Data Protection Policy

Leytonstone School

Signed by Chair of Governors: Kate Lord

Date Ratified by Governors: 18/3/15

Date to be Reviewed by Governors: 28/3/17

DATA PROTECTION

The following is Leytonstone School policy on the Use of Personal Data under the Data Protection Act. Leytonstone School is registered with Information Commissioners Office ICO reference number Z5474223. This is renewed yearly 1st July

POLICY USE OF PERSONAL DATA

Leytonstone School endorses fully the statements and the intent of the Data Protection Act 2000. The Data Protection principles contained in the Act are designed to protect the rights of the individual.

DEFINITIONS

Personal Data means data (manual or computer) which relates to a living individual who can be identified from those data (or from data and other information that is in the possession of, or is likely to come into the possession of the data controller).

Data means information that is being processed automatically or is recorded with the intention that it should be processed automatically. Any manual data that forms part of an 'accessible record' is also included in this definition.

Data Controller means a person who determines the way in which any personal data is to be processed.

NOTIFICATION

Any time that data about an individual person is held manually or on a computer, the purposes must be:

- Notified to the Council's Data Protection Officer
- In accordance with the principles of the Act
- Available to be seen by the person named

PROCESSING

Every person must be sure that data held on manual and computer files about individuals is:

- Processed fairly and lawfully
- Accurate and up-to-date
- Used only for defined purposes
- Kept private
- Kept only for as long as it is useful
- Relevant and not excessive
- All parents/carers and staff are asked to sign a data collection sheet confirming the school is required to share some data with the LBWF and DFE.

DISCLOSURE

There should be a policy for confirming the identity of any person requesting information about themselves. This will be specified to the information in question. For personal information requested by third parties the policy for disclosure will again be system and service specific. Formulating and implementing these policies will be the responsibility of the service manager.

Any time that information from a file is given to a third party, the person giving the information must be sure that the third party is properly identified, and authorised and registered to receive the data.

Before disclosing personal information to a third party it is essential to check why the data is required and to whom that party intends to disclose it. Only disclose personal information when you have checked that the disclosure is compatible with your disclosure policy and the Data Protection principles.

If you are aware of any data held or disclosures made that break the data protection principles you must report this to your supervisor or manager, or to the Data Protection Officer, in order that the breach may be addressed.

POLICY ON AUTHORITY TO ACCESS

The Computer Misuse Act 1990 [amended by Police and Justice Act 2006] identifies the legal framework for definition of and prosecution for unauthorised use or misuse of computer systems. Whilst the Act is particularly intended to deal with unauthorised accesses from outside the organisation ('hackers'), it deals equally with unauthorised accessed from inside.

It is essential that you, as a computer user, understand the extent of your authority to use and access systems. Computers used for more than one purpose and those connected to the corporate data network provide the potential for access to a large number of systems and to a great deal of personal, private and confidential data.

This policy makes it your responsibility to guard and protect your ability to access systems that you have authority to use. Passwords must not be written down or passed on (other than to your line manager). Computers must not be left logged in when unattended, particularly those in open access offices and classrooms.

Any employee finding that they have access to systems and data which they are not authorised to use must report this to their supervisor or manager, or to the ICT Department, in order that the access may be removed, Any employee with authority to access data that is no longer necessary to their work must ask for the access to be removed. Any employee who knows that unauthorised access is taking place must report this to their supervisor or manager, or to the ICT Department, in order that the access may be removed.

Penalties under the Act fall into two main categories:

- Unauthorised access to computer material –

  A person guilty of an offence under this section shall be liable—

(a) On summary conviction to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
(b) On conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

- Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.-

  A person guilty of an offence under this section shall be liable—
  (a) On summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
  (b) On conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

DATA SECURITY PROCEDURE

- Make sure your password is changed regularly.
- Do not leave your computer accessible when unattended users use Ctrl Alt & Delete to lock screen.
- Make sure you are authorised to use the systems you need.
- Remember to copy data regularly for security and back-up
- Store important files in your ‘home folder’ on your network file server if you have one – these are backed up.
-