



EMMANUEL SCHOOLS FOUNDATION

Data Protection Policy



Last Reviewed : March 2017
Approved : March 2017
Next Review : June 2019

Contents

1. General Statement	3
2. Enquiries	3
3. Fair Obtaining and Processing	3
4. Data Integrity.....	3
5. Subject Access	4
6. Processing Subject Access Requests	4
7. Authorised Disclosures.....	5
8. Data and Computer Security.....	5
9. References	6

DATA PROTECTION POLICY

1. General Statement

Emmanuel Schools Foundation (“ESF”) has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

Employees of ESF are intent 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.

2. Enquiries

Information about ESF’s Data Protection Policy is available from the Company Secretary. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www.dataprotection.gov.uk).

3. Fair Obtaining and Processing

ESF 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 subject’s 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. Data Integrity

ESF undertakes to ensure data integrity by the following methods:

4.1 Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs ESF or the school of a change of circumstances their computer record will be updated as soon as is practicable. A print-out 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, ESF or 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 governors for their

judgment. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

4.2 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, ESF will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

4.3 Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered.

5. Subject Access

The Data Protection Act extends 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 student, ESF's policy is that:

- Requests from students will be processed as any subject access request as outlined below, and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request.
- Requests from students who do not appear to understand the nature of the request will be referred to their parents.
- 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.

6. Processing Subject Access Requests

Requests for access must be made in writing.

Students, parents or staff may ask for a data subject access form, available from the school's office. Completed forms should be submitted to the Principal. 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 a date on which sufficient information has been provided. A charge of £10.00 will be made for all requested information.

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.

7. Authorised Disclosures

ESF will, in general, only disclose data about individuals with their consent. However there are circumstances under which ESF's or the school's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for ESF to perform its statutory duties and obligations.
- Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of any ESF 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 ESF.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within ESF by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within ESF who **needs to know** the information in order to do their work. ESF will not disclose anything on a student's record 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.

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 ESF, 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 who has no right to it, or one which falls outside ESF's registered purposes.

8. Data and Computer Security

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

8.1 Physical Security

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

8.2 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 **and must never**

be shared with anyone. Staff must ensure the computer is locked when they leave their workstation.
Computer files are backed up (i.e. security copies are taken) regularly.

8.3 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.

The overall security policy for data is determined by the Principal and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. ESF's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in ESF should be referred to the Principal.

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 Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

9. References

This Policy should be read in conjunction with the:-

Data Protection and Code of Practice for Information Sharing and Exchange with other Public Agencies and the Security Policy; and

The Freedom of Information Policy and Procedure.

ACCESS TO PERSONAL DATA REQUEST

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname Forenames

Enquirer's Address

.....

.....

Enquirer's Postcode Telephone Number

School the Data Request applies.....

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 (In your own words)

Additional information

DATA SUBJECT DECLARATION

I request that ESF 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 ESF.

I agree that the reply period will commence when I have supplied sufficient information to enable ESF 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)

.....

Dated