# NEN – The Education Network

## Technical Strategy Guidance Note 1:

## Protecting Electronic School Data When Working Away from School

## November 2012

**Audience:** All staff working in schools that have access to personal data.

**Disclaimer:** Although every care has been taken in assembling the information and materials in this guidance note, the materials are for general guidance only and are not, and are not intended to be, legal advice. Before taking action that may have legal consequences, you should seek professional legal advice.

This guidance aims to assist school staff on how to deal with electronic information security when working away from the school site. The type of information is classified in three bands - red, amber and green - to help you understand the level of security for school electronic data. Each school should have a senior member of staff who is responsible for information security. It is the responsibility of all staff in the school to understand how to handle data securely. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action (leading to large financial penalty notices). Local Authority registration does not remove an individual school's responsibility to register as the controller of data in its school.

Here are 5 of the Data Protection Act (DPA) principles that all staff should be aware of:

- only collect information that you need for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as you need, and only for as long as you need it; and
- allow the subject of the information to see it on request.

This document is for guidance only and does not provide a complete list of the types of data available within schools.

**Types of RED data (this is SENSITIVE personal data):**

- Individual Education Plans
- Educational Psychologist reports
- Education Welfare Officer reports
- Medical records
- Personnel records
- SEN registers
- Government connect
- Accessing your Management Information System, admin servers

If accessing this type of data over the Internet it **must** only be done via a secure connection with two-factor authentication (where the user is required to enter two pieces of secret information). Only school owned devices should be used to access and store this type of data. Personal Internet enabled devices **must not** be used, including laptops/PCs, tablets. Any files transferred or emailed

**must** be encrypted and should never be stored on a USB stick. All laptops and PCs storing this level of data **must** have full drive encryption in case the device is stolen.

**Types of AMBER data (data contains personal data that, if lost, could identify individuals):**

- Names and addresses
- Parental contacts
- Pupil reports
- Exam Results

All these types of data can be stored and transferred on a school owned USB stick or laptop/PC/tablet but it **must** be encrypted. Data can be accessed by a school laptop over the Internet as long as a unique username and password is used. Personal devices **must not** be used.

**Types of GREEN data (data does not identify individuals):**

- Lesson plans
- Class lists (only showing initials and forenames)
- Curriculum plans
- General marking

All these types of data can be stored on an un-encrypted school or personal laptop/PC/tablet. This data can be stored and transferred by USB stick. This data can be uploaded to VLE/learning platform or school file area over general Internet connection but password access must be required to do this.

Passwords are often the weakest area in a school's electronic security. All staff, especially those dealing with sensitive personal data, need to have strong alpha/numeric passwords that they change frequently. Work passwords should be different from personal ones.

**Further help and support**

Your organisation has a legal obligation to protect personal information. Your senior management should be aware of their legal obligations under the Data Protection Act 1998. For more information, visit the website of the Information Commissioner's Office (ICO):

http://www.ico.gov.uk

The ICO has provided guidance for schools on the Data Protection Act 1998:
http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

To check or register your school as a data controller:
http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

The NEN E-safety Audit tool is designed to help senior managers in school assess their e-safety provision and gaps that may exist. It covers areas such as data security and password policies:
http://www.nen.gov.uk/esafety/13/nen-e-safety-audit-tool.html

Recent example of schools breaking the data protection rules:

Hampshire school breached data protection rules
http://www.ico.gov.uk/news/latest_news/2011/hampshire_school_breached_data_protection_rules_08082011.aspx

Laptop thefts highlight the need for encryption
http://www.ico.gov.uk/news/latest_news/2011/laptop-thefts-highlight-the-need-for-encryption-05102011.aspx