# Data Protection

# Policy

**History of document: To be reviewed annually and re-approved every two years, or sooner if deemed necessary.**

| Issue number | Author | Date written | Approved by Board | Comments |
|---|---|---|---|---|
| 1 | C Burt | 10 Oct. 2017 | 17/10/2017 | |
| | | | | |
| | | | | |

**Introduction:**

Trust schools collect and use certain types of personal information about employees, students, parents/carers and other individuals who come into contact with them, in order to provide education and associated functions.
In addition, Trust schools may be required by law to collect and use certain types of information to comply with the statutory obligations of Local (Education) Authorities (LAs), government agencies and other bodies.

This Policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act 1998 (The Act) and other related legislation. 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.

The Trust is the Data Controller under The Act and will endeavour to ensure that all personal information is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. The Trust, on behalf of its schools, has a duty to be registered as Data Controller with the Information Commissioner's Office (ICO), detailing the information held and its use. These details are then available on the ICO's website.

Trust Schools also have a duty to issue a Fair Processing Notice to students/parents/carers which summarises the information held on students, why it is held and the other parties to whom it may be passed on.

All staff involved with the collection, processing and disclosure of personal information will be aware of their duties and responsibilities within these guidelines.

General information about the Data Protection Act can be obtained from the office of the Information Commissioner (**website http://www.ico.gov.uk**).

**Definitions:**

The Act regulates the use of “personal data”. To understand what “personal data” means, we need to first look at how the Act defines the word “data”.
“data” means information which:
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

“personal data” means data which relate to a living individual who can be identified
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be “personal data”.

“sensitive personal data” means personal data consisting of information as to:
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

“Processing” refers to any action involving personal information, including obtaining, viewing, recording, copying, amending, adding, deleting, extracting, storing, disclosing, destroying or otherwise using 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.

**Data Protection Principles:**

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes 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 or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this 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 or territory outside the European Economic Area 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.

The Trust is committed to maintaining these principles at all times. This means we will:

- tell you what purposes we will use information for when we collect it.
- if information will be shared we will tell you why, with whom and under what circumstances.
- check the quality and accuracy of the information we hold.
- apply our 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 to safeguard personal information whether that is held in paper files or on our computer system.
- share personal information with others only when it is necessary and legally appropriate to do so and set out clear procedures for responding to requests for access to personal information, known as subject access in the Data Protection Act.
- train our staff so that they are aware of our policies and procedures.
- update this policy, as necessary, to reflect best practice or amendments made to the Data Protection Act 1998.

**Processing:**

Personal data (including sensitive personal data, where appropriate) is processed by the Trust strictly in accordance with the Data Protection Act in order to:

- support pupils' teaching and learning.
- monitor and report on their progress.
- publish examination results.
- provide appropriate pastoral care.
- assess how well the Trust as a whole is doing.
- communicate with former pupils.
- monitor pupils' official email communications and internet use etc. for the purpose of ensuring compliance with the Trust's ICT Acceptable Use Policy.
- where appropriate, promote the Trust to prospective pupils.
- other reasonable purposes relating to the operation of the Trust. Unless you have specifically requested otherwise the School may also use your contact details to send you promotional and marketing information by post, email, SMS and other electronic means about the School and about carefully selected third parties.

**Data Integrity:**

The Trust will aim to ensure data held about students, parents/carers and staff is as accurate and up to date as reasonably possible. The Trust requests all data subjects to inform us of any changes to information held, and offers frequent reminders to data subjects to do this. Additionally, data record sheets are reviewed annually and parents/carers are asked to update and check the data collection sheets. The Trust will only gather and process data that it considers necessary to carry out its educational purposes effectively. The Trust will ensure that data is not held any longer than is necessary and, once no longer needed, it is properly destroyed/erased.

**Rights of Access to Information**

There are two distinct rights of access to information held by schools about pupils:

1. Pupils attending any type of school have a right of access under the Data Protection Act 1998 to their own information. This is known as the right of subject access. When a child cannot act for themselves or the child gives permission, parents will be able to access this information on their behalf.

2. The right of those entitled to have access to curricular and educational records as defined within The School Information (England) Regulations 2008. However, this only applies to Maintained Schools.

These procedures therefore relate solely to subject access requests made under the Data Protection Act 1998.

**Actioning a Subject Access Request**:

1. Requests for information must be made in writing; which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the student. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

*This list is not exhaustive.*

3. Any individual has the right of access to information held about them. However with students, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request.

4. The Headteacher should discuss the request with the student and take their views into account when making a decision. A student with competency to understand can refuse to consent to the request for their records. Where the student is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the student.

5. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10.
- Free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

6. The response time for subject access requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However the 40 days will not commence until after receipt of fees or clarification of information sought.

7. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

8. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

9. Any information which may cause serious harm to the physical or mental health or emotional condition of the student, or another, should not be disclosed, nor should information that would reveal that the student is at risk of abuse, or information relating to court proceedings.

10. If there are concerns over the disclosure of information then additional advice should be sought.

11. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

12. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

13. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

**Authorised Disclosures**

The Trust will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Trust 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 the Trust to perform its statutory duties and obligations.
- Student data disclosed to parents/carers 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 agreeing not to disclose the data outside the school. Such persons are contractually bound not to disclose personal data.

Only authorised staff are allowed to make external disclosures of personal data. Data used within the Trust by administrative staff, teachers and other officers will only be made available where the person requesting the information is a professional legitimately working within the Trust who needs to know the information in order to do their work.

The Trust will not disclose anything on students' 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.

**Data Security:**

The Trust 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 key fob entry, alarms, window bars, deadlocks. Only authorised persons are allowed in the server room which is locked when not in use. 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.
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 network, staff will have to undergo checks and will sign an Acceptable Use 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. Staff are aware they should 'lock' or close down computers when not in use. Deliberate data protection breaches are treated very seriously. Staff are aware that such breaches are a disciplinary matter and could lead to dismissal.

**Complaints:**

Complaints regarding these procedures, or any other data protection matter, should be made in line with the Trust's Complaints Policy. Complaints that involve consideration of personal data or sensitive personal data may be referred to the Information Commissioner.