Data Protection Policy

MAYFLOWER COMMUNITY ACADEMY PLYMOUTH POLICIES

VERSION CONTROL SHEET

POLICY NAME: Data Protection Policy

Policy Prepared by: Nigel Gooding

Document date	Filename	Meeting submitted	Summary of changes required
July 2013		July PSG	New policy
January 2016			Policy Review

General Statement
The Academy Trust Board of the academy has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions. The Headteacher of this Academy intends to comply fully with the requirements and principles of the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries
Information about the academy's Data Protection Policy is available from the Headteacher. General information about the Data Protection Act can be obtained from the Information Commissioner, Tel: 0303 123 1113, website http://www.ico.org.uk

Definitions
"processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
"data subject" means an individual who is the subject of personal data or the person to whom the information relates.
"personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, internet or media.
"parent" has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

Fair Obtaining and Processing
Mayflower Community Academy undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

Registered Purposes
The Data Protection Registration entries for the Academy are available for inspection, by appointment, at the Headteacher's office. Explanation of any codes and categories entered is available from the Headteacher, who is the person nominated to deal with data protection issues in the Academy. Registered purposes covering the data held at the academy are listed on the Academy's registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data Integrity
The Academy undertakes to ensure data integrity by the following methods:

Data Accuracy
Data held will be as accurate and up to date as reasonably possible. If a data subject informs the Academy of a change of circumstances, their records will be updated as soon as is practicable. Where a data subject challenges the accuracy of their data, the Academy will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Academy Trust Board for their judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance
Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the Academy will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. (Details should be added on how and when records are checked for irrelevant data and who has the say on what must be deleted).

Length of Time
Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Headteacher to ensure that obsolete data are properly erased.

Subject Access
The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the Academy's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the data will be provided to the requesting parent.

Processing Subject Data Requests
Requests for access must be made in writing. Pupils, parents or staff may ask for a Data Subject Access form, available from the Academy Office. Completed forms should be submitted to the Headteacher. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of the requester (if different), the type of data

required (e.g. student record, personnel record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided. Note: in the case of any written request from a parent regarding their own child's academic record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

Authorised Disclosures

The Academy will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the Academy's authorised officer may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the academy to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the academy.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, e.g. to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the academy. Officers and IT personnel writing on behalf of the LA are IT liaison officers/data processing officers and are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the academy by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the academy who needs to know the information in order to do their work. The academy will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything that suggests they are, or have been, either the subject of or at risk of child abuse. A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the academy, provided that the purpose of that information has been registered,

An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the Academy's registered purposes.

Data and Computer Security

Mayflower Community Academy undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

Physical Security
Appropriate building security measures are in place, such as alarms and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the academy are required to sign in and out, to wear identification badges whilst in the academy and are, where appropriate, accompanied.

Logical Security
Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up regularly.

Procedural Security
In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal. Overall security policy for data is determined by the Governing Body and is monitored and reviewed regularly. Any queries or concerns about security of data in the academy should in the first instance be referred to the Headteacher (the person responsible). Individual members of staff can be personally liable by law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of the Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

Policy reviewed and adopted by the Academy Council – July 2013
Date of next review – ~~September 2014~~January 2017