivity is detected
- Fully backed-up – ScoMIS File Servers are fully backed up online as a matter of course.
- Physically Secure Servers – ScoMIS File Servers are off your site, in a secure Communications Room, which has restricted access in a building which itself cannot be accessed without badged entry.

In combination with Terminal server delivery of SIMS, the VPN Gateway offers secure home access to your SIMS. The security benefits of this are:

- Secure home access
- Industry standard encryption
- SSL certification
- Password security
- Double Authentication is separate from Authorisation

ScoMIS Remote Backup Service

ScoMIS provide a fully managed, reliable and automated backup solution, which uses high speed broadband links to backup data securely over the internet. Already in use in over a hundred schools in Devon, this also offers security benefits:

- Logs kept of all backups
- Fully mirrored – school backups are held in two geographically different locations
- Checked/test restores - to ensure good backups are in place
- Monitored – machines are checked

automatically to ensure backup has taken place
- Automatic – no school intervention is needed for this too work
- Encrypted – fully protecting data in transit and in rest on the backup servers
- Secure off-site – in the event of catastrophe your data is secure

Encryption of media which contains personal data and is to be removed from school premises

In order to look at this topic, we need to look at two quotations from the BECTA Guidance

"Users may not copy or remove 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."

"Note that if your organisation does not have encryption now, we strongly recommend that you stop all copying, removing or accessing PROTECTED or RESTRICTED data until you have software to encrypt files and protect the communication links accessing this data. "

With this in mind, it becomes clear that Teachers will either have to stop taking any data about pupil away from school, or make sure that this is encrypted.

Why?

It is possible for anyone with a small amount of knowledge to access Data on a laptop which is protected with a username and password. Removing the Hard Disk Drive from a laptop may require two or more screws to be removed. The HDD can then be removed, attached to a USB cable and plugged into another computer. All information on the HDD is then available. In our Data Security Workshops, a practical demonstration of this showed that in around 4 minutes a Hard Drive could be removed, information copied and the HDD replaced.

How does encryption work?

Encryption works by converting all documents into unreadable Data unless the authorised username and password are applied. When logged on with your normal username and password, your laptop works as normal. As soon as you log off the Hard Disk Drive is fully encrypted.

ScoMIS Solution: ScoMIS Managed Encryption Service

ScoMIS have developed a Full Disk Encryption (FDE) service for schools. This will allow schools to encrypt laptops which teachers take home for their work. It will provide protection for the Data on those laptops. It will also allow audit of any device which has been lost or stolen, so that we can categorically state that the laptop was encrypted and that no pupil data could have been accessed. It will log unauthorised access attempts, but will allow registered users to obtain a password through a defined process if a password is forgotten.

ScoMIS are using a well respected solution, McAfee Endpoint Encryption, which has been carefully modified to make ease of use a prime consideration.

For more information, please see our website pages on encryption.

http://www.scomis.org/go/encryption

N.B. Other Mobile devices

Whilst we have identified Teachers' laptops as the immediate security risk, Schools need to be aware that other mobile devices such as mobile phones, PDAs, netbooks and Smart Phones are also used to hold or access data. All reasonable and proportionate means should be taken to secure these devices. If it is possible to password protect a mobile phone, then this should be applied. If these devices can be used to access data remotely then this access should be in the form of an encrypted protocol. We should also remind staff of the need to keep these devices securely, and not left where they could be accessed by other people.

Memory Sticks/Removable Hard Drives

The BECTA guidance is that all data classified as PROTECT Impact Level or higher, must be encrypted if this data is removed or accessed from outside approved secure spaces such as the school. This requirement applies to both communication links (for example, SSL or IPSec VPNs) and to files held on electronic storage media (hard drives, CDs, DVDs, USB sticks, memory cards etc.). In particular, the requirements are that:

Users may not copy or remove 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

ScoMIS Solution

There are many suppliers of encrypted media storage available to schools and Devon County Council also purchases devices which meet the relevant standards. Examples of such encrypted devices can be found at the following link:

http://www.rm.com/shops/rmshop/range.aspx?nguid=550ee8a2-a229-46e7-bbcb-32f4d3b02b2c&gsd=A--A00630|F00098-&pagesize=20

The secure deletion of personal data when no longer required

It is critical that where schools move computers from an administration area into the classroom, or prior to disposal, that all data is securely wiped from the Hard Disk Drive.

ScoMIS Solution

ScoMIS use a standard procedure to ensure that any PC that we move is securely wiped prior to re-installation of Windows

The ScoMIS Data-Wipe CD will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for wiping a PC prior to disposal or to being reused in another part of the school.

Please contact the ScoMIS Service Desk if you would like to use this service.

The safe disposal of redundant IT equipment.

Devon County Council offers a corporate scheme to assist schools in the disposal of redundant ICT equipment. The corporate scheme will dispose of most ICT equipment in a safe and environmentally friendly way in line with the WEE directive.

The disposal scheme is operated by Stone

Computers. Stone will take requests from authorised individuals for hardware that needs to be removed, and will endeavour to collect the hardware within 5 working days of the request being made. For further information about the scheme and current prices, see the following website:
http://staff.devon.gov.uk/fit/ict/hardwaresoftwarepurchases/equipmentdisposal.htm

ScoMIS Solution

Schools will be asked to indicate whether they intend to use the Devon County Council scheme, or make their own arrangements with regard to the safe disposal of redundant IT equipment which must include Secure Data Wiping and Environmental disposal. This information will be collated into a central database which will be available to Devon Audit Partnership and other colleagues within CYPS should they request it.

Please use link below to inform us of the method of secure disposal that you will be using. http://www.scomis.org/go/hw-disposal

Inventory of HDD serial numbers

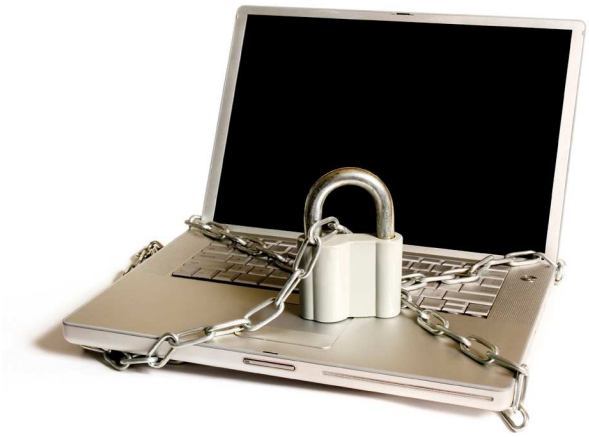
As you may be aware, the data is physically held on the Hard Disk Drive of a laptop or desktop computer. In order to have a full audit trail of our computer assets, it is necessary to hold an inventory of both laptop and desktop serial numbers and the Hard Disk Drive serial numbers.

ScoMIS Solution

To help schools fully audit the computer hardware in school, ScoMIS have developed a script that can be run on each computer in the school. The script can be downloaded onto a USB pen drive and run on each computer. This can then log the results in a spreadsheet as a record of all equipment held.

This information can then be added to your inventory in the usual manner and will be available if required for Audit purposes.

The script is available to download from: http://www.scomis.org/go/hd-audit



Next Steps

Your next steps should cover the following

- Staff training
- Staff Roles
- Risk assessment
- Paper document security
- Physical security
- Network Security
- Encryption of laptops
- Regular update of policy

Some materials to support this can be found on our Data Security website:

http://www.scomis.org/go/ds-support

Staff Training

Schools should provide data-handling awareness training for their staff. Make sure you include all staff – teachers, administrative, support, but also Governors and catering, cleaning staff. A short PowerPoint is available covering the following security topics:

- Roles and Responsibilities
- Why protect information?
- Information Assets
- Working online
- Email and messaging
- Passwords
- Laptops
- Sending and sharing
- Working on-site
- Working off-site

This can be downloaded from:

http://www.scomis.org/go/ds-presentations

Further Information

Subject Access Requests to Schools

In July 2009 a document was sent to all schools outlining their responsibilities to respond to Information Access requests from parents and students. It outlines time to respond, parameters dependent on age of the child, and possible charging frameworks. This document is available from:

http://staff.devon.gov.uk/subject_access_requests_in_schools_july_2009.doc

Using and Obtaining Images

A photograph is also part of a child's personal data. Schools should be aware of the need to process photographs in accordance with the Data Protection Act. There is a guidance document, Obtaining and Using Images in Schools, which gives clear guidance and policy examples. It can be accessed on:

http://staff.devon.gov.uk/obtainingimages.pdf