# Data Protection Policy for Staff

## Document provenance

| This policy was approved by Trustees as follows – | |
|---|---|
| Committee: Audit and Risk Committee | Date: June 2020<br><br>Next review date: June 2022 |
| Executive Leadership Team (ELT) Owner: Director of Governance and Strategy | |
| *Unless there are legislative or regulatory changes in the interim, this policy will be reviewed every two years. Should no substantive changes be required at that point, the policy will move to the next review cycle.* | |

**Summary of changes at last review:**

- Added to item 3.5 reference to cloud based software.
- Added to item 3.6 reference to recording on CPOMS.
- Inclusion of footnote reference to enable readers quick access to the relevant DPA 2018 legislation.
- Throughout the Policy, Critical Personal Data has been changed to read Special Category Data, as per the current ICO guidelines.

**Related documents:**

- IT Acceptable Use Policy[1]
- Information Security Policy[2]
- Information and Records Retention Policy[3]
- Guidance for staff for the use of photographs and videos of pupils by the Trust.[4]

[1] https://insight.e-act.org.uk/policies/ict-usage-policy

[2] https://insight.e-act.org.uk/policies/information-security-policy

[3] https://insight.e-act.org.uk/policies/information-and-records-retention-policy

[4] https://insight.e-act.org.uk/system/files/Guidance%20for%20staff%20on%20the%20use%20of%20photos%20and%20videos%20of%20pupils_0.pdf

# Data Protection Policy for Staff

## 1. Introduction

1.1. This policy is about your obligations under the data protection legislation[5]. Data protection is about regulating the way that the Trust uses and stores information about identifiable people (Personal Data). It also gives people various rights regarding their data, such as the right to access the Personal Data that the Trust holds about them.

1.2. E-ACT (the **Trust**) is ultimately responsible for how you handle personal information.

1.3. The Trust will collect, store and process Personal Data about our staff, pupils, parents, suppliers and other third parties. The Trust recognises that the correct and lawful treatment of this data will maintain confidence in the Trust, will ensure that the Trust operates successfully and is fully complaint with the law.

1.4. You are obliged to comply with this policy when processing Personal Data on behalf of the Trust. Any breach of this policy may result in disciplinary action.

1.5. The Trust Data Protection Officer (DPO) is responsible for helping you to comply with the Trust's obligations. All queries concerning data protection matters must be raised with the Data Protection Officer.

## 2. Application

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

2.2. This policy does not form part of a contract of employment. This Policy may be amended by the Trust at any time.

## 3. What information falls within the 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:

- in computer databases or cloud-based software;
- in a file, such as a pupil report;
- in the staff room;
- a register or contract of employment;

[5] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- pupils' exercise books, coursework and mark books;
- health records;
- email correspondence.

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

- a report about a child protection incident, CPOMS;
- a record about disciplinary action taken against a member of staff;
- photographs of pupils;
- on a staff room notice board with details of a pupil's individual needs (e.g. dietary, allergies);
- contact details and other personal information held about pupils, parents and staff and their families;
- contact details of a member of the public who is enquiring about placing their child at the Academy;
- financial records of a parent;
- information on a pupil's performance; and
- 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 Special Category Data**

3.8.1 The following categories are referred to as **Special Category Data** in this policy and in the Information Security Policy. You must be particularly careful when dealing with **Special Category Data** which falls into any of the categories below:

- information concerning child protection matters;
- information about serious or confidential medical conditions and information about special educational needs;
- information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
- financial information (for example about parents and staff);
- information about an individual's racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- genetic information;
- information relating to actual or alleged criminal activity; and
- biometric information (e.g. a pupil's fingerprints following a criminal investigation.

3.9. If you have any questions about your processing of these categories of **Special Category Data** please contact the Data Protection Officer (DPO).

## 4. Your obligations

### 4.1. Personal Data must be processed fairly, lawfully and transparently.

4.1.1. What does this mean in practice?

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

4.1.1.2. People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. 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 (ICO - the Data Protection Regulator).

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

4.1.1.3. If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Data Protection Officer.

4.1.1.4. You must only process Personal Data for the following purposes:

- ensuring that the Trust provides a safe and secure environment;
- providing pastoral care;
- providing education and learning for our pupils;
- providing additional activities for pupils and parents (for example activity clubs);
- protecting and promoting the Trust's interests and objectives (for example fundraising);
- safeguarding and promoting the welfare of our pupils; and
- to fulfil the Trust's contractual and other legal obligations.

4.1.1.5. 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. This is to make sure that the Trust has a lawful reason for using the Personal Data.

4.1.1.6. We may sometimes rely on the consent of the individual to use their Personal Data. The Trust will obtain consent for photographs which require additional consent, or if biometric information needs to be obtained. For more information about when to seek consent, please refer to the '*Guidance for staff on the use of photos and videos of pupils*.' The consent must meet certain requirements and therefore you should speak to the Data Protection Officer if you think that you may need to obtain consent.

**4.2. You must only process Personal Data for limited purposes and in an appropriate way.**

4.2.1. What does this mean in practice?

4.2.1.1. For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you should 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?

4.3.1.1. 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?

4.4.1.1. Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about a pupil's medical history if that Personal Data has some relevance, such as allowing the Trust to care for the pupil and meet their medical needs.

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

4.5.1. What does this mean in practice?

4.5.1.1. 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 update the Trust's information management system.

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

4.6.1. What does this this mean in practice?

4.6.1.1. 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.

4.6.1.2. Please refer to the **Information and Records Retention Policy** and/or speak to the Data Protection Officer 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:

- Information Security Policy;
- IT Acceptable Use Policy;
- Information and Records Retention Policy;
- Guidance for Staff on the use of Photographs and Videos of Pupils by the Trust

**4.8. You must not transfer Personal Data outside the UK without adequate protection[6]**

[6] Under current legislation, the UK is part of the EEA Transfers on the Basis of Adequacy rule which means there are no restrictions on data transfers to EEA countries (Article 45) and the additional countries which are considered by the EU as having adequate data protection laws. However, it is not known if the UK will continue to be included in the Transfers on the Basis of Adequacy rule once the Brexit transition has concluded. If the UK's membership is

4.8.1. What does this mean in practice?

4.8.1.1. If you need to transfer personal data outside the UK please contact the Data Protection Officer. For example, if you are arranging an academy trip to a country outside UK.

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

### 5.1. Please review and uphold the following do's and don'ts:

5.1.1. **DO** share Personal Data on a need to know basis - think about why it is necessary to share data outside of the Trust - if in doubt - always ask your immediate line manager in the first instance.

5.1.2. **DO** encrypt emails which contain Special Category Data described in paragraph 3.8 above. For example, encryption should be used when sending details of a safeguarding incident to social services. For more information on how to use encryption, please see section 8 of the Information Security Policy.

5.1.3. **DO** make sure that you have permission from your manager, the Trust-wide Communications Team or Data Protection Officer to share Personal Data on the Trust website. Please refer to the 'Guidance for staff on the use of photos and videos of pupils' and seek additional advice as needed for any instances which are deemed borderline or requiring consent.

5.1.4. **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You must seek advice from the Data Protection Officer 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).

5.1.5. **DO** be exceptionally aware of 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. Do not 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 do not recognise. Report all concerns about phishing to your academy IT department or your regional/national IT colleagues.

5.1.6. **DO NOT** disclose Personal Data to the Police without permission from the Regional Operations Director (ROD), unless it is an emergency

5.1.7. **DO NOT** disclose Personal Data to contractors without permission from the Regional Operations Director (ROD) or Data Protection Officer (DPO). This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event.

## 6. Sharing Personal Data within the Trust

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

6.2. Personal Data must only be shared within the Trust on a "need to know" basis and in line with

repealed, transfers will be made based on appropriate safeguards (Article 46) or derogations (Article 49). The General Data Protection Regulation

our polices for sharing data.

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

- 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);
- informing an exam invigilator that a particular pupil suffers from panic attacks;
- sharing contact details of parents / carers for specific pupils with a member of staff leading an Academy trip, in case of emergency; an
- 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 of sharing which are **unlikely** to comply with data protection legislation:

- informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil);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 must have received training on safeguarding issues. If you are unsure whether to share information in relation to a safeguarding matter, please contact your Designated Safeguarding Lead (DSL) in your academy or your Regional System Leader for Safeguarding (RSL).

## 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.

(a) Please let the Regional Operations Director (ROD) or Data Protection Officer (DPO) 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 electronic information which they provided to the Trust to be transferred back to them or to another organisation;

(vi) wants the Trust to stop using 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 using 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.

## 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 (SAR). 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 labelled 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 national Governance Team know when you receive any such requests by emailing governance.team@E-ACT.org.uk.

**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 authorised 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 should not deter you from recording and passing on information where this is appropriate to fulfil 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 discloses Personal Data held by the Trust without proper authority is also guilty of a criminal offence.

## 10. Compliance

10.1 All employees are asked to annually declare that they have read, understood, and will comply with this Data Protection Policy as part of their annual staff declaration.