Woolwich Polytechnic School

PolyMAT

Data Protection Policy

Reviewed September 2017

Approved by Governors: November 2017

Revision due September 2018

Introduction

Registration reference: **Z3492263**

This policy applies to all members of PolyMAT. For the purposes of this policy, the term "staff" means all members of staff within the Trust, including permanent, fixed term and temporary staff. It also refers to governors, any third party representatives, agency workers, volunteers and trainees with-in the Trust.

All contractors and agents acting for or on behalf of the Trust will be made aware of this policy.

This policy applies to all personal and sensitive personal data (see definitions below) processed on computers and stored in manual (paper-based) files. It aims to protect and promote the rights of individuals and the Trust.

(i) **Personal Data:** Any information which relates to a living individual who can be identified from the information. It also extends to any information which may identify the individual. Examples of personal data include:

- A person's name and address (postal and email);
- Date of birth;
- Statement of fact;
- Any expression or opinion communicated about an individual;
- Minutes of meetings and reports;
- Emails, file notes, handwritten notes and sticky notes;
- CCTV footage if an individual can be identified by the footage;
- Employment and student applications;
- Spreadsheets and/or databases containing lists of people set up by code or student/staff number;
- Employment or education history.

- (ii) **Sensitive Personal Data:** Any information relating to an individual's:
- Ethnicity;
- Gender;
- Religious or other beliefs;
- Political opinions;
- Membership of a trade union;
- Sexual orientation;
- Medical history;

· Offences committed or alleged to have been committed by that individual.

The Trust recognises and understands that the consequences of failure to comply with the requirements of the Data Protection Act 1998 may result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension/withdrawal of the right to process personal data by the Information Commissioner's Office (ICO);
- Loss of confidence in the integrity of the Trust's systems and procedures;
- Irreparable damage to the Trust's reputation.

Definitions

The Data Protection Act 1998 is designed to protect individuals' and personal data, which is held and processed by others on their behalf. The Act defines the individual as the 'data subject' and their personal information as 'data'. These are further defined as:

- Data subject: Any living individual who is the subject of personal data, whether in a personal or business capacity;
- Data: Any personal information which relates to a living individual who can be identified. This includes any expression of opinion about the individual;
- Data is information stored electronically i.e. on computer, including word-processing documents, emails, computer records, CCTV images, microfilmed documents, backedup files or databases, faxes and information recorded on telephone logging systems;
- Manual records which are structured, accessible and form part of a 'relevant filing system' (filed by subject, reference, dividers or content), where individuals can be identified and personal data easily accessed without the need to trawl through a file.

Anonymised data are individual data records from which the personally identifiable fields have been removed. Data subjects' identities are not discernable from such data.

Aggregated data are data which are processed to produce a generalised result and from which individuals cannot be identified. This might include data brought together to give a broad understanding of, for instance, whole School academic grade data presented publicly.

The DPA's eight data protection principles

The Data Protection Act (DPA) 1998 sets legislative requirements for organisations processing personal data (referred to under the Act as 'data controllers'). The Trust will be open and transparent when processing and using private and confidential information by ensuring we follow the eight data protection principles for good data handling, which are as follows:

Principles of the Act

1. Data shall be processed fairly and lawfully.

2. Data shall be obtained/processed for specific lawful purposes.

3. Data must be adequate, relevant and not excessive.

4. Data must be accurate and kept up-to-date.

5. Data shall not be kept for longer than necessary.

6. Data shall be processed in accordance with rights of data subjects.

7. Data must be kept secure.

8. Data shall not be transferred outside the EEA unless there is adequate protection.

Data Management

Data Gathering

Whenever new information is collected about individuals, the Trust will ensure that individuals are made aware:

- that the information is being collected;
- of the purpose that the information is being collected for;
- of any other purposes that it may be used for;
- with whom the information will or may be shared;

These requirements encompass the use of CCTV. The Trust will ensure that cameras are in the right place, that they do not breach anyone's privacy and that notices are displayed. The Trust will only obtain relevant and necessary personal data for lawful purposes and will only process the data in ways which are compatible with the purposes for which they were gathered.

Data Storage

Personal data will be stored in a secure, safe manner. The following measures will be taken to help ensure this:

- Electronic data will be protected through secure passwords, encryption software and firewall systems operated by the Trust;
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers;
- Manual personal data will be stored securely where it is not accessible to anyone who does not have a legitimate reason to view or process the data;

- Particular attention will be paid to the need for security of sensitive personal data for example, health and medical records will be kept in a locked cupboard;
- Personal data will not be left in a position where it is visible to unauthorised observers;
- The physical security of the school buildings and storage systems will be reviewed regularly;
- Staff will be trained on this policy and related data protection procedures.

What an employer should tell an employee

An employee has a right to be told:

- what records are kept and how they're used
- the confidentiality of the records
- how these records can help with their training and development at work

If an employee asks to find out what data is kept on them, the employer will have 40 days to provide a copy of the information.

An employer shouldn't keep data any longer than is necessary and they must follow the rules on data protection.

Procedures

All employees will through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.
- Understand fully the purposes for which the school uses the personal information.
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the school to meet its needs or legal requirements.
- Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.
- Not send any personal information outside of the United Kingdom without the authority of the Head teachers.
- Ensure the information is correctly input into the school's systems.

The school will:

- Ensure that there is always one person with overall responsibility for Data protection (data controller).
- Provide awareness for all staff members who handle personal information.
- Provide clear lines of report and supervision for compliance with Data Protection.

- Carry out regular checks to monitor and assess new processing of personal data and to ensure the school's notification to the Information Commissioner is updated to take account of any changes in processing of personal data.

Charges

As defined within the Data Protection Act 1998, this school charges a fee of £10 for processing any request for personal data, known as a Subject Access Request. Cheques should be made to **"Woolwich Polytechnic School".**

The only exception to this charge is for cases involving children or young people who are being or have been looked after.

Proof of identity is also required and it is requested that at least two copies of identifying documents of the data subject, such as a driving licence, passport, recent utility bill etc. are enclosed with the request. If a third party is making the request, a signed letter of consent from the data subject should also be enclosed.

Some Subject Access Requests may require further information before the process can commence. This information will be requested as soon as possible after the original request has been made. If this information is not received within 6 months, the request will be closed and a new request will have to be made.

A Subject Access Request must be made in writing.