

Good practice in information handling in school

Impact levels and labelling

A guide for staff and contractors tasked with implementing data security

Contents

1 Key points3

What data needs to be protected?	3
What measures should schools take?	3
The importance of protective marking	4

2 The Data Protection Act5

3 Determining impact levels6

3.1 Individual data items versus aggregated data	7
3.2 Derivative classification	7
3.3 Implicit or default labelling	7
3.4 Reducing the risk.....	8

4 Information marking and handling8

4.1 Protective labels – headers	10
4.2 Release/destruction markings	10
5.3 System-wide labels	10

5 Document handling, storage and transfer11

5.1 Document storage.....	11
5.2 Document access.....	11
5.3 Document transfer.....	11
5.4 Implementation strategies	12
5.4.1 User interface	12
5.4.2 Administration and privileged operations	12
5.4.3 Emulating mandatory access controls	13
5.4.4 Auditing.....	13
5.5 Printed documents	14

6 Recommendations and requirements14

Appendix A – Impact Levels for protected data15

Adapted for education	15
-----------------------------	----

1 Key points

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. Legislation covering the safe handling of this data is addressed by the UK Data Protection Act 1998 and, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, *Data Handling Procedures in Government*. This stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that they adopt these procedures too.

The aim of this document is to describe how personal data should be classified by schools in order to maintain its security, by selecting appropriate protective markings or Impact Levels. This guidance applies to the access to, storage, transmission and destruction of all personal data, both paper-based and electronic.

What data needs to be protected?

The key issue is the identification of all personal data that is sensitive – that is, data whose release or loss could cause harm or distress to the individual(s) it concerns. School management information systems, learning platforms and portals store – or are used to access and aggregate – data across a plethora of systems. Most of these systems use sensitive data (the Unique Pupil Number, User Interface Privilege Isolation or Unique Learner Number, for example, or combinations of sensitive data in student names and dates of birth) to create a unique identifier within the particular application.

The sensitive nature of the data held in schools means it is therefore subject to the requirements of the Data Protection Act according to the classification or Impact Levels of the data in question.

What measures should schools take?

It is a legal requirement to protect sensitive data, and *Data Handling Procedures in Government* sets out the measures that schools should adopt to maintain data security:

- Users may not remove or copy 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 (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Sensitive or personal data must be securely deleted when it is no longer required.

For schools, this means that they must encrypt any data that is classified as Impact Level 2 (IL2–Protect) or higher if this data is removed or accessed from outside any approved secure space such as a school, local authority or premises of contractors such as suppliers of managed services. Education organisations must also ensure that data classified as IL2–Protect or higher is encrypted when it is in transit from one location to another, including transit from one approved secure location to another.

The importance of protective marking

In order to comply with Data Handling Procedures in Government, every school will need to have a policy and procedures for identifying sensitive or personal data and assessing its impact level.

Schools therefore need to:

- have an understanding of:
 - what items require labelling as sensitive
 - how data that is not intrinsically sensitive can become sensitive when combined with other pieces of data
- ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher
- comply with the requirements for the safe destruction of sensitive data when it is no longer required
- be aware that the user producing the information is individually responsible for determining the Impact Level classification and applying the appropriate Label and Release Marking.

This document is intended for those staff or contractors in schools who are tasked with implementing a system of protective marking and labelling of data. It contains:

- a summary of the requirements of the Data Protection Act
- an overview of how you should determine the Impact Levels of your data
- guidance on information marking and handling
- good practice in document handling, storage and transfer

- an appendix containing a matrix illustrating the remote access requirements for accessing protected data at different Impact Levels.

2 The Data Protection Act

The Data Protection Act 1998 came into force on 1 March 2000 to bring the UK in line with a European Community Human Rights directive and achieve a common standard of protection across Europe. The purpose of the Act is to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data.

The Act applies to personal data (information that applies to a living person) whether it is held on a computer system or on paper. There are particularly stringent rules surrounding 'sensitive' data such as pupil identifiers, pupil characteristics, special educational needs, health, religious beliefs, ethnic background, home address and criminal offences.

The Act requires that data is processed in accordance with certain principles and conditions. Personal data can only be processed under one or more of the following rules:

- 1 An individual has given consent
- 2 It is part of a contract
- 3 It is a legal obligation
- 4 It is necessary to protect the individual
- 5 It is in the legitimate interests of the data controller

For processing sensitive data, whilst explicit consent must be obtained in many contexts, it is not necessary if there is a clear business purpose. Within the education sector, for the purposes of delivering an education, consent is not required, however, the reasons for collecting and processing personal data must be completely transparent.

Every item of personal data that is held or processed must be accurate and up to date, and held for no longer than necessary. When 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 destroyed in accordance with the relevant Impact Level of the data.

The security of personal information must be maintained and any disclosure of personal data must be properly authorised. There are specific consent requirements in respect of 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>].

It is a legal requirement to protect sensitive data. Individuals entrusted with protected data, however derived, are accountable for the protection and compliance with the laws. This is enforceable through local human resource processes and failure to comply may be construed as gross misconduct and could face prosecution.

Any security policies and procedures that have been mandated in any contractual relationship with third parties or suppliers will also need to cover the protection of sensitive data.

3 Determining impact levels

The combined force of the Data Protection Act and Data Handling Procedures in Government make it critical for schools to recognise the sensitive data they hold and apply appropriate levels of protection to it. To ensure a uniform method of assessing the impact of potential compromises to the confidentiality, integrity or availability of information and information systems, and provide comparable levels of information protection when the data is shared, Business Impact Levels tables have been devised. All data – electronic or on paper – should be labelled according to the protection it requires, based on these Impact Levels.

CSIA level		Impact level
CSIA Level 0	equivalent to	IL1–Not Protectively Marked (IL1–NPM)
CSIA Level 1	equivalent to	IL2–Protect
CSIA Level 2	equivalent to	IL3–Restricted
CSIA Level 3	equivalent to	IL4–Confidential

The following table illustrates the assignation of Impact Levels for Distress to the Public.

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
None	Likely to cause embarrassment to an individual or organisation	Likely to cause loss of reputation to an individual or organisation	Likely to cause embarrassment or loss of reputation to many citizens or organisations	Likely to cause long term (eg months) or permanent loss of reputation to many citizens or organisations	Likely to cause major long term damage to the UK population

Where data in schools is protected, this is generally classified as either IL2–Protect or IL3–Restricted. The vast majority of typical school MIS reports or teacher access is to data that is protected at IL3–Restricted level.

3.1 Individual data items versus aggregated data

Information, or data, classification is the mechanism used to assign a value to a single data item or attribute in order to determine the security controls required to protect it. How this mechanism works is clear when value can easily be assigned – for example, employee salary may range between £0 and £50k.

In most cases, however, the value can only be assigned subjectively through some form of risk analysis: how much damage will ensue if this data item is compromised in some way? For single data items this can be relatively simple to assign. For multiple data elements combined in a management report (a standard school MIS report, for example), the level of information sensitivity can be much higher.

When a data item at one Impact Level is combined with other data at the same level, the Impact Level of the whole collection is often significantly higher than the Impact Level of the compromise of any single item. For example, losing a class of pupils' records is potentially more damaging than losing a single individual's records; losing the whole school's records is correspondingly more damaging than that of a class and so on.

The combination of particular data elements is what determines the appropriate protective marking as well as the remote access security requirements. This is particularly critical when certain data – relating to special needs, looked-after children, or children at risk, for example – is combined from various sources, including external agencies. In this case, the originating agency's classification (or higher) should be applied for these aggregated reports.

3.2 Derivative classification

Derivative classification is the incorporating, paraphrasing, restating or generating in new form, information that is already protectively marked (producing a report from a school MIS, for example). The marking of the new report is consistent with the classification of the source material (typically IL3–Restricted) unless in its aggregated form it requires a higher classification – in which case the material is to be reclassified.

3.3 Implicit or default labelling

Owing to the complexity of classifying reports generated from protectively marked data, it is recommended that educational ICT systems are 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 implicitly labelling is included as

part of the functional specification and ICT requirements. If it is not available, vendors should be required to demonstrate how they will deliver this functionality within a reasonable timescale.

Note that access to protected data must be controlled according to the role of the user. Not every member of staff should need access to the whole MIS.

Becta is working with suppliers to investigate solutions for the incorporation of implicit labelling within MIS and learning platforms. Where systems are interconnected, appropriate security must be provided in the end system (that is, the system that aggregates the data), together with supporting procedural measures.

As of September 2008, the vast majority of systems do not enforce data protection on the basis of Impact Level labels.

3.4 Reducing the risk

As mentioned above, it can be complex to determine the Impact Level value of aggregated information. The purpose of information classification, however, is to determine the security controls that are required to mitigate against risk; that is, remove this from the equation. Thus with the proper security controls in place, the effect of aggregation will be reduced or removed.

For example, for information classified as IL4–Confidential, applying the specific controls limiting movement, access and audit will help mitigate against the risk of loss.

Encryption will, in most circumstances, reduce the risk to zero as the scrambled information (at data item level) has no value at all. It is therefore a very strong control to mitigate against both risk and impact.

4 Information marking and handling

All documents that contain protected data must be labelled as such with clear handling notes. This section outlines good practice as to how this can be achieved.

Information labels and release markings (including destruction) must be associated with each protected data element. This applies to both electronic and paper-based records. The figures below illustrate the use of protective labels and release markings.

Student Details: Ben Abbot **IL 3 Restricted**

Basic Details Registration Family/Home Medical **Ethnic/Cultural** Additional Information History

Medical

Doctor: Dr D Bell
East Town Community Clinic
Telephone - 855019

Emergency Consent:

NHS Number: ABCD 24 Blood Group: A+

Medical Notes:

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

Ethnic/Cultural

Ethnicity: WBRI - British Ethnic Data Source: Parent

Home Language: English Religion: Christian*

Mother Tongue: English English Additional Language: No

National Identity: British Speaks Welsh: Information Not Obtained

Nationality and Passport Details:

Nationality	Passport Number	Passport Expiry date

Securely Delete or Shred

In this example MIS screen, the data is protected at IL3-Restricted because the user is able to access medical data elements including the pupil's NHS Number

Individual Education Plan						IL 3 Restricted
Name	Ben Abbot		DOB 17/01/1986	Year Year 13	Class G	
Area/s of concern	Communication		UPN U820432190122	IEP Number		
Class Teacher.	Mrs Abell	Start date	Apr 2004	Review Date	28/05/2004	
Supported by	Mr Skeggs	Proposed Support	Speech Therapist	Support began	24/03/2004	
Targets	Achievement Criterion	Possible resources and techniques	Possible strategies for use in class	Ideas for support staff	Outcome	
1 To look at the teacher when named.	1 Observed in 1:1 / small group / class situation on several occasions.	1 Reward system. Monitor sheets. Name games. Praise.	1 Use Ben's name to start a sentence. Reinforce correct behaviour with praise.	1 Play name games with Ben. Eye contact to be established before game continues.	1	
2 To be able to stop what he is doing and listen to the teacher speak.	2 Observed on many occasions.	2 Visual or auditory cue.	2 Try to make sure that Ben's attention has been gained before speaking.	2 Sit near Ben and prompt him to stop what he is doing and listen.	2	
Parent / carer contribution Call Ben's name and wait for eye contact before speaking.						
Student's contribution Look at the teacher when his name is called.						

Copy for parent / teacher / support / file

Securely Delete or Shred

This printed individual education plan (IEP) must be classified at IL3-Restricted because it contains the pupil's unique pupil number (UPN), a data element by itself classified as IL3-Restricted.

4.1 Protective labels – headers

Information labels typically used in the educational sector are IL2–Protect and IL3–Restricted. Labelling should follow practices as defined with the UK Government protective marking scheme and the ISO 15408 Common Criteria .

[Impact Level n],		[Classification],		[Optional].
Impact Level (IL) is the Impact descriptor		Classification refers to the narrative IL descriptor		Optional is a descriptor tailored to the specific category
Example: IL3		Restricted		Identifies individual

Becta recommends a clear method of showing the labels that are applicable in schools and should be placed in the header within documentation. For example:

4.2 Release/destruction markings

Similarly, in order that protected data is securely deleted or destroyed, Becta recommends that it should be marked within the footer as below.

[Release],		[Parties],		[Restrictions].		[Encrypt, Securely delete or shred]
The authority descriptor		The individuals or organisations the information may be released to		Descriptor tailored to the specific individual		How the document should be destroyed
Examples:						
Senior Information Risk Owner		School use only		No internet access No photos		Securely delete or shred
Teacher		Mother only		No information to father ASBO		Securely delete or shred

5.3 System-wide labels

As the majority of the existing school MIS and learning platforms do not have built-in labels, they must be explicitly specified. A general practice is to label the entire system and all output from that system at the highest classification level

'System High' mode of operation applies to a system when each user has clearance for all of the data on that system; however, not all of the users have a valid need-to-know for all of the data on the system.

This system-wide label is the most effective way to protect legacy systems that cannot be changed to meet current security requirements.

Non-hierarchical components are usually held as sets of categories or compartments. Accesses here are made based on whether one set is a superset of another (dominates). For a user to have permission to amend or add to this data, both sets must be equal; if, for example, you are granted access to IL-2 data you cannot access IL-3 data because level 2 is lower than level 3.

5 Document handling, storage and transfer

5.1 Document storage

It is important that an ICT system handling protected data is able to label information based on its sensitivity.

Firstly, there is the need to hide the existence of files from unauthorised users, and secondly, many systems place restrictions on the labels of files in a file/directory hierarchy, which make the mixing of files with different labels difficult.

Having separate directories at the correct levels also makes the automated copying and labelling of data easier to enforce.



5.2 Document access

Users must be assigned a clearance that will determine which files are accessible to them. If the existence of files will also be restricted, then the application must have some way of enforcing this (by only searching in the appropriate directories, for example).

Files can be stored in directories that reflect their label (a directory labelled 'IL-2', for example) to facilitate this process.

5.3 Document transfer

Most complications will occur when documents are transferred between systems. The main issue here is ensuring that the appropriate label is maintained.

If the label configurations on the systems are compatible (ideally homogeneous), then the label can be simply reused, subject to ensuring that the representations are correct (that is, the same values are used).

The act of transferring data will also require security policies to be enforced by each system to ensure that only particular data flows are allowed. For example, a link might only be suitable for a particular range of labelled documents.

When transfer across national borders is involved, international laws and regulations will also need to be considered. Whilst it is perfectly legal to transfer personal data between European Economic Area (EEA) countries for example, the same is not true when exporting data from the EEA to non-EEA countries. In this case, the label could be enhanced to include a country identifier in order that such data flows can be strictly controlled.

5.4 Implementation strategies

5.4.1 User interface

The addition of labels to a document management system or MIS goes beyond just adding the ability for users to select an appropriate label from a drop-down list. It is also critical to design the user interface carefully to ensure the correct label is assigned if the user is to have any choice over which label to apply.

A complex labelling system may confuse users and lead to mislabelling, which could have dangerous results. Labels themselves can be simplified via the use of aliases, so that a more understandable version can be displayed. Colour and symbols can be used to enhance the displayed labels to ensure that the potential for confusion is reduced.

Built-in safety can be enhanced by setting a 'safe' default where users are given a choice. If the system can ascertain the correct label it must do so, equally if it can reliably guess then it should do so. For example, the most sensible default for most users is likely to be the label assigned to them at log-in.

It is also important that the application should confirm label usages that involved downgrading an Impact Level from IL3 to IL2 (that is, to a less sensitive and therefore less protected level), and those that involve the assignment of very sensitive labels. In the former case, there is a risk otherwise of a security breach, and in the latter case, once highly sensitive (IL-4 and above) data has been mislabelled, it may be difficult to subsequently assign the correct label.

5.4.2 Administration and privileged operations

Administration on systems implementing labels is more complex, especially if the administrators are not cleared to access the data they are managing.

If the file structure has been changed, the administrative procedures will need to be revised.

Similar problems will occur within the application itself. Most trusted labelling systems have measures in place to ensure that users cannot elevate their privileges by creating a new user with the higher privileges. These systems enforce separation of duties and therefore require multiple users to create a new user account. It is imperative that you ascertain if your applications and system enable the functionality of trusted labelling.

Other problems will occur in a document management system or MIS if documents are changed, and therefore need to be re-graded, or if the wrong label has been assigned to a document. These are privileged operations and special measures need to be implemented to prevent abuse.

5.4.3 Emulating mandatory access controls

Although it is possible to emulate labelled systems, this is likely to be inferior to the 'real thing'. One area where it might be appropriate, however, is where a system operates at a single (as far as the label level is concerned) security level (the classic 'system high' configuration), but needs to be able to import and export data with other systems.

In this case, data flows would need to be established via an agent that can analyse the labels and enforce the information flows. This is possible using commercial application filtering gateways such as Microsoft's Internet Application Gateway. Implicit (default) Impact Levels are associated with the system, encoded in the IP header, and when passed between co-operating ICT systems the security policy enforces the classification and release markings.

An alternative to this is to encrypt each document with a key that is related to the label. This would allow all data to be exported (since only a legitimate user could read the contents) but this would require a PKI (Public Key Infrastructure) to support it.

5.4.4 Auditing

Labelled systems can only be fully effective when backed up by an equally high assurance audit system. This audit system must record all operations regarding labels.

Data Handling Procedures in Government outlines security requirements for logging activities of data users in respect of electronically held personal information and for appropriate responsible individuals to check it is being properly conducted. It has particular focus on those working remotely and those applications with higher levels of access (IL2 and above).

Note: Summary records must be shared with the applicable Information Asset Owner (IAO) and be available for inspection by the UK Information Commissioner's Office on request.

5.5 Printed documents

Printed documents require labels that appear on each page of protected data, in the header and footer. Typically, they should be produced by the system as a system-wide implicit label for any protected data produced from these systems at the system classification level.

6 Recommendations and requirements

- All education ICT systems must be classified for the highest level data processed by the system and automatically labelled at the corresponding level. This will generally be IL3–Restricted.
- For organisations that share protected data, a uniform method of labelling is required because each organisation must be confident that the shared information is managed equivalently. For schools, this will require a method that is uniform with their local authority.
- All paper-based protected data must 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, or accessed remotely, from the school or other relevant government or commercial premises.
- All IL2–Protect and IL3–Restricted printed material must be held in a lockable storage area or cabinet.
- Protected data at IL2 or above, in either paper or electronic form, must be disposed of in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten (at least seven times) and other media must be shredded, incinerated or otherwise disintegrated.

Appendix A – Impact Levels for protected data

Adapted for education

Impact Level	Example data types	eGIF requirements		Example networks	External access			
	Aggregated reports	Registration level	Authentication requirements		Gov PC to www	Internet café	PDA	Home Gov PC LAN
					Wi-fi	3G card	Bluetooth	Bootable USB
IL4 Confidential	<ul style="list-style-type: none"> National Pupil Database Looked-after children Witness protection SEN IL4 data elements 	Level Three ID verification with vetting and 'need to know' measures	Physical/ personal/ procedural protection with appropriate authorisation	GSI CJX	Y ¹	N	N	Y ²
					N	N	N	Y ³
IL3 Restricted or NHS Confidential	<ul style="list-style-type: none"> School MIS Teacher access to learning platform/ portals Special educational needs (with no IL 4 data elements) Pupil characteristic Contact point Health records 	Level Two ID vetting and 'need to know' measures IAO approval	Mandatory two-factor user ID, password and token Internet/virtual private network (VPN) and token	N3 GSI GCSx CJX	Y	N	Y ⁴	Y ⁵
					Encrypted internet VPN	Y ⁶	Y ⁷	N
IL2 Protect	<ul style="list-style-type: none"> General student data Learning platforms/ portals 	Level One basic ID verification	User ID and password	Internet	Y ¹	N	Y	Y
					Y	Y	Y ²	Y
IL1/ IL0	<ul style="list-style-type: none"> Google search BBC News 	Anonymous	Authentication not required	Any	Y	Y	Y	Y

- 1 Via thin client internet browse-down
- 2 Via hard-wired Government-issued secure laptop (RAS)
- 3 Requires a strong business case and CESG advice
- 4 Via CESG-approved product such as Blackberry
- 5 Via CESG-approved VPN or validated Manual T or Manual V solutions
- 6 Implementations must be compliant with CESG Manual Y
- 7 Via Government issued secure laptop with software encryption (RAS)
- 8 Using software-based cryptography
- 9 Requires strong business case and CESG advice