Data Protection Policy: Practical Guidance for Staff

SEARCH
Education Trust
Strong, Sustainable, Successful Schools

DATE POLICY APPROVED:	**October 2022 (TBC)**	**APPROVED BY:**	**F&R Committee**
REVIEW DUE:	**October 2023**	**TYPE OF POLICY:**	**Statutory**
AUTHOR:	**Molla Abdullah**	**OWNER:**	**CFO**

Contents

1 Introduction

1.1 This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that the Trust uses and stores information about identifiable people (Personal Data). Data protection legislation also gives people various rights regarding their data - such as the right to access the Personal Data that the Trust holds on them.

1.2 We will collect, store and process Personal Data about our staff, pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in the Trust and will ensure that the Trust operates successfully.

1.3 You are obliged to comply with this policy when using Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

1.4 The Data Protection Officer / Finance Director is responsible for helping you to comply with the Trust's obligations. All queries concerning data protection matters should be raised with the Data Protection Officer / Finance Director.

2 Application

2.1 This policy is aimed at all staff working in the Trust (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, trustees, contractors, agency staff, work experience / placement students and volunteers.

2.2 Employees only: This policy does not form part of your contract of employment and may be amended by the Trust at any time.

3 Scope of this policy

3.1 Data protection concerns information about individuals.

3.2 Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available.

3.3 Information as simple as someone's name and address is their Personal Data.

3.4 In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

3.5 Examples of places where Personal Data might be found are:

3.5.1 on a computer database;

3.5.2 in a file, such as a pupil report;

3.5.3 a register or contract of employment;

3.5.4 pupils' exercise books, coursework and mark books;

3.5.5 health records; and

3.5.6 email correspondence.

3.6 Examples of documents where Personal Data might be found are:

3.6.1 a report about a child protection incident;

3.6.2 a record about disciplinary action taken against a member of staff;

3.6.3 photographs of pupils;

3.6.4 a tape recording of a job interview;

3.6.5 contact details and other personal data held about pupils, parents and staff and their families;

3.6.6 contact details of a member of the public who is enquiring about placing their child at the Trust;

3.6.7 financial records of a parent;

3.6.8 information on a pupil's performance; and

3.6.9 an opinion about a parent or colleague in an email.

3.7 These are just examples - there may be many other things that you use and create that would be considered Personal Data.

3.8 **Categories of Critical Trust Personal Data:** The following categories are referred to as **Critical Trust Personal Data** in this policy and in the Information Security policy. You must be particularly careful when dealing with Critical Trust Personal Data which falls into any of the categories below:

3.8.1 information concerning child protection matters;

3.8.2 information about serious or confidential medical conditions and information about special educational needs;

3.8.3 information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offense and whether or not the allegation has been proved);

3.8.4 financial information (for example about parents and staff);

3.8.5 information about an individual's racial or ethnic origin;

3.8.6 political opinions;

3.8.7 religious beliefs or other beliefs of a similar nature;

3.8.8 trade union membership;

3.8.9 physical or mental health or condition;

3.8.10 sex life or sexual orientation;

3.8.11 genetic information;

3.8.12 information relating to actual or alleged criminal activity; and

3.8.13 biometric information (e.g. fingerprints used for controlling access to a building).

3.9 If you have any questions about your use of these categories of Critical Trust Personal Data please speak to the Data Protection Officer/ Finance Director.

4 Your obligations

4.1 Personal Data must be processed fairly, lawfully and transparently

4.1.1 What does this mean in practice?

(a) "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

(b) People must be told what data is collected about them, what it is used for, and who it might be shared with. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

This information is provided in a document known as a privacy notice. Copies of the Trust's privacy notices can be obtained from the Data Protection Officer/Finance Director or accessed on the Trust's website. You must familiarize yourself with the Trust's Pupil, Parent and Staff Privacy notices.

(c) If you are processing Personal Data in a way which you think an individual might think is unfair please speak to the Data Protection Officer/ Finance Director.

(d) You must only process Personal Data for the following purposes:

(i) ensuring that the Trust provides a safe and secure environment;

(ii) providing pastoral care;

(iii) providing education and learning for our pupils;

(iv) providing additional activities for pupils and parents (for example activity clubs);

(v) protecting and promoting the Trust's interests and objectives (for example fundraising);

(vi) safeguarding and promoting the welfare of our pupils; and

(vii) to fulfill the Trust's contractual and other legal obligations.

(e) If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must speak to the Data Protection Officer / Finance Director. This is to make sure that the Trust can lawfully use the Personal Data.

(f) We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you must speak to the Data Protection Officer / Finance Director] if you think that you may need to seek consent.

(g) If you are not an employee of the Trust (for example, if you are a volunteer), then you must be extra careful to make sure that you are only using personal data in a way that has been expressly authorized by the Trust.

4.2 **You must only process Personal Data for specified, explicit and legitimate purposes.**

4.2.1 What does this mean in practice?

(a) For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you must not use those photographs for another purpose (e.g. in the Trust's prospectus). Please see the Trust's Code of Conduct and the Guidance for Staff on the use of Photographs and Videos of Pupils by the Trust for further information relating to the use of photographs and videos.

4.3 **Personal Data held must be adequate and relevant for the purpose**

4.3.1 What does this mean in practice?

(a) This means not making decisions based on incomplete data. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil.

4.4 **You must not hold excessive or unnecessary Personal Data**

4.4.1 What does this mean in practice?

(a) Personal Data must not be processed in a way that is excessive or unnecessary. For example, you must only collect information about a pupil's siblings if that Personal Data has some relevance, such as allowing the Trust to determine if a sibling fee discount is applicable.

4.5 **The Personal Data that you hold must be accurate**

4.5.1 What does this mean in practice?

(a) You must ensure that Personal Data is complete and kept up to date. For example, if a parent notifies you that their contact details have changed, you must ensure that the Trust's information management system has been updated.

4.6 **You must not keep Personal Data longer than necessary**

4.6.1 What does this mean in practice?

(a) The Trust has a policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data.

(b) Please speak to the Data Protection Officer / Finance Director for guidance on the retention periods and secure deletion.

4.7 **You must keep Personal Data secure**

4.7.1 You must comply with the following Trust policies and guidance relating to the handling of Personal Data:

(a) information security policy;

(b) Guidance for Staff on the use of Photographs and Videos of Pupils by the Trust;

(c) IT acceptable use policy for staff; and

(d) information and records retention policy.

4.8 **You must not transfer Personal Data outside the UK without adequate protection**

4.8.1 What does this mean in practice?

(a) If you need to transfer personal data outside the UK please contact Data Protection Officer / Finance Director . For example, if you are arranging a school trip to a country outside the UK.

4.9 **Accountability**

4.9.1 The Trust is responsible for and must be able to demonstrate compliance with the data protection principles. You are responsible for understanding your particular responsibilities under this policy to help ensure we meet our accountability requirements.

5 Sharing Personal Data outside the Trust - dos and don'ts

5.1 Please review the following dos and don'ts:

5.1.1 **DO** share Personal Data on a need to know basis only - think about why it is necessary to share data outside of the Trust - if in doubt - always ask your Data Protection Officer.

5.1.2 **DO** encrypt emails which contain Critical Trust Personal Data described in paragraph 3.8 above. For example, encryption must be used when sending details of a safeguarding incident to social services. Further information on encryption can be found in the Information Security policy.

5.1.3 **DO** make sure that you have permission from your manager or the Data Protection Officer / Finance Director to share Personal Data on the Trust website.

5.1.4 **DO** share Personal Data in accordance with the Trust's Safeguarding Policy. If you have any questions or concerns relating to safeguarding, you must contact the Designated Safeguarding Lead.

5.1.5 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organizations. You must seek advice from the Data Protection Officer/ Finance Director where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent but using a different email address).

5.1.6 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise or if you have any concerns about the message. You must report all concerns about phishing to [the IT department] immediately.

5.1.7 **DO NOT** disclose Personal Data to the Police without permission from the Data Protection Officer/ Finance Director (unless it is an emergency).

5.1.8 **DO NOT** disclose Personal Data to contractors without permission from the Data Protection Officer/ Finance Director. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event.

6 Accessing or sharing Personal Data within the Trust

6.1 This section applies when Personal Data is accessed or shared within the Trust.

6.2 Personal Data must only be accessed or shared within the Trust on a "need to know" basis.

6.3 Examples which are **likely** to comply with data protection legislation:

6.3.1 a teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil);

6.3.2 sharing Personal Data in accordance with the Trust's Safeguarding Policy;

6.3.3 informing an exam invigilator that a particular pupil suffers from panic attacks; and

6.3.4 disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).

6.4 Examples which are **unlikely** to comply with data protection legislation:

6.4.1 the Head teacher being given access to all records kept by nurses working within the Trust (seniority does not necessarily mean a right of access);

6.4.2 a member of staff looking at a colleague's HR records without good reason. For example, if they are being nosey or suspect their colleague earns more than they do. In fact accessing records without good reason can be a criminal offense (see paragraph 9.2 below).

6.4.3 informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); and

6.4.4 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

6.5 You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please contact [• name of contact] as a matter of urgency.

7 Individuals' rights in their Personal Data

7.1 People have various rights in their information.

7.2 You must be able to recognise when someone is exercising their rights so that you can refer the matter to the Data Protection Officer/ Finance Director. These rights can be exercised either in writing (e.g. in an email) or orally.

(a) Please let the Data Protection Officer/ Finance Director know if anyone (either for themselves or on behalf of another person, such as their child):

(i) wants to know what information the Trust holds about them or their child;

(ii) asks to withdraw any consent that they have given to use their information or information about their child;

(iii) wants the Trust to delete any information;

(iv) asks the Trust to correct or change information (unless this is a routine updating of information such as contact details);

(v) asks for personal data to be transferred to them or to another organization;

(vi) wants the Trust to stop processing their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the Trust newsletter or alumni events information; or

(vii) objects to how the Trust is processing their information or wants the Trust to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

(b) Please note, a person may be committing a criminal offense if they alter, block, erase, destroy or conceal information to prevent it from being disclosed (for example, to prevent its disclosure if a subject access request for that information has been received). Therefore if you are asked to provide information or documents to a colleague at the Trust who is preparing a response to a request for information then you must make sure that you provide everything.

8 Requests for Personal Data (Subject Access Requests)

8.1 One of the most commonly exercised rights mentioned in section 7 above is the right to make a subject access request. Under this right people are entitled to request a copy of the Personal Data which the Trust holds about them (or in some cases their child) and to certain supplemental information.

8.2 Subject access requests do not have to be labeled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid subject access request. You must always immediately let the Data Protection Officer/ Finance Director know when you receive any such requests.

8.3 Receiving a subject access request is a serious matter for the Trust and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorized to do so.

8.4 When a subject access request is made, the Trust must disclose all of that person's Personal Data to them which falls within the scope of his/her request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a subject access request.

However, this must not deter you from recording and passing on information where this is appropriate to fulfill your professional duties, particularly in relation to safeguarding matters.

9 Breach of this policy

9.1 A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

9.2 A member of staff who deliberately or recklessly obtains or discloses Personal Data held by the Trust (or procures its disclosure to another person) without proper authority is also guilty of a criminal offense. In some cases, it can also be an offense to re-identify information which has been de-identified. Please speak to the Data Protection Officer/ Finance Director before doing this.