

# **Dulwich Hamlet Educational Trust**



## **Data Protection Policy**

# Dulwich Hamlet Educational Trust

## Data Protection Policy

### 1. General Statement

The Board of Trustees (DHET) is responsible for ensuring that Dulwich Hamlet Junior School and The Belham Primary School complies with the Data Protection Act 1998 (DPA).

Each school will comply fully with the requirements and principles of the DPA. All staff involved with the collection, processing and disclosure of personal data will be made aware of their duties and responsibilities within these guidelines.

### 2. Enquiries

Information about the Trust's Data Protection Policy will be available on both school websites on the page relating to common policies of DHET. Information about the DPA can be obtained from the Information Commissioner (Information Line 01625 545 745, website: [www.ico.gov.uk](http://www.ico.gov.uk)).

### 3. Fair Obtaining and Processing

DHET 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 are 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.

**“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.

#### **4. Registered Purposes**

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.

#### **5. Data Integrity**

The school undertakes to ensure data integrity by the following methods:

#### **6. Data Accuracy**

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the schools of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the schools 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.

#### **7. 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

#### **8. 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 person compiling the records to ensure that obsolete data are properly erased.

#### **9. 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 it 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.

#### **10. Processing Subject Access Requests**

Requests for access must be made in writing which can be by email.

Pupils, parents or staff may ask for a Data Subject Access form (Copy at Annex A) available from the School Office or available to download from the School's web site. Completed forms should be submitted to the Headteacher/Head of School. Provided that there is sufficient information to process the request, an entry will be made in the "online" 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. Pupil 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.

Note: 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.

## II. 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 demeanor 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. Officers and IT personnel working for the Trust are IT liaison/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 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 which suggests that they are, or have been, either the subject of or at risk of child abuse.

- ◆ DHET follows the procedures set out by the Local Safeguarding Children Board and takes account of guidance issued by the DCSF to keep children safe. For the purposes of this document, multi-agency professionals working together under Local Safeguarding Children Board procedures are included in the description of staff in school. Information is shared under locally agreed protocols.

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.

## **12. Data and Computer Security**

DHET undertakes to ensure security of personal data by the following general methods:

### **13. 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 use of computers or in the computer room. Disks, printouts and all other confidential information are locked away securely when not in use. Visitors to the schools are required to sign in and out, to wear identification badges whilst in the schools and are, where appropriate, accompanied.

### **14. 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 (i.e. security copies are taken) regularly.

Full details of the schools’ back up/contingency arrangements are contained within the MAT Business Continuity Plan.

### **15. Procedural Security**

In order to be given authorised access to the computer, staff will have to undergo checks and will sign the school’s Acceptable Use Policy, agreeing to keep any staff or pupil information available via digital technologies confidential, except where required by law to disclose information to an appropriate authority. 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 DHET and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. Security information (including passwords) is kept in a safe location at all times.

Any queries or concerns about security of data in the school should in the first instance be referred to the Headteacher/Head of School.

Individual members of staff can be personally liable in law under the terms of the DPA. 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 either of the school offices

**DATA PROTECTION ACT 1998    SUBJECT ACCESS REQUEST (SAR) FORM**

Enquirer's name.....

Enquirer's address .....  
.....  
.....  
.....

Enquirer's Email .....

Contact Telephone Number .....

Are you the 'Data Subject' (The person about whose personal data records you are enquiring?)

YES/ NO

If NO,

Do you have parental responsibility for a child who is the Data Subject    ?    YES/NO

If YES,

Name of child or children about whose personal data records you are enquiring:

.....  
.....  
.....  
.....

Information Requested

Please email reply in the first instance to the email addresses as shown on each of the school's websites under "contact us".

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, including supplying any identification as may be required by the School.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above authorised by me to receive such information).

Signature of Data Subject (or Subject's Parent) .....

Name of Data Subject (or Subject's Parent) .....

Dated .....