

Good practice in information handling in schools

Keeping data secure, safe and legal

Contents

1 Introduction	3
2 Who is responsible and what data handling changes are required?	4
3 Good practice in information handling	6
Appendix A – Quick wins for data handling compliance.....	13
Appendix B – Additional core requirements.....	14

1 Introduction

Following several high-profile losses of personal data by government agencies, the Prime Minister ordered a review into how government agencies handle data. As a result of this review, the Cabinet Office published a report on 25 June 2008, called *Data Handling Procedures in Government* [http://www.cabinetoffice.gov.uk/reports/data_handling.aspx]. This sets out how the government is 'improving its arrangements around information and data security, by putting in place core protective measures, getting the working culture right, improving accountability and scrutiny of performance'.

These measures require both technical solutions and a change in practice, and are being implemented across central government and other public bodies. As such, the intent of these procedures should also be followed by schools and local authorities. This document aims to distil the key messages outlined in *Data Handling Procedures in Government* so they are applicable to schools and is intended for school leaders, senior leadership teams, network managers and other members of staff who have responsibility for handling and securing data.

There are four accompanying good practice guides:

- Impact levels and labelling
- Data encryption
- Audit logging and incident handling
- Secure remote access.

These guides provide a description of the procedures and suggest possible technical and operational solutions that can assist schools in minimising the risk of data security incidents and complying with existing legislation. These good practice guides should be read by school network managers and those responsible for implementing technical solutions.

The underlying principle of this 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.

In following this guidance, schools will be able to identify:

- data and information assets (information, stored in any manner, which is recognised as important or 'valuable' – not just in financial terms – or important to the organisation), with named owners responsible for them
- a framework for ensuring sensitive data is correctly labelled, managed and protected
- methods for the systematic assessment of risks and recording of data loss so that appropriate mitigating measures can be established.

2 Who is responsible and what data handling changes are required?

Data Handling Procedures in Government highlighted two roles that have responsibility for information security risk management. In schools, these roles may already be carried out by various individuals, and with different titles, but it is strongly recommended that the titles below – and the responsibilities attached to them – are adopted by schools.

2.1 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 Office of Public Sector Information (OPSI) has produced a guide to Managing Information Risk, to support SIROs in their role. This is available online [<http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf>].

2.2 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.

As a result, the IAO is able to manage and address risks to the information and ensure that information handling both complies with legal requirements and is used to the full to support the delivery of education.

Typically, there may be several IAOs within a school, whose roles may currently be those of e-safety, ICT, information management systems or admin coordinator.

Although these roles have been explicitly identified, the handling of protected school data is everyone's responsibility – whether you are an employee, consultant, software provider or managed service provider. Failing to apply

appropriate controls to protect this data could amount to gross misconduct or even legal action.

2.3 Required changes

To address the minimum protective measures outlined in *Data Handling Procedures in Government*, schools will need to implement several operational and technological changes. Some of these can be accomplished quickly and within existing resources, others will require investment and the participation of suppliers of school ICT systems and managed services. Becta will be working with suppliers to ensure they are aware of these procedures and to identify areas in which they can assist.

Until new technology or enhancements to your existing ICT infrastructure can be put in place, you are likely to need to make operational changes. These may mean that certain types of sensitive data may no longer be accessible away from the school in the short term.

In your own school, the level of required changes will need to be determined by Information Asset Owners following a risk assessment of the applicable data and specific requirements for remote access. Other changes that may be required include data handling awareness training, labelling, encryption, ICT event logging, incident response planning, provision of secure remote access using two-factor authentication, a review of contract clauses for data protection and processing (including cross-border data flows if data is processed abroad) and formal reviews of all user access requirements for remote access to, and storage of, protected sensitive data.

More detailed guidance on setting up procedures is given in the accompanying good practice guides. You can find a summary of the key points in the following section.

It should be noted that the suggested good practice is not definitive and is intended to be representative of the types of technologies, products and procedures that schools should adopt, and that as technologies are developed, new systems and procedures will need to be developed to ensure data security.

3 Good practice in information handling

This section provides an overview of the four good practice documents that provide the specific detail of how schools can comply with the mandatory minimum requirements of *Data Handling Procedures in Government*.

3.1 Protected markings and labels

This good practice guide describes how protective markings (or Impact Levels) are determined and how they should be applied to both paper-based and electronic systems. All documents that contain protected data must be labelled clearly, as shown below.

The screenshot shows a web-based form for 'Student Details: Ben Abbott'. At the top, a red banner indicates 'IL 3 Restricted'. The form is divided into several sections: 'Basic Details', 'Registration', 'Family/Home', 'Medical', 'Ethnic/Cultural', 'Additional Information', and 'History'. The 'Medical' section is currently active and contains the following information:

- Doctor:** Dr D Bell, East Town Community Clinic, Telephone - 859019
- Emergency Consent:**
- NHS Number:** ABCD 24
- Blood Group:** A+
- Dietary Needs:**
 - Artificial colouring allergy
 - Gluten free
 - Kosher foods only
 - No dairy produce
 - No nuts of any type/quantity
 - No pork
- Medical Notes:** A table with columns for Attachment, Summary, and Type.

Attachment	Summary	Type
	Asthma	Student Medical Note
	Hearing problems	Student Medical Note
	Video Clip - Teacher Assessment	Student Medical Note

Below the 'Medical' section is the 'Ethnic/Cultural' section, which includes dropdown menus for Ethnicity (WBRI - British), Home Language (English), Mother Tongue (English), National Identity (British), Ethnic Data Source (Parent), Religion (Christian*), English Additional Language (No), and Speaks Welsh (Information Not Obtained). At the bottom, there is a section for 'Nationality and Passport Details' with a table for Nationality, Passport Number, and Passport Expiry date.

Securely Delete or Shred

Impact Level Labels and Release Markings must be associated with each protected data element or report with onscreen displays or printed materials clearly indicating that the information requires protection.

Individual data elements require protection based on their sensitivity. When more than one data item is combined with other data at the same Impact Level, the Impact Level of the whole collection is often significantly increased. For example, losing a class of pupil records is potentially more damaging than losing a single individual's records; losing the whole school's records is more damaging than that of a class and so on.

Often, data is brought together from various different systems, which mean the aggregated data requires protection at higher levels. It is critically important that aggregated data is classified by the Information Asset Owners. The combination of particular data elements is what determines the appropriate protective marking as well as the remote access security requirements.

Due to the complexity of classifying reports generated from protectively marked data, it is recommended that where possible **educational ICT systems should be set up**

to label the output of any protected data as IL3-Restricted by default (implicit labelling). Where new systems are being procured it is recommended that implicit labelling is included as part of the functional specification and ICT requirements.

In summary, key guidelines and considerations are that:

- labelling practices must be in place
- all education ICT systems must be classified for the highest level data processed by the system and automatically labelled at the corresponding level
- all paper-based protected data shall have a header and footer printed on each page containing the Impact Level and Classification in the header and the Release and Destruction marking in the footer
- IL2-Protect and IL3-Restricted material must be encrypted if the material is to be removed from the school or other relevant government or commercial premises
- IL2-Protect and IL3-Restricted material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)
- disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

3.2 Data encryption

The Data encryption good practice document describes the types of encryption software that must be in place for laptops and mobile computing devices that access or store protected data.

The Cabinet Office guidance is that all data classified as Impact Level 2 (IL2-Protect) or higher must be encrypted if this data is removed or accessed from outside approved secure spaces such as the school or local authority. 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
- when data is required by an authorised user from outside the school premises (by a teacher working from their home, for example) access must be via a secure remote access solution (for example, two-factor authentication to the management information system).

In order to comply with the intent of *Data Handling Procedures in Government*, it is essential that a holistic approach is taken to data security. Encryption does not work in isolation from the other Information Assurance (IA) elements. These elements include requirements for identification, authentication, authorisation, accountability and audit, all of which are explained in detail in the good practice guide.

3.2.1 Encryption restrictions

It is important to note that although encryption is required to be used within the UK, there are some broader usage considerations when travelling to some foreign countries:

- Some countries ban the use, or severely regulate the import, export or use of, encryption technology. Taking a laptop with encryption software to certain countries could risk imprisonment or cause your laptop to be confiscated.
- You may not be able to meet certain import or export requirements, and must, before travelling to countries with restrictions, remove encryption software from your laptop or mobile device, avoid taking encrypted files to these locations, and remove protected data from your devices.

You can find further information on countries that restrict or ban the use, import or export of encryption from:

- <http://rechten.uvt.nl/koops/cryptolaw/index.htm>
- <http://www.wassenaar.org>

3.2.2 Encrypting devices and media

The need for encryption of local data on laptop computers and portable media can be fulfilled in two ways – full-disk encryption or file/folder encryption. These options are discussed in more detail in the guide, but in general, full-disk encryption is preferred as it requires no user knowledge regarding its operation or configuration.

Another option is the choice of enterprise-wide or stand-alone (point) solutions. Enterprise solutions provide a more manageable and reliable infrastructure, but the costs are greater when compared to the free or low-cost point solutions. Consideration should be based upon your specific circumstances and needs, such as the number of users that will require encrypted devices, also taking into account the Total Cost of Ownership and support costs.

The guide highlights a range of products that will meet the intent of *Data Handling Procedures in Government*. These products were selected as being indicative of those currently used in schools to show how they should be properly configured to ensure compliance. (Please note that the products listed have not been tested by Becta and are presented as examples only; other products may also meet the mandatory minimum requirements.).

The products in the following table and described in more detail in the good practice guide have not been tested by Becta and are only presented as examples. Other products may also meet the mandatory minimum requirements.

Representative products	Windows	Mac	Unix / Linux	Symbian	Windows Mobile	USB	Ad-hoc file encryption
MS BitLocker	X					X	
MS Windows EFS	X						
WinZip	X	X				X	X
Disk Protect	X					X	
CheckPoint	X	X	X			X	
PGP Desktop/Enterprise	X	X	X	X	X	X	X
Entrust Entelligence	X	X	X			X	X
FileVault		X					
DiskUtility		X					
Knox		X				X	
TrueCrypt	X	X	X			X	
BestCrypt For Linux			X				
Pointsec Mobile				X	X		
McAfee Endpoint				X			
BeCrypt PDA Protect					X	X	
Cruzer						X	
IronKey						X	
StealthMXP						X	
Kingston						X	
Kanguru						X	

3.2.3 Encrypting protected data in transit

As well as protecting data on devices and media, it is also necessary to protect sensitive or personal data that is transmitted between systems, applications or locations (known as data in transit). The secure transmission of protected data in transit relies on both encryption and authentication. There are four critical functions provided by this technology:

- Encryption of the data itself
- Ensuring that the computers at each end are the computers they say they are
- Ensuring that the user at the remote end is who they say they are
- Ensuring that the user is authorised to access the requested data.

The guide explains a number of solutions that offer compliance to *Data Handling Procedures for Government* requirements.

3.2.4 Securely deleting protected data

Finally, this guide explains how simply deleting a file does not make it non-recoverable. It suggests a number of solutions that meet the government requirement of secure deletion of temporary files, files left in Recycle Bin or Trash by overwriting to government standards (usually seven times).

3.3 Audit logging and incident handling

This good practice document provides guidance on how to keep logs to effectively handle security incidents such as a loss of protected data or the breach of the Acceptable Use Policy. The value of data can only be realised if the correct data is gathered and it is stored in a secure manner. It is also desirable to gather data in ways that avoid performance problems on the monitored systems, do not overstretch system resources, or unduly increase the workload of ICT administrators.

3.3.1 Audit logging

Audit log collection goes beyond just providing a common framework to facilitate collection and analysis. The rapid growth of ICT in schools and the current regulatory landscape requires educational organisations to collect data from a much broader set of sources including physical devices, network and security devices, hosts, databases and a range of commercial and bespoke applications. Log collection infrastructures must therefore be able to meet these needs whilst delivering secure and evidential quality audit log collection.

Most of these systems encompass more than one school, so where appropriate, schools should ensure that their logging infrastructure and policies are aligned with their local authority's.

A typical local authority with a 50,000 user system can produce logs with 7-8 million transactions each month. How long these logs are kept is dependent on a locally determined policy, the system(s) being monitored and whether protected data is involved.

This document outlines the minimum infrastructure a school should have in place to ensure that logs can be kept for compliance with audit log collection and monitoring requirements. It focuses on the native capabilities of the various operating systems, application event logs and reporting capabilities of critical security-related systems (MIS, learning platforms, portals, firewalls, and remote access, for example). It also outlines the processes required for maintaining logs in response to particular incidents that may be required as evidence in legal proceedings.

The first steps necessary to implement the basic infrastructure include the need to:

- complete an inventory of the systems that are deemed critical (including those with IL2-Protect data and above) and determine what auditing or

logging functions are turned on, where their data is written, the format, who owns the system and obtain access to that data

- compile a report that summarises this data and focus on the amount of data produced to determine network bandwidth, data storage requirements and recording format
- acquire the necessary servers, hubs, network-attached storage and firewalls to build a secure area for these items to be installed
- establish who has responsibility for operating this security solution, what information is to be reported, archival processes and procedures for resolving discoveries and remediation requirements.

3.3.2 Responding to security incidents

Data Handling Procedures in Government requires organisations to have in place a process for responding to security incidents. Your local authority may have a policy for this, which you should follow. If not, then GovCertUK (the body responsible for Computer Security Incident Response within UK Government) has produced some incident response guidelines that may be useful in determining your own policy [http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines.pdf].

To respond to a security incident response you need to know an incident has occurred. The sooner an incident is contained, the lower the risk of loss (both financial or data compromise). The following points are essential components for managing incidents effectively and are described in more detail within the good practice guide:

- Management commitment, in terms of human resources, budget and priority
- A resolution team
- Primary responsible person for each incident
- Communications plan, including escalation procedures
- Plan of action for rapid resolution
- Plan of action for non-recurrence
- Knowledge base of past security incidents, including steps taken for resolution and non-recurrence
- Awareness campaign.

3.4 Secure remote access

The Secure remote access document outlines a number of solutions that schools can use to allow users to access sensitive or personal data from outside school, including using Shibboleth via the UK Access Management Federation for Education and Research, and use of the forthcoming Employee Authentication Service for two-factor authentication.

The guide also explains how schools can reduce the need for two-factor authentication (such as a hardware token) by careful selection of the types of data that can be accessed remotely. For example, the type of data that schools make available online to parents should not be sensitive enough that it will require parents to be issued tokens.

In certain cases, however, it will be necessary to share protected data, such as information on pupils' special educational needs that is classified as IL3-Restricted. In this case, two-factor authentication and the use of password-protected files will be necessary to enable secure communication between the school and parents. This should be seen as an exception, rather than the rule.

Appendix A – Quick wins for data handling compliance

Becta recognises that conflicts exist in existing policy, practice, technology and budgets. We are working across government, education and with suppliers to implement the required changes, but there are a number of requirements that can be implemented relatively easily to minimise the risks of data loss or security breaches.

Operational

- Read and understand the *Data Handling Procedures in Government* final report and the associated Cross Government Actions: Mandatory Minimum Measures documents – [http://www.cabinetoffice.gov.uk/reports/data_handling.aspx]
- Appoint a Senior Risk Information Officer (SIRO)
- Identify information assets and for each one, identify an Information Asset Owner
- Label all school information management systems, learning platforms and portals at the highest level of data that can be accessed (generally, IL3-Restricted) as a default
- 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

- Implement two-factor authentication for all users accessing data at IL3-Restricted or above
- 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.

Appendix B – Additional core requirements

After addressing the quick wins in Appendix A, schools should implement the following:

Operational

- Incorporate requirements for managing information risk in HR and contract processes as necessary
- Ensure all new or changed contracts implement the latest OGC security and data protection clauses
- Ensure that user data is not exported outside the EEA unless EU Model Contracts or Binding Corporate Rules (BCR) are in place; particular attention is required to be sure your support contractors are fully compliant (note that BCRs require written approval from the UK Information Commissioner's Office). For more information, see the ICO [http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx]
- Conduct Privacy Impact Assessments (PIA) in accordance with the ICO [http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html]
- Report significant data protection incidents through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Technological

- Stipulate that suppliers implement the encryption and remote access requirements in each application
- Require suppliers to implement Impact Level headers and footers for any system-printed material that contains protected data and within the application screens if they contain protected data
- Implement a basic level audit and event logging infrastructure
- Implement necessary changes to applications to restrict access based on the Impact Levels associated with the data.