

**AMI Education  
Solutions Ltd**

Data Handling in  
Schools

White Paper

## Contents

<b>INTRODUCTION .....</b>	<b>3</b>
<b>IMPACT LEVELS AND LABELLING .....</b>	<b>4</b>
<b>DATA ENCRYPTION .....</b>	<b>5</b>
<b>AUDIT LOGGING AND INCIDENT HANDLING.....</b>	<b>6</b>
SECURITY EVENT AUDITING .....	7
SECURITY INCIDENT RESPONSE.....	8
<b>REMOTE ACCESS .....</b>	<b>9</b>
<b>RANGER SOLUTIONS .....</b>	<b>10</b>
RANGER FOR NETWORKS.....	10
RANGER OUTPOST .....	10
DEVICESHIELD.....	11

## Introduction

Data protection legislation states that all those who hold personal data, whether on paper or electronically, must keep that data secure. This also applies to schools. **Personal data** is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This includes; **names, contact details, gender, dates of birth, unique pupil number (UPN)** and so on, as well as other sensitive information such as academic achievements, other skills and abilities, and progress in school. It may also include behaviour and attendance records.

Following a [Cabinet Office Report](#) the procedures outlined in this report have been cascaded down to public bodies such as Becta. Becta have in turn worked with the Department for Children Schools and Families (DCSF), the Information Commissioner's Office, schools and suppliers to produce information handling security good practice guidance to reflect the procedures in the Cabinet Office Report.

Becta have produced [5 Documents](#), an introductory document and 4 good practice guides addressing aspects of data handling:

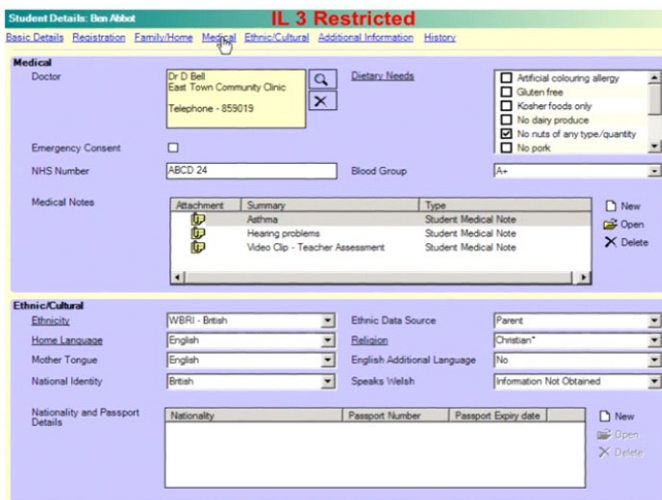
- Impact levels and labelling
- Data encryption
- Audit logging and incident handling
- Secure remote access.

The following précis outlines the key areas of each of the guides and discusses how Ranger can help schools meet their data handling requirements.

# Impact Levels and Labelling

All documents that contain protected data must be labelled clearly including a measure of their sensitivity referred to as its Impact Level. 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.

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. 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).

**Securely Delete or Shred**

Figure 1 - Impact Level and Release Marking

Individual Education Plan						IL 3 Restricted			
Name	Ben Abbot		DOB	17/01/1986	Year	Year 13	Class	G	
Area/s of concern	Communication		UPN	US20452190122		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				
<b>Parent / carer contribution</b> Call Ben's name and wait for eye contact before speaking.									
<b>Student's contribution</b> Look at the teacher when his name is called.									

Copy for parent / teacher / support / file

**Securely Delete or Shred**

Figure 2 - Impact Level and Release Marking

## Data Encryption

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.).

- 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.
- Authorised users accessing data from outside the school premises must do so by secure remote access
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Organisations or users must securely delete sensitive or personal when it is no longer required.

The data encryption guide makes it clear that all schools need to act now to ensure data encryption solutions are in place:

***“... if your school does not have encryption now, you should stop all copying, removing or accessing protected data until you have software to encrypt files and protect the communication links accessing this data.”***

## Audit Logging and Incident Handling

Schools and local authorities must keep audit logs to provide evidence of accidental or deliberate security breaches. These could include loss of protected data or breach of an acceptable use policy. The first steps to implementing a basic infrastructure are;

- **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. Examples of systems to be audited are:
  - Web servers
  - Domain controllers
  - Learning platform web-servers
  - Web portal, database, query and index servers
  - Mail servers and web mail servers
  - File servers
  - Routers
  - Networked PCs and other connected devices
- **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 the data
- **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.

### ***Security Event Auditing***

Further to the requirement of Schools to audit their data, schools need to carry out **Security Event Auditing**. Security event auditing is the process of collecting ICT system events and reviewing the impact of these against security policy. The purpose of the audit is to identify any events that indicate suspicious activity. These would include, for example, users who repeatedly failed to log on; who logged on at unusual times; login from unknown remote systems; users who failed to open files or folders due to insufficient permissions; unusual use of admin privileges; and users who have repeatedly attempted to access system services, but failed due to insufficient privileges. Schools will need to audit and review their security configuration and will rely on their systems event logs to supply the facility to monitor activity.

The guide makes it clear that it is good practice to have a statement of intent that covers both the type and reason for monitoring, such as:

*“We are going to use monitoring to identify threatening behaviours including inappropriate use of resources or access to sensitive data, and attempts to circumvent policy across our network so that we can focus our limited resources on measurable threats.”*

Monitoring of this sort should be made clear in any staff handbook, and in any acceptable use policy for staff, together with the response that the school will take in cases of misuse.

### ***Security Incident Response***

Data Handling Procedures in Government stipulates that public sector organisations should establish a security incident response capability

A prerequisite for an effective security incident response is the detection of the security incident in the first place. Thereafter, the effectiveness of the response team should be measured based on the extent of damage that resulted from each incident. The sooner the incident is contained, the lower the risk of financial loss or data compromise.

Good practice highlights the following components for the successful resolution of an incident:

- Management commitment, in terms of human resources, budget and priority
- A resolution team of technical and legal experts
- Primary responsible person for each incident
- Communications plan, including escalation procedures and interfaces with inter departmental and law enforcement agencies
- 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

## Remote Access

Remote access requirements are based on data protection Impact Levels (IL). The Guide details a range of measures to ensure secure remote access. Together with the requirements of the Data Protection Act 1998, these measures place new obligations upon schools in relation to any data that is classified as Impact Level 2 (IL2–Protect) or higher if this data is removed or accessed from outside the school. 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. Providing secure remote access to educational systems and the protected data they contain requires multiple technologies that address:

- **Authentication** – who or what system is trying to connect (identity management); ensuring that the users and the computers at each end are who they say they are
- **Authorisation** – the types of tasks you wish to perform and ensuring that the users at the remote end are authorised to access the data
- **Geographical restrictions** – protected data may not be accessed remotely unless encrypted, and access requires specific network connection
- **Encryption** – to protect sensitive data in transit, and file or full disk encryption for any storage media that holds protected data
- **Audit** – logs of access to protected data must be held at evidential quality for seven years.

The majority of typical school management information system (MIS) reports or teacher access is to data that is protected at ‘IL3–Restricted’. Aggregating data elements into typical reports – data on special educational needs, for example – generally increases the Impact Level. General student data and Learning Platforms are designated IL2-Protect.

- **Remote Access to data designated IL2 requires User ID and password authentication.**
- **Remote Access to data designated IL3 requires Mandatory two-factor user ID, password and token**

A basic requirement for schools and/ or local authorities will be to configure secure remote access systems in a manner that facilitates the evidential quality collection and consolidation of event data related to remote access of protected data

## Ranger Solutions

As specialist suppliers to the education market Sentinel Products are well placed to assist schools to meet these new best practice guidelines.

### *Ranger for Networks*

Ranger for Networks provides schools with a simple solution to their PC network security, management and control. Real-world benefits in regard to the data handling guidelines are:

- Simple user friendly “out-of-the-box” security settings
- User and secure password creation/enforcement
- Event Monitoring
- Log File creation
- Automated response to network events and security risks
- Software Auditing
- Management Reporting

Ranger for Networks provides ICT technicians and administrators with tools that will assist them to quickly and simply meet key data handling commitments.

### *Ranger Outpost*

Ranger Outpost enables secure remote file access. The solution has been developed to enable students and staff to have access to their network files (general student data -IL2) off of the school network. The solution ensures that the security of the school network is not compromised through the following measures:

- Security against user spoofing - all connections secured using industry standard RSA 1024 bit public/private keys
- File access security - NT's file permissions provide server access security. Only authenticated users can access files
- Login security - user passwords are not passed across the Internet as an authentication public/private key pair system is used
- Data Encryption - all file transfers are encrypted using advanced RC4 encryption
- Limiting Access - users only have access to their home folder and designated network shared folders

Ranger Outpost also assists schools meet the key monitoring guideline for Remote Access by providing reporting tools to give schools complete visibility of remote access activities.

### ***DeviceShield***

DeviceShield safeguards the school network by monitoring real-time traffic and applying customised, highly-granular security policies over all physical, wireless and storage devices.

The solution will:

- Provide an audit of all file transfers on and off the network to any portable media device
- Provide automatic email updates of activity
- Enforce file encryption
- Centralise control
- Manage what devices can connect to the network
- Enable management reporting
- Restrict copying on/off network by file type
- Enforce read only access

### **More Information**

More information and free trials of the full suite of Ranger solutions are available online at <http://www.rangersuite.com>

*For more details and to download free software trials go to  
[www.rangersuite.com](http://www.rangersuite.com)*