Mayesbrook Park School

Alternative Provision for young people in Barking and Dagenham

DATA PROTECTION POLICY

November 2016

DATA PROTECTION POLICY

Version:	**2**
Approving Committee:	**Finance and Personnel**
Date Ratified:	**03/11/2016**
Reference Number	**1**
Name/Department of Originator/Author:	**Suresh Singh/ Caroline Kenny**
Name/Title of Responsible Committee/Individual: Finance and staffing	**Annie Blackmore Head of MPS Chair: Robert Turner**
Date Issued:	**November 2016**
Review Date:	**November 2017**
Target Audience:	**Staff/Parents/Governors/LA**

Version	Date	Control Reason
Version 2	03/11/2016	Update DFE advice

MPS Data Protection Policy 2016 - 2017

Overview

The Data protection Act:

- Regulates the processing of personal data relating to living individuals (data subjects)
- Imposes legal obligations upon data controllers (the school)
- Provides Data Subjects with legal rights relating to how their personal data is processed
- Introduces sanctions for breaches of the Act

Summary

- Information about the school's Data Protection Policy is available from the front office and can also be viewed on the school website.
- The school will give all data subjects 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.
- All data subjects have a right of access to their own personal data. Such requests must be made in writing, using the Data Subject Access form (available from the front office).
- The school will endeavour to ensure the accuracy of the data held.
- The data held will be accurate, relevant and not excessive.
- Staff must ensure that when staff or pupil information (electronic or otherwise) is taken off site that it is kept secure at all times.
- The school will ensure that all personal data held (be it in hard copy or electronic form) is secure.

The Governing Body of the school 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 Head Teacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1984 and 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.

Definition of ‘Personal Data’: Can a living individual be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the school?

The Eight Principles of the Data Protection Act

Principle 1: Personal data must be processed fairly and lawfully and only under certain circumstances. Principle 2: Personal data must be processed for purposes that are compatible with the original purpose of obtaining it.
Principle 3: Data collected and stored must be adequate, relevant and not excessive.
Principle 4: Data must be accurate and up-to-date.
Principle 5: Data must not be kept for longer than necessary.
Principle 6: Data must be processed in line with Data Subject’s legal rights. Principle 7: Data must be kept safe and secure.
Principle 8: Data must not transferred outside the European Economic Area unless the destination country can adequately protect personal data.

Enquiries
Information about the school's Data Protection Policy is available from the front office and can also be viewed on the school website. General information about the Data Protection Act can be obtained from the Information Commissioner's Office (ICO), (website www.ico.org.uk)

Fair Obtaining and Processing
MPS 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. "Data subject" means an individual who is the subject of personal data or the person to whom the information relates. "Parent" has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

Registered Purposes
The Data Protection registration entries for the School are available for inspection, by appointment, at the School Office. Explanation of any codes and categories entered is available from **Caroline Kenny** who is nominated to deal with data protection issues in the school.

Registered purposes covering the data held at the school are listed on the school'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 accuracy
Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the School 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 Governing Body for their judgement. 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 School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. Annually, parents are asked to update the contact information held by the school for accuracy. Also, admin staff checks any information held by the school against parental consent forms for trips.

Length of Time
Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of admin staff and Teachers to ensure that obsolete data is properly erased, using the 'Retention Guidelines for Schools' documentation issued by the LA.

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 school'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 copy will be sent in a sealed envelope to the requesting parent.

Processing Subject Access Requests
Requests for access must be made in writing. Pupils, parents or staff may ask for a Data Subject Access form (Appendix 1), available from the School Office. Completed forms should be submitted to the main office or head teacher's PA if appropriate. 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 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 date on which sufficient information has been provided.

In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

Authorised Disclosures
The School will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the School'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 school 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 school. • Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example 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 school. Personnel working on behalf of the LA 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 school 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 school who need to know the information in order to do their work. The school 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 that they are, or have been, either the subject of, or at risk of, child abuse.
- The school must ensure that any 'third party' contractors, other than the LA, handling data sign an undertaking to abide by the principles of the Data Protection Act.

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 school, 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 School's registered purposes. It is worth noting that comments on Facebook / Twitter etc. which disclose privileged personal data would fall into the category of 'illegal disclosure'.

Data and Computer Security
MPS undertakes to ensure security of personal data in the following ways:

1) Physical Security
Appropriate building security measures are in place, such as alarms, window bars, deadlocks 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 school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

2) Electronic Security
Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files. Computer files are backed up (i.e. security copies are taken) regularly. Clearly, many documents in school contain sensitive and personal data. (For example, IEPs, SEN statements and annual reviews, exclusion letters) Great care must be taken when taking a copy of these documents off-site. Memory sticks containing personal and sensitive data should be encrypted and documents password-protected. Technical assistance with this is available from the IT Services Department in school.

3) Procedural Security
. In order to be given authorised access to the computer, staff will have to undergo checks and will agree a confidentiality agreement (this is done when staff log on to the computer).
. Staff should not leave their computers logged on to personal data (for example, MIS) when they are not present in the room.
. All staff are trained in their Data Protection obligations and their knowledge updated as necessary.
. Computer printouts as well as source documents containing personal data are shredded before disposal. (For example, personal data recorded for school trips)
. Students' school record files should not be taken off-site except under exceptional circumstances
. Staff should avoid leaving documents containing personal and sensitive data in places easily seen by others; for example, left on desks at the end of the day.

Overall, security policy for data is determined by the Head Teacher/Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Individual members of staff can be personally liable in 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 this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from the school.

Data Subject Access form; Appendix 1

Access to Personal Data Request (Data Protection Act 1998, Section7)
Enquirer's Surname…….....
Enquirer's Forenames……..
Enquirer's Address ……....
…….....
Enquirer's Postcode ……..... Telephone
Number …….....

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")? YES / NO
If NO,
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about? YES / NO If YES,
Name of child or children about whose personal data records you are enquiring
……..
Description of Concern / Area of Concern
…….
Description of Information or Topic(s) Requested
…….
Additional information
…….

Please despatch Reply to: (if different from enquirer's details as stated on this form)
Name.....
Address.....
Postcode.....

Data Subject Declaration
I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information). Signature of "Data Subject" (or Subject's Parent)

……

Name of "Data Subject" (or Subject's Parent)
(PRINTED)…….

Date …….