

Trust Policy

Data Protection Policy



Contained within this document:

- Information about how the schools within the trust, and the trust itself manages, processes and protects data
- Provides an individual with access to all personal data held on them

This policy should be read in conjunction with:

0010101001010101000101010101010
10100101011011010110101010110101
0101001000111010101010100001010
11101001001101001010101010010
0101010101010101010100010001010
0101010100101001010101001010100
01010101010101001010101010100
01010101010100110100101010010
0101010100101010101010010101001
01010101010101010101010101010
10101011110101010101010101010
10101101010110101010101010101
10101000101010101010101010101

Data Protection Policy

Policy/Procedure management log

Document name	Data Protection Policy
Author	Eversheds
Date approved	Pending
Date issued	June 2017
Date of review	May 2018
Reviewer	Director of Data (Data Controller for the Trust)

Document history

Version	Date authored	Author	Date approved	Date issued
V1	1 st Sept 2016	Eversheds	1 st Sept 2016	1 st Sept 2016
V1.1	1 st May 2017	C Holmes		
V1.2	22 May 2017	A Ingram	June 2017	June 2017

Data Protection Policy

Introduction

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with within our trust properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings. Schools within our trust collect a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the schools. In addition, the schools within our trust may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Eight Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

1. Data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Responsibilities

The schools within our trust, and the trust itself, must:

- Manage and process personal data properly
- Protect the individual's right to privacy
- Provide an individual with access to all personal data held on them.

The trust has a legal responsibility to comply with the Act. The trust, as a corporate body, is named as the Data Controller under the Act. Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

The trust/school is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link:

<https://ico.org.uk/ESDWebPages/DoSearch>

Every member of staff that holds personal information has to comply with the Act when managing that information.

The trust is committed to maintaining the eight principles at all times. This means that the schools within the trust will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice.
- check the quality and accuracy of the information held
- apply the records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act (**see appendix 1**)
- train all staff so that they are aware of their responsibilities and of the trust/school's relevant policies and procedures

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Please follow this link to the ICO's website (<https://ico.org.uk>) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

Appendix 1- Right to access own personal data

Subject Access

The Data Protection Acts extend to all data subjects the 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 trust'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

(i) Requests for access must be made to the trust/school in writing.

(ii) Pupils, parents or staff may ask for a Data Subject Access form (see Appendix 2). Completed forms should be submitted to the office of the Head of School/Headteacher.

Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log, 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.

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 days in accordance with the current Education (Pupil Information) Regulations 2005.

Authorised Disclosures

The Trust/School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Trust'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 trust/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 trust/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 Trust/School.

Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the trust/school by administrative staff and teachers and will only be made available where the person requesting the information is a professional legitimately working within the trust/school who **need to know** the information in order to do their work. The trust/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 where suggests that they are, or have been, either the subject of or at risk of child abuse.

"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 trust/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 trust/school's registered purposes.

Appendix 2 – Access to Personal Data Request Form

Name:		
Address:		
Telephone number:		
Email address:		
Are you the person who is the subject of the records you are enquiring about?	Yes/No	
If No,		
Do you have parental responsibility for the child who is the "Data Subject"	Yes/No	
Name of student or students about whose personal data records you are enquiring:-		
1)		
2)		
3)		
Description of Concern/Area of Concern		
Description of Information or Topic(s) Requested		
Additional Information		
Data Subject Declaration		
<p><i>I request that the trust/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 trust/school.</i></p> <p><i>I agree that the reply period will commence when I have supplied sufficient information to enable the trust/school to perform the search.</i></p> <p><i>I consent to the reply being disclosed and sent to me at my stated address.</i></p>		
Signature of "Data Subject" (or Subject's Parent)		
.....		
Name of "Data Subject" (or Subject's Parent)		
PRINTED).....		
Dated		