Data Protection Policy

Version:	**v5**		
Ratified by:	**Board of Trustees**	**Date:**	**21st May 2025**
Next Review date:	**May 2027**		

This policy applies to all members of Sussex Learning Trust (the "Trust"). For the purposes of this policy, the term "Staff" means all members of staff within the Trust including permanent, fixed term, and temporary staff. It also refers to Members, Trustees, Governors, any third party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the Trust.

All contractors and agents acting for or on behalf of the Trust will be made aware of this policy. This policy applies to all personal and sensitive personal data processed on computers and stored in manual (paper based) files. It aims to protect and promote the rights of individuals and the Trust.

Definitions

Personal Data: Any information which relates to a living individual who can be identified from the information.

Sensitive Personal Data: Any information relating to an individual's ethnicity, gender, religious beliefs, political opinions, trade union membership, sexual orientation, medical history, or criminal history.

Data Subject: Any living individual who is the subject of personal data.

Data: Includes all electronically stored and manually filed personal data.

Data Controller (DC): A person or organisation who determines the purposes and means of processing personal data. **The Trust is the Data Controller under the UK GDPR and the Data Protection Act 2018.**

Data Protection Officer (DPO): Appointed by the Trust to monitor compliance and provide advice.

Data Processor (DP): Any person or organisation that processes data on behalf of the Data Controller.

Data Champions (DC): Designated staff responsible for key data assets and supporting the DPO.

Processing: Includes obtaining, recording, storing, altering, retrieving, disclosing, or deleting data.

Private Network / Public Cloud: Storage models defined to ensure safe, secure processing of personal data. Only the Trust-authorised public cloud (Google Workspace) is permitted for non-sensitive data.

Legal Framework

This policy complies with the UK General Data Protection Regulation (UK GDPR) retained in UK law under the European Union (Withdrawal) Act 2018, and the Data Protection Act 2018.

Lawful Bases for Processing Personal Data

The Trust will process personal data only when there is a lawful basis under Article 6 of the UK GDPR, including:

- Consent
- Performance of a contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

For special category data, the Trust will identify a further lawful condition under Article 9 of the UK GDPR

Data Subject Rights

Under the UK GDPR, data subjects have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

The GDPR six data protection principles

Under Article 5(1) of both the EU GDPR and the UK GDPR, personal data must be:

1. Lawfulness, fairness, and transparency
2. Purpose limitation – collected for specified, explicit and legitimate purposes
3. Data minimisation – adequate, relevant and limited to what is necessary
4. Accuracy – kept accurate and up to date
5. Storage limitation – kept for no longer than necessary
6. Integrity and confidentiality – processed in a secure manner

Appendix 1: Sussex Learning Trust: Data Protection Governance Structure

The Trust is the Data Controller for the purposes of GDPR and therefore the Trust Directors will have overall responsibility for compliance with the GDPR.

Each academy will approach compliance with GDPR within their own organisation and should be encouraged to appoint their own DPO.

The Director of Digital Services & E-Learning currently acts as DPO to overview the compliance model and ensure that other trust academies are ready in terms of compliance.

The DPO is responsible for:

- Keeping the Heads of Trust schools and Trust Data Controller up to date with changes in how the Academies processes data.
- Obtaining consent for disclosure of personal data, including routine consent from parents/carers and pupils for using photographs for general academy purposes.
- Ensuring the use of CCTV is compliant with this policy.
- Ensuring data protection statements are included on forms that are used to collect personal data.
- Acting as a central point of advice for local staff on data protection matters.
- Coordinating requests for personal data.
- Arranging appropriate data protection training for staff.
- Keeping up to date with the latest data protection legislation and guidance.
- Ensuring staff are following the Trust DP policy for compliance with this policy.
- Ensuring new software or new services for the Academy are compliant with this policy

Staff Engaged in Data Processing, together with the DPO, are responsible for:

- All information which is held will be relevant and accurate for the purpose for which it is required.
- The information will not be kept for longer than is necessary and will be kept secure at all times.
- Not attempting to gain access to information that is not necessary to hold, know or process.

- Staff who manage and process personal or sensitive personal information will ensure that it is kept secure and where necessary confidential.
- Sensitive personal information will only be processed fairly and lawfully and in line with the provisions set out in the GDPR 2016 and only processed in accordance with instructions set out by the respective Data Protection Officer.
- The Trust will ensure that all personal or sensitive personal information is anonymised as part of any evaluation of assets and liability assessments except as required by law.
- The Trust will ensure that Data Processing Agreements are applied to all contracts and management agreements where the Trust is the Data Controller contracting out services and processing of personal data to third parties (data processors).
- The Trust will ensure this agreement clearly outlines the roles and responsibilities of both the data controller and the data processor.
- Breach of the Policy, Non compliance of this policy and data protection legislation by a member of staff is considered a disciplinary matter which, depending on the circumstances, could lead to dismissal.

Data Management Data Gathering

Whenever an academy collects new information about individuals the Trust will ensure individuals are made aware:

- that the information is being collected,
- of the purpose that the information is being collected for,
- of any other purposes that it may be used for,
- with whom the information will or may be shared,

and how to contact the Data Controller. These include the use of CCTV ensuring that cameras are in the right place and they don't intrude on anyone's privacy . Notices are displayed in suitable places to notify data subjects. The Trust will only obtain relevant and necessary personal data for lawful purposes and will only process the data in ways which are compatible with the purpose for which it was gathered. Data Protection statements will be included in the prospectus and on forms that are used to collect personal data.

Data Storage

Personal data will be stored in a secure and safe manner. The following measures are taken to help ensure this:

- Electronic data will be protected through secure passwords, encryption software and firewall systems operated by the Trust.
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers.
- Manual personal data will be stored securely where it is not accessible to anyone that does not have a legitimate reason to view or process the data.
- Particular attention will be paid to the need for security of sensitive personal data, for example health and medical records will be kept in a locked cupboard.
- Personal data will not be left out visible on desks.
- The physical security of academy buildings and storage systems will be regularly reviewed.
- Staff will be trained on this policy and related data protection procedures.

The only Trust authorised Public Cloud, for storage of data, online document collaboration and webmail, is Google Workspace. No other Public Cloud or cloud email system, such as Dropbox or Hotmail, should be used for storage of personal and sensitive data. Sensitive Personal Data should only be accessible through the Private Cloud and data should be saved internally (not on the Public Cloud), with the exception of teaching marking and tracking documents after explicit approval from the Data Protection Officer. There is sometimes a slight risk that aggregated data might still allow an individual to be identified, for example by the results producing a very small group of results, from which other data may be used in identifying an individual, even though personal data has been removed. To safeguard data subjects and to manage the Trust's risk, aggregated data, which comprise no more than five individual records, should not be used or disclosed and stored in the Public Cloud without Data Protection Officer (DPO) approval, unless such aggregated data can in no way be matched to identify individual data subjects.

Data Checking

Systems will be put in place to ensure the personal data that the Trust holds is up to date and accurate (For example the Trust/academies will ensure that parents/carers are asked at least once a year to confirm their contact details). Any inaccuracies discovered or reported will be rectified as soon as possible.

Data Disclosure

Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive their data, or organisations that have a legal right to receive the data without consent being given. When requests to disclose personal data are received by telephone, the academy will ensure that the caller is entitled to receive the data and verify their identity. In some circumstances the academy may call the caller back to check the identity of the caller. Personal data will not be included on the website, in newsletters or to other media without consent of the individual (or his/her parents/carers where appropriate). Routine consent may be requested from parents/carers to avoid the need for frequent, similar requests for consent being made by academies and on the understanding that consent can be revoked or revised on written request. Personal data will only be disclosed to the police if they are able to supply a form which notifies of a specific, legitimate need to have access to specific personal data.

Destroying Data

Out of date information will be securely discarded if no longer relevant. Personal data will only be kept for as long as reasonably needed, for legal or business purposes.

Data Subjects Rights

The Trust acknowledges individuals (data subjects) rights under the Data Protection Act to access any personal data held on our systems and in our files upon their request, or to delete and/or correct this information if it is proven to be inaccurate, excessive or out of date. The Trust recognises that individuals have the right to prevent data processing where it is causing them damage or distress, or to opt out of automated decision making and stop direct marketing. Consent can be revoked or revised at any time on written request.

Data Subject Access Requests (SAR)

Any person whose personal data is held by the Trust is entitled, under the DPA, to ask for access to this information. The request must be in writing. The right is to view or be given a copy of the personal data, rather than to the whole document which contains personal data. There are some exceptions to the rights of access to information in certain records held by an academy (e.g. in relation to examination scripts, legal advice). When a request is received by a member of staff, this should be passed to the academy's Data Protection Officer (DPO) without delay. The request must be dealt with promptly; a response must be provided as soon as possible and no later than within 28 calendar days from the date the request was received.

The Trust may make a charge of £10 for responding to a request for personal data under the DPA if the request is deemed to be **'manifestly unfounded or excessive'** but would not charge otherwise. The Trust will need to confirm the requester's identity. Parents/carers can make data subject access requests on their child's behalf, if their children are deemed too young to look after their own affairs. If a request is made by a parent for personal data relating to their child and the child is aged 12 years or older, written consent will need to be sought from the child before the data is disclosed to the parent. A record will be kept of all data subject access requests made that require formal consideration. The trust has a right to withhold information if the information requested is deemed to **'adversely affect the rights and freedoms of others'**.

Biometric Data

As of May 2025, Chichester Free School uses a biometric recognition system (fingerprint scanning) to allow students to pay for food at break and lunchtime. This system complies with the requirements of the Protection of Freedoms Act 2012, and written consent is obtained from at least one parent or carer before any biometric data is collected or processed.

All other academies within Sussex Learning Trust do not currently collect or process biometric data.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash as an alternative.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV

Where we use CCTV in various locations around our school sites to ensure it remains safe. We will adhere to the ICO's HYPERLINK "https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf"code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to facilities managers of the specific site.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our schools.

We will obtain written consent from parents/carers, or pupils for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

All schools add and adapt to reflect your school's uses of photographs and videos for communication, marketing and promotional materials:

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Personal data breaches

The school will make all reasonable endeavors to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person

- The theft of a school laptop containing non-encrypted personal data about pupils
- Emails not using BCC or copied to an incorrect address

Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary – if any changes are made to the legislation that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the local governing bodies and Board of Trustees.

Records of Processing Activities (RoPA)

The Trust will maintain a Record of Processing Activities (RoPA) in accordance with Article 30 of the UK GDPR, updated by the DPO.

International Data Transfers

Where personal data is transferred outside the UK, appropriate safeguards such as standard contractual clauses or adequacy decisions will be implemented.

Automated Decision-Making and Profiling

The Trust does not currently use automated decision-making or profiling. If introduced, the Trust will inform affected individuals and ensure appropriate legal safeguards are in place.

Linked Documents

Other documents that have relevance to this document:

Policies:

E-Safety Policy (EPOL)

CCTV Policy

Freedom of Information Act Policy (FOIA)

Procedures:

Digital Security Procedures

Acceptable User Agreement (AUA)

Freedom of Information Act Policy (FOIA)

Privacy Statements for Students, parents/carers and staff

Data Retention Policy

Appendix 2: Personal data breach procedure

This procedure is based on HYPERLINK "https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/"guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - **Unauthorised reversal of pseudonymisation (for example, key-coding)**
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Where the ICO must be notified, the

DPO will do this via the HYPERLINK "https://ico.org.uk/for-organisations/report-a-breach/"'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Document Revision Log

Date	Version	Comment	Ratified by	Reviewer
July 2021	3	No material changes	Trustees (21/7/21)	DPT/MS
January 2023	4	Additions and minor revision re data champions (list of key data assets and where the Trust would expect to have data champions). Note re biometric data - no current use or collection	Trustees (22/2/23)	D Thomas & A Drury
May 2025	5	Updated references to UK GDPR and Data Protection Legislation 2018 Have produced a condensed version which could be considered a governance level policy and removed the embedded guidance. Definitions have been made more concise and focuses on core legal and governance policy elements Added additional sections related to Lawful Bases for Processing Data, Data Subject Rights, Data Protection Governance Structure (Procedural Guidance) has been amended to become a Appendix 1 Data Breach Procedure has been amended to Appendix 2	Board of Trustees 21/5/25	J Hickey