Good practice in information handling

Information risk management and protective marking

A guide 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 the DCSF and Department for Business, Innovation and Skills, and a number of cross-sector organisations JISC Legal, The Information Authority and JANET(UK), as well as from schools, local authorities, RBCs and suppliers.

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

Contents

Key points

Educational organisations should use information risk management to help them look after the security of personal data, sensitive personal data and data that is critical to the organisation.

Most data will need the NOT PROTECTIVELY MARKED or PROTECT marking. A small subset of data will need a higher marking. Organisations should put in place extra restrictions and controls to prevent unauthorised access or potential loss of this data.

This guide applies to the access to, storage, transmission and destruction of all sensitive and personal data and critical data, both paper and electronic. Its aim is to help organisations to assess their information risks as part of an overall approach to managing information.

The guide also explains how to use the Government Protective Marking Scheme[1], which will help make staff aware of how confidential a document is and how they should treat it.

This guide is for staff or contractors in educational organisations carrying out an information risk assessment and putting in place a system of protective marking.

It contains:

- an explanation of what data needs to be secured
- a summary of the Data Protection Act 1998
- an overview of information risk assessment
- information about the Government Protective Marking Scheme
- good practice in document handling, storage and transfer
- issues for schools to consider in online information for parents and carers.

[1] http://www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx

1 What data do organisations need to secure?

The Data Protection Act 1998 came into force on 1 March 2000, bringing the UK in line with a European Directive on Personal Data (95/46/EC). The Act is there to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data.

The Data Protection Act 1998 requires all organisations, including educational organisations, to hold personal data securely.

The Information Commissioner's Office (ICO) is the UK's independent public body set up to protect personal information and promote public access to official information. The ICO provides guidance on rights, responsibilities and obligations to protect information. It has legal powers, including the power to issue information and enforcement notices, conduct audits and prosecute offenders. Organisations can obtain further information about the Act from the ICO [http://www.ico.gov.uk] including queries relating to obligations under this Act.

Personal data

The Data Protection Act applies to *personal data* (data that applies to a living person) held on a computer system or on paper. Stricter rules apply to *sensitive personal data* including (but not limited to) special educational needs, health (mental or physical), religious beliefs, racial or ethnic origin and criminal offences.

The first step for all organisations must therefore be to identify, within all the data they hold, which data counts as 'personal'. A quick reference guide produced by the Information Commissioner's Office (ICO) offers guidance on this.[2]

Personal data must be processed in accordance with certain principles and conditions.

[2] *What is personal data? – A quick reference guide to help organisations determine what is personal data* [http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf]

Anyone who processes personal information must comply with eight principles, which make sure that personal information is:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept for longer than is necessary
6. processed in line with the individual's rights
7. secure
8. not transferred to other countries without adequate protection.

Personal data can only be processed under one or more of the following rules:

- An individual has given consent
- It is part of a contract
- It is a legal obligation
- It is necessary to protect the individual
- It is necessary to carry out public functions
- It is in the legitimate interests of the data controller.

While explicit consent must be obtained in many contexts, consent is not required for the purposes of delivering an education within the education sector. However, the reasons for collecting and processing sensitive personal data must be completely transparent.

It is a legal requirement to protect sensitive personal data. In an educational organisation, 'sensitive' personal data would include, for example, data recording that a pupil was considered 'at risk', or that a member of staff had had extended leave for mental health problems. Individuals entrusted with sensitive personal data, however derived, are accountable for its protection and compliance with the law.

Every item of personal data that is held or processed must be accurate, up to date and held for no longer than necessary. When personal data is no longer relevant to the purpose for which it was originally obtained, and/or has reached the end of the period for which it must legally be retained, it must be securely destroyed in accordance with its relevant protective marking.

Where the educational organisation has contracted a third party to manage all or part of information management through managed services, a policy will need to be in place covering the protection of personal or sensitive data. Responsibility for data security still rests on the educational organisation.

The security of personal data must be maintained, and any disclosure must be properly authorised. There are specific consent requirements in respect of personal data transferred to countries outside the European Economic Area (EEA). You can find further information from the Information Commissioner's Office [http://www.ico.gov.uk].

Other data

Although not defined as personal data, organisations should also secure any data that is *critical* to the running of their organisation. This might include, for example, all financial data as well as a wide range of correspondence. Educational organisations need to consider the risk of financial loss not only to them but also to another party if there was a breach of security.

2 What should organisations do?

It is a legal requirement of the Data Protection Act 1998 to secure personal data. *Data Handling Procedures in Government*[3] sets out the measures that government organisations should adopt to protect personal data:

- Users should not remove or copy personal or sensitive personal data from the organisation or authorised premises unless the media is encrypted, is transported securely, and will be stored in a secure location.
- When personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff, teacher, lecturer, tutor or learner working from their home, or by a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users should protect all portable and mobile devices, including media, used to store and transmit personal data using encryption software.
- Organisations or users should securely delete sensitive personal data or personal data when it is no longer required.

Protective marking

The Cabinet Office recommends applying the *Government Protective Marking Scheme*[4] to documents, to indicate the level of protection the data requires. Becta recommends that educational organisations apply this scheme, to both paper and electronic documents.

The Protective Marking Scheme has six categories of confidentiality, of which four are applicable to educational institutions. These are, in increasing order: NOT PROTECTIVELY MARKED, PROTECT, RESTRICTED and CONFIDENTIAL.

Educational organisations will typically use NOT PROTECTIVELY MARKED or PROTECT, with some data being RESTRICTED. Section 5 contains guidance on working out the correct protective marking.

Organisations should control access to protected data according to the role of the user. For example, organisations should not as, a matter of course, simply grant every member of staff access to the whole management information system.

[3] http://www.cabinetoffice.gov.uk/reports/data_handling.aspx
[4] http://www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx

Educational organisations should encrypt any data that is marked as PROTECT[5] or higher if this data is removed from, or accessed from outside, any approved secure space. Examples of approved secure spaces include physically secure areas in schools, colleges, universities, local authorities and the premises of support contractors. Educational organisations should also encrypt data marked as PROTECT or higher when it is in transit from one location to another, including transit from one approved secure location to another.

In most cases, electronic transmission (using encrypted email or FTP, for example) and storage of data in electronic format is more secure than paper-based systems.

Where, for example, schools or colleges use managed services for ICT, they should consult their supplier on how to achieve this.

All paper-based secured data should have a header or footer printed on each page containing the Protective Marking. Where paper reports are produced from management information systems organisations should find out from the supplier what their plans are to achieve this automatically. Where printed material is marked as PROTECT or higher, it should be secured in a lockable area or cabinet.

[5] For further information on the meaning of the term PROTECT, please see Section 5.

3 Carrying out an information risk assessment

To manage information risk effectively, organisations should carry out a risk assessment. This will show what security measures are already in place and whether they are the most appropriate (and cost effective) available. *ISO/IEC 27005*[6] contains a guide to putting in place a full risk management system.

Carrying out an information risk assessment will generally involve:

- recognising which risks are present
- judging the size of the risks
- prioritising the risks.

Once an organisation has assessed the risks, it can decide how to reduce them or to accept them.

However, risk assessment is an ongoing process, and organisations will need to carry out risk assessments at regular intervals as risks change over time.

3.1 Recognising risks

Organisations should start by listing all the personal and critical information assets they hold. They should then assign each information asset (examples of information assets include the organisation's MIS or the finance system) to an Information Asset Owner (IAO). IAOs play a key role in risk assessment, and more details on their role are available in *Good practice in information handling: Keeping data safe, secure and legal*[7].

Organisations should use their list of assets to identify possible threats to data security. Threats may be deliberate or accidental and can come from many sources, ranging from physical threats such as flooding or fire damage, to human threats such as theft, hackers, criminals or poorly trained staff. *BS ISO/IEC 27005* provides a detailed list of possible threats. The Open Security Foundation [http://datalossdb.org], which monitors public reports of data loss worldwide, reports that for UK public sector organisations (including education), threats arise mainly from lost documents or lost portable media. Stolen or lost laptops are also frequent sources of breaches, with breaches of web security and insufficient destruction of disposed data being occasional causes.

Organisations will already have some measures and controls in place to reduce the risk from the threats they have identified. For example, critical data may already be

[6] http://www.bsigroup.com/en/Shop/Publication-Detail/?pid=000000000030117274
[7] Available from http://www.becta.org.uk/schools/datasecurity and http://www.becta.org.uk/feandskills/datasecurity

regularly backed up and held securely off-site, and server hardware may be located in a physically secure location. Organisations will already control and restrict access to management information systems, may anonymise sensitive data, and may enforce the use of strong passwords, and restrictions may be in place discouraging the copying of data to personal mobile devices or portable media.

However, organisations should check that any existing measures or controls they have in place are both applied and effective. Failing measures or controls do not reduce risk.

Existing security measures or controls that do not adequately reduce threats create vulnerabilities that organisations need to examine closely. Organisations should consider the consequences of someone exploiting a vulnerability or set of vulnerabilities. In other words, assume a security breach has happened and think through the consequences (impact). At this point in the risk assessment, organisations should use the *Government Protective Marking Scheme*[8] (and associated Impact Levels) to help them establish the consequences of a security breach. Details about the scheme and Impact Levels follow in Section 4 of this document.

3.2 Judging the level of risk

Judging the level of a risk involves judging both the likelihood and the consequences of any given risk. This is a difficult task, and the outcome will depend on the individual institution. However, Table 1 may help organisations to qualify risk levels. This uses Protective Marking categories to qualify the potential consequences of a risk occurring and combines them with likelihood to indicate an overall risk level of low, medium or high. These terms do not quantify the level of risk, since this can only be assessed by each organisation, but should help organisations prioritise the risks that they identify. For more information on Protective Markings, see Section 4.

Table 1: Combining protective marking and likelihood to give an overall risk level

	Very unlikely	Unlikely	Possible	Likely	Frequent
PROTECT	Low	Low	Medium	Medium	Medium
RESTRICTED	Low	Medium	Medium	Medium	High
CONFIDENTIAL	Medium	Medium	Medium	High	High

[8] http://www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx

3.3 Prioritising risks

Organisations should use their lists of risks and associated levels to identify the risks they need to address as a matter of priority. The higher the level of risk, the higher the priority must be to tackle it. A simple information risk actions form is shown in the Appendix.

4 The Government Protective Marking Scheme and Impact Levels

Security breaches can:

- release confidential data
- make data inaccurate or incomplete
- stop data being available for organisations to use.

Security professionals call these losses of confidentiality, integrity or availability.

The Cabinet Office recommends applying the *Government Protective Marking Scheme*[9], to indicate how confidential the data in a document is. Becta recommends that educational organisations apply the scheme to both paper and electronic documents.

The Government Protective Marking Scheme has six categories of confidentiality: NOT PROTECTIVELY MARKED, PROTECT, RESTRICTED, CONFIDENTIAL and, at the highest level, SECRET and TOP SECRET. Only the first four categories are applicable to educational organisations, which will typically use NOT PROTECTIVELY MARKED or PROTECT, with some data being RESTRICTED. Section 5 contains guidance on working out the correct protective marking.

As the Government Protective Marking Scheme does not show the impact of security breaches on the integrity or availability of data, the Cabinet Office also recommends assessing the *Impact Level* of data. The Government Protective Marking Scheme can be mapped against Impact Levels, and this is shown in Table 2.

Table 2: Mapping the Government Protective Marking Scheme against Impact Levels for confidentiality

Government Protective Marking Scheme label	Impact Level (IL)
NOT PROTECTIVELY MARKED	0
PROTECT	1 or 2
RESTRICTED	3
CONFIDENTIAL	4

Details on both Impact Levels and the Government Protective Marking Scheme have been included in this document as organisations may still come across Impact Levels when dealing with other organisations in the public sector. However, Becta recommends that educational organisations apply protective marking for their data, rather than using Impact Levels.

5 Working out the appropriate Protective Marking for data

Educational organisations should use information risk management to help them look after the security of personal data, sensitive personal data and data that is critical to the organisation.

Protective marking is designed to identify – and protect – data that falls into these three categories. The simplified process described below will help organisations to choose the appropriate protective markings by carrying out the first few stages of an information risk assessment.

Step 1

Imagine a potential security breach, and consider:

1. Will it affect any member of the public?
2. Will someone lose more than £100?
3. Will it cause any kind of criminal case to fail?
4. Is there a risk of discomfort to someone?
5. Is anyone's personal safety at risk?
6. Will it embarrass anyone?

If you answered **no** to **all** the questions, a document can be labelled as **NOT PROTECTIVELY MARKED**. This shows everyone that you have assessed it. If you answered **yes** to any of the questions, the document requires a higher level of protective marking.

Step 2

Imagine the *same* potential security breach as above, and consider:

1. Will it affect many members of the public and need extra resources locally to manage it?
2. Will an individual or small trader lose £1000 to £10,000?
3. Will a serious criminal case or prosecution fail?
4. Is someone's personal safety at a moderate risk?
5. Will someone lose his or her reputation?
6. Will a large company or organisation lose £100,000 to £1,000,000?

If you have answered **yes** to **any** of the above questions, mark your document as **RESTRICTED**. However, if you think that the potential impact *exceeds* that stated in

[9] http://www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx

the question (for example, someone's personal safety is at high risk) mark your document as **CONFIDENTIAL**.

Step 3

Mark all documents that **do not fit** NOT PROTECTIVELY MARKED **or** RESTRICTED as **PROTECT**. Where there is concern that a document *might* require a higher level of protection, organisations should err on the side of caution.

In general, most of your documents and data should be either NOT PROTECTIVELY MARKED or PROTECT.

6 Applying protective marking

Becta recommends that organisations mark all documents, whether electronic or paper. This section outlines good practice in achieving this.

6.1 Protective marking terminology

Becta recommends that educational organisations use the terms in the Government Protective Marking Scheme. In increasing order these are:

- NOT PROTECTIVELY MARKED
- PROTECT
- RESTRICTED
- CONFIDENTIAL.

It is common practice to put protective markings in the footer or header of documents, as in this document.

6.2 Destruction markings

Organisations may include extra handling instructions to help staff remember to securely delete or destroy data. These could be part of the labelling scheme organisations use, such as including destruction markings in the footer of a document.

Schools can find guidance on how long to keep data in *Records Management Toolkit for Schools* [http://www.rms-gb.org.uk/resources/848] from The Records Management Society.

6.3 Examples of protective marking in practice

6.3.1 Learner details exported from the MIS

A typical export of learners' details from the management information system (MIS) might include sensitive personal data such as medical data and notes and ethnic origin. Organisations should mark any electronic or printed exports of this data with the appropriate protective marking (likely to be either PROTECT or, in some cases, RESTRICTED). Organisations may also add extra notes (see above), instructing handlers to securely delete or destroy the data after use.

6.3.2 Emergency contact information for a field trip

Staff need to take emergency contact/medical data with them when taking learners on a field trip. The data may be held on paper, electronically, or both. Organisations should ensure that staff keep the data as secure as is practical. However, they should balance this against the need to make sure that the data is readily available to staff they need it. Staff should make sure that they securely destroy the data when they no longer need it.

7 Electronic document storage and transfer

7.1 Storage and access control

Access to any data or documents marked PROTECT or higher will need to be controlled by the organisation. Where documents are in printed form, they should be secured in a locked cabinet or area, and access restricted to appropriate personnel only. Access to electronic data or documents needs to be controlled by effective access rights set by the system, and backed up by ‘strong’ passwords.

Data that is marked PROTECT or higher should be stored in separate system folders or directories, and not share folders with documents with lower markings. This will help to restrict access to authorised people.

Access to RESTRICTED data should be secured by two-factor authentication which combines something specific to an authorised person (such as a fingerprint or a token key fob) with a password, to authenticate that the user is who they claim to be.

7.2 Transfer

Frequently, organisations need to move documents between systems, when making returns to the local authority or awarding bodies, for example, or when learners transfer between schools. Organisations should make sure that they maintain protective markings and that the overall level of risk of a security breach does not increase because of the move. All data that is marked ‘PROTECT’ should be encrypted before transfer.

If organisations wish to move personal data across national borders, they must consider international laws and regulations. For example, different rules apply to transferring personal data between European Economic Area (EEA) countries to moving data from the EEA to non-EEA countries. For more information, see the ICO website [http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx].

8 Considerations for schools on data security and online information

The requirements for schools to enable online reporting to parents and remote access to learning platforms will also involve considerations of data security. At the same time, schools should promote the use of an integrated range of technologies such as websites, learning platforms, portals, email and text messages in order to encourage parental engagement with children's learning. Table 3 shows some of the ways that schools can exploit ICT while at the same time ensuring data security.

Table 3: Data security and online information for parents/carers

	Typical information	Technology available	Notes on Protective Markings
School life and events	School term times, holidays, training days, the curriculum, sports events and results, extra-curricular activities, events, displays of pupils' work, lunchtime menus, extended services, parent consultation, homework resources, school prospectus	Common practice is to use publicly accessible technology such as school websites or portals, and downloadable or emailed newsletters. Services such as email and text messaging can also provide updated information where parents opt for this.	Most of this information will fall into the NOT PROTECTIVELY MARKED category.
Learning and achievement	Information on how parents can support their individual child's learning, individual learners' academic achievements, assessments, attainment, progress with learning, learning behaviour, personalised curriculum and Individual Education Plans for learners with special educational needs	Schools will make information available by parents logging on to systems that provide them with appropriately secure access. Examples include: a secure area of the school's network, a learning platform, or access through a portal to management information system data. Schools could also send communications to a personal device or email account belonging to the parent/carer.	Most of this information will fall into the PROTECT category. There may be learners whose personal data requires a RESTRICTED marking or higher (for example, the home address of a child at risk). In this case, the school may decide not to make this learner's record available in this way.
Messages and alerts	Alerts and messages regarding information held by the school, such as individual learners' attendance, behaviour and special educational needs.	Email and text messaging are increasingly used by schools to contact and inform parents. Messaging systems integrated with management information systems and learning platforms are able to manage what information is available online or sent to parents using email and text messages. Learning platforms or portals might be used to provide secure access to further detail and context.	Most of this information will fall into the PROTECT category. Although it may be possible to encrypt email or text messages to parents, schools should not send detailed sensitive information in this way. A telephone call or face-to-face meeting may be more appropriate.

Appendix

Information risk actions form

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