Schools
ICT Security
Self Audit

The use of ICT in schools is developing very quickly and there is evidence that we must develop a much better understanding of security and the protection of personal data in particular. Education is not alone in this. As yet high-profile newspaper exposés cover other areas of the public sector, but our time could come.

This ICT self-audit offers headteachers a tool to investigate the level of security awareness in their schools and to indicate policy, technical and training measures that may be required.

The Data Protection Act imposes personal liability on the directors and other officers of an organisation which has committed an offence under the DPA. Is the security of people, systems and data covered in your school?

Grahame Ward
Director Resources, Children Families and Education Directorate
May 2009

Schools ICT Security Self-Audit

Headteachers are responsible for the security of people, personal data and ICT systems, and face disciplinary action should problems arise in any of these areas. The Criminal Justice and Immigration Act makes it an offence for anyone to "intentionally or recklessly disclose information" or "repeatedly and negligently" allow information to be disclosed. Some schools are at risk! While sound security measures are essential, headteachers may not be familiar with all the technical or legal details. Sources of help and further reading are provided later in the document.

Reasons for concern:

- A recent check revealed schools with unsecured wireless networks installed by a parent or a local firm. With an ordinary laptop and little technical skill, details of pupils, staff and parents could be obtained as a first stage in building trust with a pupil. The school's Internet access could be used for criminal purposes that would be traced back to the school.
- Many staff take data home, for instance to write reports or appraisals. The intention is applauded, but loss of an unencrypted USB drive would make personal data easily available.
- A school laptop allocated to a teacher but used by family members or friends may be returned to school virus infected or with traces of unsuitable material having been viewed.
- Staff using personal email addresses for professional purposes would have difficulty in demonstrating that school data could not fall into the wrong hands.
- The Conficker virus does not affect fully protected networks (ref: 2). However a surprising number of school systems proved vulnerable and some still are.
- It is known that a pupil was able to alter their own MIS behavioural record because a member of staff left their MIS workstation logged in and unattended.

CFE has constructed this self-audit to help headteachers investigate ICT security. The audit is not exhaustive; indeed it covers only a few indicative areas. CFE does not require the audit to be returned, but would be interested in observations by schools. Headteachers, however, may wish to report the results to the Governing Body, probably with an action plan.

Self-styled "experts" can sometimes make questionable recommendations and/or decisions. One school was advised that an unencrypted wireless link across a public road should be used to increase the speed of data transfer. Headteachers may decide to require technical staff or suppliers to provide written responses to audit questions to emphasise the seriousness of the audit. External advice may be required to verify the technical answers provided. If headteachers have any doubt whether they have satisfactory answers to these questions, they should contact EIS.

In addition to YES / NO answers, it is useful to acknowledge where planning is in place to correct a security issue. Headteachers may wish to see an action plan with dates and designated staff before allowing this response. Schools may need to restrict activity in the short term, for instance not allowing personal data to be taken off the premises until encryption has been implemented.

We would value your comments on the audit, which is suggested as an annual activity.

Item	Audit requirement	Staff Responsible	Status found: No–Planned-Yes
Personal Data			
1	Has your school conducted a risk assessment on the identification and storage of personal data, which identifies the Information Levels involved? (Ref 1c)		
2	Has the Becta Data Handling Guidance been obtained and reviewed by a senior member of staff? (Ref 1a)		
3	Is personal data provided to any external organisations, for instance to populate a VLE? Have the data subjects been made aware of this use of their data through a Fair Processing Notice? (Ref 4)		
4	Are office, teaching and support staff sufficiently aware of their responsibilities for protecting personal data? For example the 8 principles of data protection? (Ref 4)		
5	Has your school notified the Information Commissioners Office that it processes people's personal data, as required under the Data Protection Act? (Ref 5)		
6	When personal data is taken off the premises by staff, is the data always encrypted, whether on USB memory stick or laptop hard disk?		
Network Security			
7	Is your school network server physically secure, for instance located in a locked room to protect the data and intellectual property stored?		
8	Is your school network data backed up regularly with the backup data stored securely off-site?		
9	Are senior leadership confident that security measures such as operating system patches and anti-virus signatures are applied to every school computer on a regular basis? (Ref 2)		
10	Does your school network access policy force the use of strong passwords where needed and restrict the use of elevated privileges? (e.g. inappropriate use of administrative accounts)		
11	Is your school certain that the wireless network is secure and that access to data from outside the school is not possible via this path?		
12	Does your school have a policy in place to control the use of unauthorised or uncontrolled devices on the network?		
e-Safety (a full e-safety self-audit is available at ref 3)			
13	Does your school have an e-Safety Policy that has been agreed by governors and has been revised within the last year? (Ref 3)		
14	Has the e-Safety policy been shared with and accepted by pupils, staff, and parents?		
15	Are all staff aware of how to respond to an incident of concern, for instance when the police need to be informed?		

Where to get help

- EIS provides advice and consultancy to assist schools in implementing appropriate technical security measures - contact the EIS Service Desk on 01622 672779 or go to www.eiskent.co.uk and click on the ICT Security button.
- Michelle Hunt is the CFE data protection officer, and can provide advice on ensuring your school complies with Fair Processing and the Data Protection Act, including impact labelling.

Further Reading

1) **Becta's revised data security guidance (April 2009):**
   Essential reading by responsible staff, or via your ICT support organisation!
   1a. Keeping data secure, safe and legal outlines the key measures for organisations.
   1b. Dos and Don'ts is a common sense guide to help staff keep data secure
   Plus more detailed documents on:
   - **Data encryption**
   - **Audit logging and incident handling**
   - **Secure remote access**

   http://www.becta.org.uk/schools/datasecurity

   1c. Good practice in information handling in school – impact levels and labelling
   http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf

2) **EIS advice on ICT Security:**
   All school network support agencies should be aware of this information.
   http://www.eiskent.co.uk/sc_members/supportportal.cfm?snid=349
   Contact: eis.support@kent.gov.uk

3) **e-Safety Guidance:**
   The Kent policy and guidance on e-Safety and materials such as posters and leaflets for parents are widely used, alongside material from Becta and CEOP.
   www.kenttrustweb.org.uk?esafety
   Contact - Rebecca Avery: Rebecca.avery@kent.gov.uk

4) **Data Protection Act 1998:**
   Guidance for schools on the DPA, Fair Processing Notices and staff training.
   http://www.kenttrustweb.org.uk/Policy/dpfoi_data.cfm
   Contact - Michelle Hunt: michelle.hunt@kent.gov.uk

5) **Information Commissioners Office:**
   A useful checklist to help compliance with data protection legislation.
   http://www.ico.gov.uk/what_we_cover/data_protection/your_legal_obligations.aspx

6) **Advisory Service Kent:**
   Details of e-Safety materials for primary schools and the ASK e-Safety course.
   http://www.kented.org.uk/ngfl/ict/safety.htm
   http://www.kented.org.uk/ngfl/news/courses/index.htm