Good practice in information handling: Keeping data secure, safe and legal

For staff and contractors tasked with implementing data security

This document is one of a series of good practice guides to help schools, colleges and universities protect personal and sensitive data. Building on good practice from industry and central government these guides describe procedures and possible technical and operational solutions that can help organisations reduce the risks of data security incidents and comply with current legislation.

Produced by Becta on behalf of the Department for Children, Schools and Families, these guides have been reviewed and updated with feedback from a number of cross-sector organisations including DCSF, DIUS, JISC Legal, The Information Authority and JANET(UK), as well as from schools, local authorities, RBCs and suppliers.

For further information on these guides, please see http://www.becta.org.uk/schools/datasecurity and http://www.becta.org.uk/feandskills/datasecurity.

Contents

1 Introduction

In September 2008, Becta published a series of good practice guides on information handling in response to the Cabinet Office report *Data Handling Procedures in Government* [http://www.cabinetoffice.gov.uk/reports/data_handling.aspx]. This report 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' in response to high-profile losses of personal data. Building on these requirements, the Cabinet Office published *HMG Security Policy Framework* [http://www.cabinetoffice.gov.uk/spf.aspx]. It contains seven policies which outline the mandatory security requirements and management arrangements to which all government departments and agencies (defined as including all bodies directly responsible to them, including local authorities) must adhere.

These policies provide core security principles that organisations should follow to ensure that government assets (information, property and staff) are secured in a proportionate manner and that information (including personal data) can be shared confidently, knowing it is reliable, accessible and secured to agreed standards.

Becta has updated the original good practice guides to reflect the new policies and to incorporate feedback from a number of parties from across the education and skills sector. This has led to us taking a more pragmatic approach that will enable schools, colleges and universities to follow the spirit of the government procedures in a way that is more proportionate and appropriate for them. Following these policies will help organisations comply with the Data Protection Act 1998.

This summary document includes the key messages in *Data Handling Procedures in Government* and *HMG Security Policy Framework* for those in the education and skills sector. It is intended for leaders, senior leadership teams, network managers and other members of staff who have responsibility for handling and securing data.

Becta has also produced a new cross-sector 'dos and don'ts' guide on data security for end users.

We have also reviewed and updated our technical good practice guides (aimed at a technical audience). These cover:

- data encryption
- audit logging and incident handling
- secure remote access.

These guides describe procedures and possible technical and operational solutions that can help organisations reduce the risks of data security incidents and comply with current legislation. Network managers and staff responsible for implementing data security should read these.

The underlying principle of our guidance is that through a combination of technical and procedural solutions, organisations should do everything within their power to ensure the safety and security of any personal data (or data that is important to the secure running of an organisation).

In following this guidance, the reader will be able to identify:

- data and information assets (data, 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 data is correctly marked, managed and secured
- 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. Organisations may already have staff with different titles who carry out these roles. However, we strongly recommended that organisations adopt the titles below (and the responsibilities attached to them).

2.1 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is a senior member of staff who is familiar with information risks and the organisation'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 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 has produced *Managing Information Risk* [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

2.2 Information Asset Owner (IAO)

Organisation 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.

2.3 Recommended 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
- audit logging
- responding to security incidents
- secure remote access (using two-factor authentication where needed)

- reviewing contracts for data protection and processing (including cross-border data flows if data is processed abroad)
- reviewing user access requirements for remote access to, and storage of, secured data.

We provide more detailed guidance on these in our good practice guides. The good practice we suggest is not definitive. However, we think it represents the kinds of technologies, products and procedures that organisations should adopt. As new technologies are developed, organisations will need to develop new systems and procedures to maintain and improve data security.

3 Information risk assessment

It is important that organisations conduct thorough risk assessments on the assets they hold. This will help them plan security measures that are practical and proportionate to their specific size and risk profile.

3.1 Conducting an information risk assessment

Organisations should work out criteria for assessing risks. These will need to take into account:

- the assets involved
- legal requirements (such as the Data Protection Act 1998)
- the practicalities of running the organisation day to day
- the impact of incidents on reputation in the community.

Organisations should then identify, describe and prioritise risks against these criteria. The first step in identifying risks is for Information Asset Owners to list information assets that contain personal data or data valuable to the organisation.

Steps in identifying risks include identifying:

- assets
- threats
- existing controls
- vulnerabilities
- consequences.

Once organisations have identified risks they can estimate the size of those risks, that is, the combination of consequence and likelihood.

4 Good practice in information handling

This section gives an overview of our more technical good practice guides. They should help organisations secure data and so reduce the risk of security incidents. They will also help organisations meet the minimum requirements of *Data Handling Procedures in Government*.

4.1 Impact levels and protective marking

Since the first version of this document was published, the Government has published *HMG Security Policy Framework* [http://www.cabinetoffice.gov.uk/spf], which recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data. The scheme is made up of five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most learner or staff personal data that is used within educational institutions will come under the PROTECT classification. For more information about the Government Protective Marking Scheme, visit the Cabinet Office website [http://www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx#18].

We 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. Further guidance will be published when available.

4.2 Data encryption

Our *Good practice in information handling: Data encryption* guide explains what data organisations should encrypt. It gives some examples of encryption solutions and information on taking data abroad.

It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. The Information Commissioner's Office (ICO) recommends[1] that portable and mobile devices (including media) used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Organisations should encrypt any personal or sensitive data that is removed or accessed from outside an approved secure space. Examples of approved secure spaces include physically secure areas in schools, colleges, universities, local authorities and the premises of support contractors. This applies to both communication links (for example, SSL or IPSec VPNs) and to files held on

[1] Visit the ICO website [http://www.ico.gov.uk/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx].

electronic storage media (for example, hard drives, CDs, DVDs, USB sticks and memory cards). In particular:

- when sensitive or personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- organisations or users must securely delete personal or sensitive data when it is no longer required.

In order to comply with the intent of *Data Handling Procedures in Government*, organisations must take a comprehensive approach to data security. On its own encryption is not enough to secure data. Other important measures include identification, authentication, authorisation, accountability and audit, all of which are explained in detail in the good practice guides.

4.2.1 Encryption restrictions

Although recommended for protecting data in the UK, some countries ban the use, or severely regulate the import, export or use of, encryption technology. You should always check current restrictions before leaving the UK with encryption software or encrypted data – you can find out about current restrictions from the two websites below. It may be safer to remove the software and data from your laptop or mobile device than to risk violating compliance requirements in these countries. Not doing so could risk imprisonment or confiscation.

You can find further information on countries that restrict or ban the use, import or export of encryption from the Crypto Law Survey [http://rechten.uvt.nl/koops/cryptolaw/index.htm] and the Wassenaar Arrangement [http://www.wassenaar.org].

4.2.2 Encrypting devices and media

Organisations and individuals can encrypt personal data on a device – for example, a laptop – using either full disk encryption (also known as whole disk encryption) or file/folder encryption (also known as file system level encryption). These options are explored in the guide but, in general, we recommend full disk encryption as it is easier for users.

Organisations must also choose between enterprise solutions and stand-alone solutions. Enterprise solutions provide a more manageable and reliable infrastructure, but the start-up costs are higher compared with free or low-cost point solutions. Organisations should consider their specific circumstances and needs, such as the number of users that will require encrypted devices. Organisations should also allow for ongoing support and management costs, when comparing enterprise and stand-alone solutions.

The guide includes some information on products that meet the intent of *Data Handling Procedures in Government*. Becta has not conducted a formal evaluation of these products and, therefore, does not recommend any specific solution. Other suitable products are available that are not listed in the guide.

4.2.3 Encrypting protected data in transit

As well as protecting data on devices and media, organisations should also encrypt personal data that is transmitted between systems, applications or locations (known as data in transit). Secure transmission of data relies on encryption, authorisation and authentication.

Secure transmission involves:

- encrypting the data
- making sure that the computers communicating are who they say they are
- making sure that a user at the remote end is who they say they are
- ensuring that a user is authorised to access the data.

4.2.4 Securely deleting protected data

A normally deleted file can be recovered, since only the directory entry and not the file contents are removed from the disk. Government guidelines mandate the secure deletion of files (when they are no longer needed) by randomly overwriting files to government standards (usually seven times).

4.3 Audit logging and incident handling

Good practice in information handling: Audit logging and incident handling gives guidance on how to effectively handle security incidents using audit log data. For example, loss of secured data or breach of an acceptable-use policy (AUP). Audit logging is only valuable if organisations collect the correct log data and store it securely.

Organisations should also collect data in ways that do not overburden systems or make unnecessary work for technicians.

It is a legal requirement of the Data Protection Act 1998 to have a statement of intent that tells staff what kinds of actions are logged or monitored and the level of detail involved.

4.3.1 Audit logging

Organisations should collect log data from a range of items including physical devices, network and security devices, hosts, databases, and commercial and bespoke applications. Log collection infrastructures must secure log data and collect data of evidential quality.

Systems may cover more than one organisation, so where appropriate, organisations should ensure that their logging infrastructure and policies are aligned with their local authority or network service provider.

In one month a university, college or local authority with 50,000 users can produce logs with around eight million entries. Organisations should retain logs for the length of time stated in their retention policy. The duration depends on the systems being monitored and the type of data involved.

Good practice in information handling: Audit logging and incident handling outlines an infrastructure an organisation might use to ensure that it can collect logs and provide effective audit and monitoring. It examines some of the native capabilities of operating systems, application logs and critical security-related systems (such as management information systems, learning platforms, portals, firewalls and routers). It also outlines the processes needed to maintain the integrity of logs and respond to security incidents where log data may be required as evidence in legal proceedings.

The first steps to implement an infrastructure include:

- listing critical systems (including those with sensitive and personal data) and determining what logging is turned on, where this log data is stored, how long it needs to be kept, the format, who owns the system and who can access it
- calculating the amount of data produced to work out network bandwidth and storage space requirements and recording format
- getting hold of the necessary servers, hubs, network attached storage and firewalls to build a secure internal area for these items. Organisations may need to build more than one audit/logging area due to the spread-out nature of their infrastructure.
- naming staff who have responsibility for operating the infrastructure (including the information that is to be reported), archiving processes, and procedures for resolving discoveries and remediation requirements.

4.3.2 Responding to security incidents

Data Handling Procedures in Government requires organisations to have in place a process for responding to security incidents. In the case of schools, their local authority may have a policy for this, which schools should follow. Other organisations may find *Incident Response Guidelines* from GovCertUK helpful [http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines_v1-1.pdf].

Organisations need to know that a security incident has happened before they can respond. The sooner an organisation contains an incident, the lower the risk of harm to individuals or the organisation through financial or reputation loss or data compromise.

The following points are key to managing incidents effectively (and are described in more detail in *Good practice in information handling: Audit logging and incident handling*):

- Management commitment, in terms of human resources, budget and priority
- A resolution team
- A person who is primarily responsible for each incident
- A 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
- An awareness campaign.

4.4 Secure remote access

Our *Good practice in information handling: Secure remote access* guide outlines some solutions that organisations can use to allow users secure remote access. It includes using Shibboleth (via the UK Access Management Federation for Education and Research) and Employee Authentication Services (EAS) (via the UK Government Gateway) for two-factor authentication.

The guide also explains how organisations can reduce the need for two-factor authentication by choosing the kind of data that users can access remotely with care. This is particularly important for schools putting in place online reporting to parents, who do not need to use two-factor authentication.

5 Quick wins for data handling compliance

It is recognised that conflicts exist in existing policy, practice, technology and budgets. Becta is working with suppliers to implement the recommended changes, but there are a number of requirements that organisations can implement more easily to reduce the risks of security incidents.

5.1 Operational

- Make sure staff[2] with access to personal data on children or vulnerable adults have enhanced Criminal Records Bureau (eCRB) clearance.
- Read *HMG Security Policy Framework* [http://www.cabinetoffice.gov.uk/spf.aspx].
- Appoint a Senior Risk Information Officer (SIRO).
- Identify information assets and for each one, identify an Information Asset Owner.
- Conduct data security training for all users.
- Put in place a policy for reporting, managing and recovering from incidents which put information at risk.
- Shred, pulp or incinerate paper when no longer required.
- Make staff and learners (and parents where applicable) aware of what data is being held about them and what it is being used for by issuing privacy[3] or fair processing notices[4].
- Make sure that, where appropriate, contracts for employment state that misuse of such data is a disciplinary matter.

5.2 Technological

- Implement two-factor authentication for all users with access to large data sets, such as all the contents of a management information system.
- Implement and/or require suppliers or hosting partners to implement SSL or IPSec encryption for remote access to personal data in management information systems, learning platforms and portals.
- Encrypt media that contains personal data that is to be removed from the organisation.
- Securely delete and overwrite to government standards all files that contain personal data when no longer required.

[2] Includes permanent and contract staff within organisations and suppliers.
[3] At the time of writing, the ICO [http://www.ico.gov.uk] launched a public consultation prior to publishing a code of practice for privacy notices. The code of practice will help organisations to draft clear privacy notices and make sure that they collect information about people fairly and transparently. It contains good examples that organisations will be able to use to help draw up their own privacy notices.
[4] Schools should see the DCSF fair processing notice [http://www.teachernet.gov.uk/management/IMS/datamanagement/FPNpupils].

6 Additional requirements

After addressing the 'quick wins', organisations should:

6.1 Operational

- Incorporate requirements for managing information risk in HR and contract processes as necessary.
- Ensure all new or changed contracts implement the latest Office of Government Commerce (OGC) security and data protection clauses.
- Ensure that personal data is not exported outside the European Economic Area (EEA) unless EU Model Contracts or Binding Corporate Rules (BCRs) are in place; particular attention is required to be sure your support contractors are fully compliant (note that BCRs require written approval from the Information Commissioner's Office (ICO)). For more information, see the ICO website [http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx].
- Conduct privacy impact assessments 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 ICO based on the local incident handling policy and communication plan.

6.2 Technological

- Stipulate that suppliers implement encryption and remote access requirements in each application.
- Require suppliers to implement protective markings for any system-printed material that contains personal or sensitive data.
- Put in place an audit logging infrastructure.
- Implement necessary changes to applications to restrict access.