Data Protection Policy: Practical Guidance for colleagues

Document information.

Document title	Data Protection Policy - Practical Guidance for Colleagues		
Owner	HR Operations Team HROT		
Version	1.0	Status Pending	Final
Last updated	24.04.2024	Last updated by	Lea Millinchip
Approved on	15.05.2024	Effective from	01.06.2024
Review Date	01.06.2026		
Purpose	This policy applies to all colleagues across the organisation		
This policy links to:	Information Security Policy Guidance for Colleagues on the Use of Photographs and Videos CCTV Policy IT Acceptable Use Policy for Colleagues Information and Records Retention Policy		

If you would like this information in another language or format, please contact the Trust Data Protection Officer or Director of Operations.

lea.millinchip@stchads.uk or zoe.Heath@stchads.uk

1 Introduction

1.1 This policy is about your obligations under data protection law. Data protection law regulates the way that the Trust uses and stores information about identifiable people (Personal Data). Data protection law 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 We will collect, store and process Personal Data about our colleagues, 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 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.

2 Application

2.1 This policy applies to at all colleagues working in the Trust (whether directly or indirectly), whether paid or unpaid, whatever their position, role, or responsibilities. This includes colleagues, trustees, local governors, contractors, agency colleagues, peripatetic colleagues, work experience, students, and volunteers.

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

3 Personal Data

3.1 Personal Data is information that relates to a living person who can be identified either from that information alone, or from the information when combined with other information.

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

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

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

3.4.1 a computer database.

3.4.2 a file, such as a pupil report.

3.4.3 a register or contract of employment.

3.4.4 pupils' exercise books, coursework, and mark books.

3.4.5 health records; and

3.4.6 email correspondence.

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

3.5.1 a report about a child protection or safeguarding incident.

3.5.2 a record about disciplinary action taken against a colleague.

3.5.3 photographs and videos of pupils.

3.5.4 a tape recording of a job interview.

3.5.5 contact details and other Personal Data held about pupils, parents and colleagues and their families.

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

3.5.7 financial records of a parent.

3.5.8 information on a pupil's performance; and

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

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

3.7 Data protection law requires us to be extra careful when handling Personal Data about children.

3.8 Critical Trust Personal Data**:** The following types of information are referred to as **Critical Trust Personal Data** in this policy and in the Information Security Policy. You must be particularly careful when handling Critical Trust Personal Data.

3.9 Critical Trust Personal Data is information about:

3.9.1 child protection or safeguarding matters.

3.9.2 someone's special educational needs.

3.9.3 a serious allegation made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved).

3.9.4 financial information (for example, a parent's bank details or a colleague's salary).

3.9.5 an individual's racial or ethnic origin.

3.9.6 an individual's political opinion.

3.9.7 someone's religious or philosophical beliefs.

3.9.8 trade union membership.

3.9.9 someone's physical or mental health. This includes information about the provision of healthcare which reveals information about their health status.

3.9.10 sex life or sexual orientation.

3.9.11 genetic information.

3.9.12 actual or alleged criminal activity or the absence of criminal convictions (e.g., Disclosure and Barring Service checks); and

3.9.13 biometric information which is used for the purpose of uniquely identifying an individual (e.g., fingerprints used for controlling access to a building).

3.10 If you have any questions about your using of these categories of Critical Trust Personal Data, please speak to the Data Protection Officer.

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 doing virtually anything with Personal Data, including using, sharing (internally or externally), 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 data, 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 provided in a document known as a privacy notice. Copies of the Trust's privacy notices can be obtained from the Data Protection Officer or accessed on the Trust/academy's website. You must familiarise yourself with the Trust's privacy notices.

(c) If you are processing Personal Data in a way someone might think is unfair, or in a way that they might not expect, please speak to the Data Protection Officer.

(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 including safeguarding, child protection and promoting the welfare of our pupils.

(iii) making sure that the Trust is a good place to work and in relation to HR and colleague matters.

(iv) providing education and learning for our pupils.

(v) providing additional activities for pupils and parents (for example, activity clubs)

(vi) protecting and promoting the Trust's interests and objectives (for example, fundraising and commercial ventures); and

(vii) to fulfil 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. This is to make sure that the Trust can lawfully use the Personal Data.

(f) We may sometimes rely on the consent of an individual to use their Personal Data. This consent must meet certain requirements and therefore you must speak to the Data Protection Officer 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 authorised 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) You must not use Personal Data for a reason that is incompatible with the original reason for collecting it. For example, if pupils are told that they will be photographed to enable colleagues to recognise them when writing references, you must not use those photos for another purpose (e.g., in the Trust's prospectus).

(b) Please see the Trust's Code of Conduct and the Guidance for Colleagues on the Use of Photographs and Videos by the Trust for further information relating to the use of photos 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:

(i) when writing reports, you must make sure that you are using all of the relevant information about the pupil; and

(ii) when making a note of a disciplinary incident you must include all relevant details.

4.4 **You must not collect or use excessive or unnecessary Personal Data**

4.4.1 What does this mean in practice?

(a) You must limit the Personal Data that you collect or use to the minimum needed to meet your objectives.

(b) For example, you must only collect information about a pupil's siblings if that Personal Data has some relevance.

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.

(b) For example, if a parent notifies you that their contact details have changed, you must ensure that the Academy Trust's management system has been updated.

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

4.6.1 What does this 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.

(b) You must be particularly careful when you are deleting or disposing of data.

(c) Please 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 Personal Data must be kept safe at all times. This includes paper and electronic information. This is a critical area of compliance; most data protection fines and compensation claims happen because of security breaches.

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

(a) Information Security Policy.

(b) Guidance for Colleagues on the Use of Photographs and Videos by the Trust policy.

(c) CCTV Policy.

(d) IT Acceptable Use Policy for Colleagues; and

(e) 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 DPO@stchads.uk For example, if you are arranging a school trip to outside the UK.

4.9 **Accountability**

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

4.9.2 Before using Personal Data in a new way, or in a way that might present a risk to individuals if something went wrong (e.g., before implementing new software to store medical information) please speak to the Data Protection Officer.

5 Sharing Personal Data outside of 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 the 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 or child protection 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 Exec-/Principal or the Data Protection Officer to share Personal Data on the Trust website or social media accounts.

5.1.4 **DO** share Personal Data in accordance with the Trust's Safeguarding and Child Protection Policy. If you have any questions or concerns relating to safeguarding or child protection, you must contact Sarah Davies or Lea Millinchip.

5.1.5 **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).

5.1.6 **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 your IT provider and the Trust Compliance Officer immediately.

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

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

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 law:

6.3.1 a teacher discussing a pupil's academic progress with colleagues (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 and Child Protection 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 law:

6.4.1 the Principal 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 colleague 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 offence (see paragraph 9.2 below);

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

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

6.5 You must make sure that you file and save Personal Data in the correct place. For example, emails which may be needed in the future should not be stored in your inbox but instead stored somewhere centrally.

6.6 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, safeguarding and child protection issues. If you have not received this training, please contact your manager 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. These rights can be exercised either in writing (e.g., in an email) or orally.

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

(i) wants a copy of the Personal Data that the Trust holds about them or their child. This is commonly known as a Subject Access Request SAR.

(ii) asks to withdraw any consent that they have given to use their Personal Data or Personal Data about their child.

(iii) wants the Trust to delete any Personal Data.

(iv) asks the Trust to correct or change Personal Data (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 organisation.

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

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

(viii) wants the Trust to stop using a computer programme to make an important decision about them.

7.2.2 Please note, a person may be committing a criminal offence if they alter, block, erase, destroy or conceal information to prevent it from being disclosed (for example, to prevent its disclosure under a Subject Access Request). Therefore, if you are asked to provide information or documents to a colleague who is preparing a response to a subject access request 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 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 Data Protection Officer 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. Colleagues 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 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 fulfil your professional duties, particularly in relation to safeguarding and child protection 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 colleague who deliberately or recklessly obtains or discloses Personal Data held by the Trust (or procures its disclosure to another person) without proper authority might be committing a criminal offence.

9.3 In some cases, it can also be an offence to re-identify information which has been de-identified. For example, if names have been removed from information to protect the privacy of the individuals and you were to re-insert the names. Please speak to the Data Protection Officer before doing this.