Data Protection/GDPR Policy

Approved by:	Finance and Resource Committee	**Date:** October 2021
Last reviewed on:	October 2021	
Next review due by:	October 2023	
Monitoring & Review	Board of Trustees; Local Governing Bodies; Data Protection Officer	
Links	Retention Schedule; CCTV Procedures; Privacy Information Notices; Enrolment Forms; Consent Forms; Procurement Policy	
Staff responsible	Trust Lead for Data, Insight and Analysis; Director of Estates and Facilities; Principals	

Contents

1. Aims

Summit Learning Trust is committed to upholding the key principles of data protection law.

This policy sets out how we will do that, by:

- applying data protection law to the day-to-day work of Summit Learning Trust and its Academies;
- clarifying roles and responsibilities with respect to our data protection duties;
- outlining the ways we will process different kinds of personal data, including the various security arrangements we will put in place; and
- explaining how we will uphold the rights people have under data protection law.

2. About this policy

This policy applies to all personal data used by Summit Learning Trust and its Academies to carry out its functions. It does not form part of any contract of employment and it may be amended at any time, subject to approval from the Board of Trustees.

Any breach of this policy – by any staff member, apprentice, volunteer, governor or Trustee, of Summit Learning Trust and/or any of its Academies – may result in disciplinary or other action.

This policy meets the requirements of the GDPR and Data Protection Act 2018. It is based upon guidance from the Information Commissioner's Office (ICO).

It also meets the requirements of the Protection of Freedoms Act 2012.

This policy links with the following documents, which can be accessed through SharePoint:

- Retention Schedule;
- CCTV Procedures;
- Privacy Information Notices;
- Enrolment Forms; and
- Consent Forms.

3. Definitions

In this policy, the functions of the Trust and/or its Academies are the provision of education as well as any pastoral, business, administrative, community or similar activities associated with that provision. References to our functions are references to these activities.

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. Examples include: contact details; identification numbers; assessment data; location data; financial data; online identifiers; and so on.

Special category data	Types of personal data that are more sensitive, and so need more protection. It includes information about an individual's: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetics; • biometrics, where used for identification purposes; • physical or mental health; and • sex life or sexual orientation.
Criminal offence data	Any personal data relating to the commission of, or proceedings for, any criminal offence committed or alleged to have been committed by a person.
Processing	Anything done to personal data, including: collecting; recording; organising; structuring; storing; adapting; altering; retrieving; using; disseminating; erasing; or destroying. Processing can be manual or automated.
Data protection law	All laws applicable to England and Wales that relate to the processing of personal data – as may be amended, re-enacted, replaced or superseded from time to time – including: • the General Data Protection Regulation ((EU) 2016/679) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426), or else any laws which incorporate those provisions in the event of the United Kingdom's withdrawal from the European Union; and • the Data Protection Act 2018.
Data subject	The identified, or identifiable, living individual whose personal data is processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data. Summit Learning Trust is the data controller for all personal data, including that which is processed by its Academies, used to carry out its functions.
Data processor	A person or organisation, other than an employee of the Trust or any of its Academies, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Roles and responsibilities

4.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations to which it is subject.

4.2 Local Governing Bodies

Local Governing Bodies may scrutinise their Academy's compliance with this policy and with data protection law more broadly.

4.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for:

- overseeing the implementation of this policy;
- monitoring the Trust's overall compliance with this policy and data protection law;
- advising on the development of related policies, procedures and guidelines;
- supporting with Data Protection Impact Assessments;
- acting as a contact point for data subjects and the supervisory authority; and
- reporting on their activities, including any advice and recommendations about any data protection issues, directly to the Board of Trustees.

The DPO role is currently held by S4S, who can be contacted by email at dpo@summitlearningtrust.org.uk.

4.4 Summit Learning Trust

Summit Learning Trust is responsible for:

- advising and supporting the Academies to meet their data protection obligations;
- developing and maintaining any procedures and associated documentation required to operationalise this policy;
- ensuring a consistent approach to data protection across the Trust;
- arranging appropriate training and guidance to support staff in meeting their duties under data protection law;
- investigating personal data breaches which are either:
    - subject to a conflict of interest at the Academy where the breach occurred;
    - caused by Summit Learning Trust exclusively;
    - caused by the Professional Learning Institute exclusively; or
    - caused by South Birmingham SCITT exclusively.
- responding to information requests which are either:
    - especially sensitive in nature;
    - about multiple Academies within the Trust;
    - about Summit Learning Trust exclusively;
    - about the Professional Learning Institute exclusively; or
    - about South Birmingham SCITT exclusively.

4.5 Principals

Principals are responsible for:

- providing day-to-day leadership on data protection issues within their Academies;
- appointing a staff member to act as the Operational Lead on data protection issues within their Academy, and ensuring they fulfil their duties (see section 4.6); and
- ensuring their staff complete training arranged by Summit Learning Trust.

4.6 Operational Leads

Operational Leads are responsible for:

- acting as the Academy's main operational contact with Summit Learning Trust, with respect to data protection issues;
- maintaining an up-to-date information asset register for their Academy;
- maintaining an up-to-date register of processing activities for their Academy;
- investigating personal data breaches which occur at their own Academy, unless caused by the Operational Lead themselves (see section 12);
- responding to information requests which relate to their own Academy exclusively;
- co-ordinating any compliance visits; and
- maintaining records of all data protection training completed by staff within their Academy.

4.7 Lead Trainers

Lead Trainers are responsible for:

- maintaining records of all data protection training completed by trainees within their Academy.

4.8 All Staff

All staff are responsible for:

- processing personal data in accordance with this policy, any associated guidance and any supplementary procedures issued by Summit Learning Trust;
- informing their Line Manager about any relevant changes to their own personal data, such as a change of address (for example);
- fully participating in all data protection training arranged for them, including any updated guidance that is issued by Summit Learning Trust;
- cooperating with any reasonable request for involvement in compliance monitoring;
- reporting any personal data breach as soon as they become aware of it, in accordance with section 12 of this policy;
- ensuring data protection issues are considered before they procure any new service, in line with section 14 of this policy; and
- notifying their Operational Lead, Summit Learning Trust or the DPO if they:
    - have any questions about the operation of this policy or data protection law;
    - have any concerns that this policy is not being followed;
    - are unsure whether they can use personal data in a particular way; or
    - receive a request from an individual to exercise their rights, in accordance with section 11 of this policy.

5. Collecting personal data

We will only collect personal data where we have identified and documented a lawful basis on which to do so. For special categories of personal data, we will meet both a lawful basis and a condition outlined within data protection law to allow that data to be processed. For criminal offence data, we will meet both a lawful basis and a condition outlined within data protection law.

Whenever we collect personal data, we will provide the data subject with the relevant information required by data protection law unless the data subject has already been given this information or it would be otherwise unreasonable to provide it.

We will only collect the personal data that is necessary to fulfil the purposes for which it is required.

In the event we intend to use personal data for a purpose that differs from the one for which it was originally collected, we will inform the data subject before such processing takes place and we will seek consent where necessary.

5.1 Consent

For most of the personal data we process, we do not need consent. It depends on the purposes for which we want to use it.

For some purposes, however, consent will be required. For example, we will need to obtain consent before we use someone's image as part of our marketing and promotional materials (unless we are otherwise licensed to use the image for that purpose).

For personal data about pupils, we will usually seek consent from at least one parent/carer. However, we may instead decide it would be more appropriate seek consent from the pupil themselves. In that situation, we will consider:

- the pupil's general ability to give informed consent;
- how well the pupil understands the particular details about what they are being asked to consent to; and
- how strongly the pupil feels about the matter.

For personal data about pupils at our sixth form college, however, we will seek consent from pupils directly.

For personal data about parents/carers and staff, we will seek consent from the data subject directly.

In all cases, consent must be:

- informed;
- freely given by the appropriate person; and
- actively given.

Consent can be refused or withdrawn at any time.

We will maintain a consent form to help obtain, record and manage consent.

6. Storing personal data

We will protect the confidentiality, integrity and availability of the personal data we process. That is:

- only people who are authorised to use the data will be allowed to access it (confidentiality);
- the data will be kept accurate and up-to-date (integrity); and
- the data will be stored on central systems – not on individual computers or drives – to ensure all authorised users will be able to access it for authorised purposes (availability).

We will take appropriate organisational and technical steps to minimise the risk that personal data is lost, damaged or accessed without authorisation. Such measures will include, for example:

- entry controls to restrict physical access to areas in which personal data is stored;
- user-level or role-based permissions to control access to electronic records;
- encryption to protect electronic records;
- secure, lockable storage facilities for paper records;
- frequent backups to enable lost or damaged data to be restored;
- regular data-checking exercises to ensure data is accurate and up-to-date; and
- regular training to ensure staff are aware of our expectations for good practice.

Staff can find details about their obligations relating to data security in:

- the staff code of conduct; and
- the staff guidance maintained by Summit Learning Trust.

7. Sharing personal data

We often need to share personal data with other organisations in order to carry out our functions. This includes, but is not limited to, where:

- we use a third party supplier or contractor to help us carry out our functions;
- we are required to complete a data return to another public sector organisation, such as the Department for Education; and
- we need to report a serious concern about the safety of our pupils or staff.

We will take appropriate organisational and technical steps to ensure personal data is shared securely. Such measures will include, for example:

- data processing agreements for any third parties who process personal data on our behalf;
- passwords to restrict access to electronic files;
- encryption to protect email contents (particularly those to external organisations); and
- pseudonymisation or anonymisation, where this would not undermine the processing.

Where we transfer personal data internationally, we will do so in line with data protection law.

8. Disposing of personal data

We will only retain personal data for as long as we need it in order to fulfil the purposes for which it was processed. We will maintain a retention schedule to outline how long we will keep different types of personal data.

Once personal data is no longer needed, we will dispose of it securely. Disposal methods include:

- shredding or incineration for paper records;
- deleting or overwriting electronic records; and
- physical destruction of old devices, drives, disks and other media.

9. Photographs and videos

We take photographs and record images of individuals within and around our premises, as well as some other situations such as during trips. We do this for various purposes, including to:

- identify pupils in order to operate certain systems and services, such as school meals;
- identify staff and visitors to our premises so that we know who is permitted to be on-site;
- celebrate pupils' work and general life within our Academies;
- help showcase the Academies as part of our marketing and promotional materials; and
- operate our CCTV systems.

We will obtain consent before we use someone's image as part of our marketing and promotional materials, in line with section 5.1.

Any photographs or videos taken by parents/carers at Academy events for their own personal use are not covered by data protection law. However, for safeguarding reasons, such images should not be shared publicly – particularly on social media – where they include other people.

For other purposes, however, consent to use people's images may not be required.

We will maintain separate procedures relating to the operation of our CCTV systems.

10. Biometric recognition systems

Some of our Academies use biometric recognition systems to control access to premises and/or to deliver a cashless catering service. These systems use fingerprints for identification purposes.

When operating biometric recognition systems, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers, pupils and staff will be notified before any new biometric recognition system is put in place. We will obtain consent before we collect biometric data, in accordance with section 5.1.

11. Rights of data subjects

We are committed to upholding individuals' rights under data protection law.

It is important to understand that not all of these rights apply at all times. However, we will ensure all requests to exercise a right are always considered fairly and lawfully.

We may need to ask for identification from the person making the request before we act upon it.

11.1 Right to be informed

People have the right to be informed about what personal data we collect about them and how we use it. We will uphold this right by:

- providing data subjects with the relevant privacy notice at the time we collect their personal data, unless this information has already been given to them or it would be otherwise unreasonable to provide it.

11.2 Right of access

People have the right to access their personal data. We will uphold this right by:

- providing a simple form that can be used to make a subject access request;
- ensuring staff are able to recognise such a request made by any other method; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported.

Subject access requests can be made through this form.

11.3 Right to rectification

People have the right to have their personal data corrected if it is inaccurate, or completed if it is incomplete. We will uphold this right by:

- conducting regular data-checking exercises to give people the opportunity to identify inaccurate data;
- ensuring staff are able to recognise a request to amend personal data; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported.

11.4 Right to erasure

People have the right to have their personal data erased in certain circumstances. We will uphold this right by:

- ensuring staff are able to recognise a request to erase personal data; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported.

11.5 Right to restrict processing

People have the right to request that we limit how we use their data in certain circumstances. We will uphold this right by:

- ensuring staff are able to recognise a request to restrict processing; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported.

11.6 Right to data portability

People have the right to obtain and reuse their personal data across different services by copying or transferring it between systems in a secure way. We will uphold this right by:

- ensuring staff are able to recognise a request for data portability; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported.

11.7 Right to object

People have the right to object to the processing of their personal data in certain circumstances. We will uphold this right by:

- including clear information about this right as part of our privacy information;
- ensuring staff are able to recognise a request to object; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported.

11.8 Rights related to automated decision-making, including profiling

People have the right not to be subject to a decision based solely on automated processing, including profiling, which has a significant affect upon them. We will uphold this right by:

- informing people, as part of our privacy notices, about any processing activity that uses automated decision-making and/or profiling;
- completing a data protection impact assessment for any processing activity that is based solely on automated processing, including profiling, and

implementing any agreed actions that arise from any such assessment (see section 13);
- ensuring staff are able to recognise a request made under this right; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported.

12. Personal data breaches

We will take all reasonable steps to minimise the risk of a personal data breach. However, where a data breach does occur, it is important that staff are open and honest about it so that it can be managed quickly.

On discovering or causing a breach, or potential breach, the staff member must report it immediately using the breach report form on SharePoint. An automatic notification will be sent to the Operational Lead, Summit Learning Trust and the Data Protection Officer.

Breaches that occur at an Academy will normally be investigated by the Operational Lead for that Academy. However, if this would create a conflict of interest, the investigation will be completed by Summit Learning Trust. Breaches that occur elsewhere within the organisation, or which are caused by a data processor, will be investigated by Summit Learning Trust.

All breach investigations will:

- consider how the breach was caused;
- assess the likely risk to individuals as a result;
- recommend any actions that might be taken to mitigate that risk; and
- reflect on how to reduce the likelihood that a similar breach will occur in future.

In the event that the investigation finds a risk to individuals is likely, we will report the breach to the ICO. Where feasible, we will do this within 72 hours; otherwise, we will do this without undue delay. Any such reports will be completed by our Data Protection Officer.

In the event that the investigation finds a risk to individuals is high, we will notify those individuals directly and without undue delay.

We will record all personal data breaches, including those that are not reported to the ICO.

13. Data protection impact assessments

In the event we plan to introduce a new data processing activity, or that we plan to change the way any existing processing is conducted, we will consider whether to carry out an impact assessment.
We will maintain a screening tool to ensure this is considered consistently across the Trust.

It is the Project Lead's responsibility to ensure that the screening tool is completed for any project that involves personal data.

Where we decide an impact assessment should be carried out, it will be completed during the project planning stage before any decisions are made about whether to approve the processing. This will allow us to identify the associated data protection risks early enough that we can act to minimise them.

Our Data Protection Officer will have a significant role in all data protection impact assessments.

14. Third party suppliers

Whenever we procure a service from a third party supplier – such as a piece of software, an app or an online subscription – we will consider whether it needs to process personal data on our behalf. Where it does, that supplier would be our data processor.

Staff must first discuss their intention to use such a service with an appropriate person within their Academy (such as a Subject Leader, Operational Lead or Principal). There should be agreement that the service:

- would have a clear benefit; and
- does not duplicate a service that is already in use.

Once agreement is reached, staff must request approval before they procure the service. All such requests should be made using the approval form on SharePoint. Staff should give as much notice as possible in advance of the date on which the service is required.

Summit Learning Trust will arrange for those checks to be carried out, before we enter into any contract with a data processor, to assess their compliance with our data protection standards.

The outcome will be explained to the staff member who made the request, and might be to:

- authorise the service for immediate use;
- authorise the service subject to certain conditions; or
- refuse authorisation.

Where authorisation is given, an appropriate data processing agreement must be in place before any personal data is shared with the supplier. We will maintain a template for this purpose.

Where authorisation is refused, the service must not be used.

15. Training and support

We are committed to supporting our staff to meet their duties relating to data protection. Accordingly, we expect all staff to complete:

- a mandatory induction in data protection when they join the organisation, which will include:
    - an essential overview of basic data protection law;
    - the detailed guidance about our expectations for good practice; and
    - a copy of this policy; and
- mandatory annual refresher training.

Operational Leads will keep a record of the mandatory training completed by Academy-based staff.

Lead Trainers will keep a record of the mandatory training completed by trainees.

Summit Learning Trust will keep a record of the mandatory training completed by Trust-based staff.

Staff will have ongoing access to training materials in case they would like to refresh their own understanding of the content.

Staff will also have access to key people in case they have any questions about data protection or any concerns about poor practice. Staff can contact:

- the Operational Lead for their Academy (usually the Academy's Business Manager);
- Summit Learning Trust (trust.data@summitlearningtrust.org.uk); or
- the Data Protection Officer (dpo@summitlearningtrust.org.uk).

16. Monitoring and review

The Data Protection Officer will independently monitor our compliance with this policy – and with data protection law more broadly – on an annual basis. Independent monitoring will include:

- site walks to identify any examples of poor practice to address, or good practice to share;
- interviews to assess the level of understanding among staff and to identify any potential training requirements;
- a review of any data breaches to assess how they were handled and learned from; and
- a deep dive into a particular theme related to data protection.

The results of independent monitoring will be reported directly to the Board of Trustees and circulated to Summit Learning Trust and the Academies.

Summit Learning Trust, the Academies and their Local Governing Body may carry out additional monitoring at their discretion.

This policy will be reviewed by the Board of Trustees every two years, or else following any proposal to change its content significantly.