THE LATYMER SCHOOL

Founded 1624

DATA PROTECTION POLICY

Policy adopted	Full Governors' Meeting October 2011
Policy circulated	October 2011
Review policy	To be reviewed every 2 years

Legislation: The Data Protection Act 1998 (with consideration to the eight data protection principles appearing in Schedule 1).

DATA SECURITY GUIDELINES

INTRODUCTION

The school has a duty of care towards the processing and management of students' data in electronic form.

Staff use student data for a variety of purposes, for example, recording attendance, collecting money, contacting home, preparing assessment data and reports, health and safety information. Access is primarily made on site but often information is transferred off-site, for example, to complete assessments and reports.

GUIDELINES FOR STAFF

The Data Protection Act 1998 is much wider in scope than the 1984 Act which it replaced. In particular:

- The definition of "data processing" has been broadened to include collection, recording, holding, retrieval, consultation, use and disclosure of data.
- Certain types of data are now classed as "sensitive" [data relating to ethnicity, political opinion, religion, trade union membership, health, sexuality or criminal record of the data subject] and the requirements for processing such data are more stringent.
- New conditions affect transfer of data to countries outside the European Economic Area – publishing on the World Wide Web may fall into this 'data transfer' category.

The intention of the Act is not to prevent data processing, but to ensure that it is done fairly and without adverse effect on the individual the data relates to. To this end, the Act lays down specific conditions for processing personal data.

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that access to the data must be restricted. All staff should ensure that:

- Computerised information is password-protected.
- Passwords must be set-up and changed according to the password policy (see below)
- Computer monitors are sited so that they are not visible except to authorised people. Screens must not be left unattended when personal data is being processed.
- Data storage devices (e.g. USB pens, portable hard drives) must be kept securely.
- Personal computers in the home where personal data is accessed must be password protected. Staff laptops are password protected and are best used for working with personal data.
- Treat "sensitive data" with extreme care

PROCEDURES IN PLACE AT THE LATYMER SCHOOL

Password policy

The school network logins require a password policy. The password policy is:

- All users must have a password
- Passwords are case-sensitive
- Password must meet complexity requirements
- Not contain all or part of the user's account name
- Be at least eight characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)

The FULL password policy can be found in the Staff Handbook under the ICT Policy.

Disposal of hardware and destruction of data

Hardware must be disposed by the ICT Team. **Lee Surrey** (ljs@latymer.co.uk) is the point of contact within the ICT team for this. All obsolete equipment is then passed to a third party disposal service provider to dispose of the equipment in line with the Waste Electronic & Electrical Equipment (WEEE) directive. This ensures that any remaining data is removed from the PC's hard drive.

Media Destruction Techniques

Media, which is no longer required (or has passed its effective reuse period), should be dealt with appropriately. Any of the techniques described for the destruction of media must only be undertaken by the ICT Team.

CD-ROM and DVD Destruction

Teachers/ staff may have stored personal data on a CD/ DVD e.g. video of school play, photographs of school events, audio recordings. The construction of plastic media such as CDs makes them particularly vulnerable to damage if handled roughly. Most CDs and DVDs are simply a plastic base with a laser sensitive substrate applied to one side. All redundant CDs and DVDs must be disposed of using the designated shredding machine located in the IT office.

Solid-State Devices

Examples of solid-state devices are USB pen drives or memory storage cards for PDA's, digital cameras, video cameras and other handheld devices. Due to the compact nature of their internal makeup, the complete physical destruction of the device is required to ensure that any recovery of data is impossible. Such devices should be physically destroyed. This ensures that it is not possible to reuse any aspect of the internal storage mechanism.

Magnetic Tape Backup

The most effective method for the destruction of magnetic tape is the disintegration or shredding of the tape media. Physical destruction of the tape casing will then occur.

Encryption Procedures

USB Pens

If you wish to use a USB pen to carry personal data between school and home you must use encryption software. This software requires a password to access the USB pen.

See **Lee Surrey** (ljs@latymer.co.uk) for further advice or to obtain an encrypted USB pen for this purpose.

Staff Laptops and other school machines

Encryption of the hard drives for staff laptops and other machines will be considered with the installation of Windows 7.

Online Services

Some online resources may require student detail to be uploaded into an external website. You need to make sure that the organisation providing the service has necessary security procedures and protection in place.

If you require advice, please see the ICT Team before you make a purchase.

Home PC Security Passwords

If you are using a personal home computer to access personal data then you must use password protection. This helps protect any data stored on the computer (e.g. files saved to the computer, email attachments opened) in the event the computer is lost or stolen. This is deemed as good practice for any home PC.

Penetration Testing

The ICT Team shall organise yearly testing to review data protection procedures. Penetration testing simulates the threat of a malicious attack on our computer network. This will identify any existing vulnerabilities. It will be undertaken by an external provider..

Leon Oxenham
Head of ICT 13.09.2011