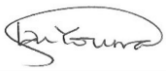
The Sycamore Church of England Trust

Grow together, Learn forever

Data Protection Policy

Applicable to:	All Trust Schools
Adopted By:	Trust Lead
Date Adopted:	February 2022
Authorised Signatory:	
Mr Ian Young – Trust Leader and CEO	
Mr Mark Granby – Chair of Board of Trustees	
Review Period:	Annually
Next Review:	February 2025

Grow together, Learn forever

Record of Policy Changes and Reviews

Date	Details	Reason for Review / Change
March 2023	Policy reviewed by our newly appointed DPO (Shard Business Services).	Annual Review, Updated guidance incorporating data breach policy and subject access request policy
February 2024	Annual review	Annual review

Overview

The Sycamore Church of England Trust (hereafter "the Trust"), takes the security and privacy of personal data seriously. The Trust needs to gather and use information or 'data' as part of its day-to-day business and to manage its contractual relationships. The Trust intends to comply with its legal obligations under the Data Protection Act 2018 (the '2018 Act') and the United Kingdom General Data Protection Regulation ('UK GDPR') in respect of data privacy and security. The Trust has a duty to notify staff, Trustees and other stakeholders who work for and on behalf of, the Trust of the information contained in this Policy.

This policy applies to current and former employees, Trustees, volunteers and other who work for and on behalf of the Trust. If you fall into one of these categories, please read this policy alongside your contract of employment (or contract for services) and any other notice the Trust issues from time to time in relation to personal data.

This policy also informs parents, carers, guardians, and pupils of the Trust's approach to data protection.

The Trust has measures in place to protect the security of personal data in accordance with the Data Security Policy.

The Trust will hold data in accordance with the guidance contained in the Information and Record Management Society's Toolkit for Academies. The Trust will only hold data for as long as necessary for the purposes for which it was collected.

The Trust is a 'Data Controller' for the purposes of processing personal data. This means that the Trust determines the purpose and means of the processing of personal data.

This policy explains how the Trust will hold and process personal data. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Trust.

This policy does not form part of your contract of employment (or contract for services if relevant) and may be amended by the Trust at any time.

Legislation and Guidance

This policy is fully compliant with the Data Protection Act (2018) and the UK GDPR and is based on guidance provided by the Information Commissioner's Office (ICO). If any conflict arises between those laws and this policy, the Trust intends to comply with the Data Protection Act 2018 the UK GDPR.

Definitions

The terms in this document have the meanings as set out in Article 4 of the GDPR unless amended by the Act.

For clarity, the following have been reproduced:

- '**personal data**' means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **'special category personal data'** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- **'processing'** means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **'data controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **'data processor'** means a person, other than an employee of the data controller, who processes the data on behalf of the data controller.
- **'data subject'** means a person whose personal data is held or processed.

Roles and Responsibilities

Trust Board

- The Trust Board has overall responsibility for ensuring that the Trust complies with its obligations under the UK GDPR and the Data Protection Act 2018.

Data Protection Officer

- The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
- The DPO will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on school data protection issues.
- DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.
- Our DPO is Shard Business Services (See Contact details below)

CEO/Central Team

- The CEO acts as the data controller's representative of the Trust.
- The Central Team acts as the data controller's representative on a day-to-day basis.
- The Central Team will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

All Staff

- Staff are responsible for:

- ensuring that they collect and store any personal data in accordance with this policy.
- keeping the school informed of any changes to their personal data, such as a change of address.
- contacting the DPO in the following circumstance:-
  - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - if they have any concerns that this policy is not being followed
  - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the United Kingdom
  - if there has been a data breach
  - before engaging in a new activity that may affect the privacy rights of individuals
  - if they need help with any contracts or sharing personal data with third parties

Data Protection Principles

The UK GDPR is based on the following data protection principles or rules for good data handling:

- data shall be processed fairly, lawfully and transparently
- personal data shall be obtained only for one or more specific, explicit and legitimate purposes
- personal data shall be adequate, relevant and limited to what is necessary to fulfil the purpose(s) for which it is processed
- personal data shall be accurate and, where necessary, kept up to date
- personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- personal data shall be processed in a way that ensures it is appropriately secure
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and accidental loss or destruction of, or damage to, personal data

Lawful Bases for Processing Personal Data

The Trust will process personal data where there is one or more lawful bases to do so under the legislation, including:

- The data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g., to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest, and carry out its official functions

Where the Trust is not operating in its capacity as a public authority, for example for the purposes of facilities hire, or after-Trust activities not tied to curriculum, the lawful basis for that processing will be legitimate interest.

The Trust may process personal data for these purposes without knowledge or consent.

The Trust will not use personal data for an unrelated purpose without disclosing the intent, providing the lawful basis for the processing and seeking consent if necessary.

Whenever personal data is collected from individuals, they will be provided with the relevant information including details of the data collected and how it is collected, stored and shared, via a Privacy Notice (sometimes called a Fair Processing Notice) as required by the UK GDPR and the Data Protection Act (2018).

When processing 'special categories' of personal data, the Trust will identify one of the special category conditions for processing set out in the UK GDPR, and where relevant a condition specified in Schedule 1 to the Data Protection Act 2018 (see Appendix1: ***Appropriate Policy Document***), in that:

- The data is processed to ensure the vital interests of the individual where they are physically or legally incapable of giving consent
- The data has been made public by the individual e.g., on social media
- Processing is necessary to carry out rights and obligations under employment law
- Processing is necessary for the assessment of a person's working capacity either based on UK Law or under contract with a health professional such as an occupational health provider
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest, based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Where no lawful basis for processing exists, the Trust must seek consent for that processing. For example, where the Trust wishes to use images of pupils in marketing publications or on social media channels, written consent must be sought from the parent/carer.

Criminal Convictions

The Trust may use information relating to criminal convictions where the law allows us to do so.

The Trust will hold information about criminal convictions if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if any information about criminal convictions becomes apparent during a stakeholder's relationship with the Trust.

Information about criminal convictions and offences will be used in the following ways:

- To ensure employee suitability to work
- For safeguarding purposes

Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect an individual's interests (or someone else's interests) and they are not capable of giving consent, or where information has already been made public.

Sharing Personal Data

The Trust will not share personal data with third parties, without consent, unless the law and our policies allow it to do so.

The Trust is required, by law, to pass certain information to specified external bodies, to meet our statutory obligations. Examples of organisations with whom personal data may be shared regularly include, but are not limited to:

- Department for Education
- The Local Authority
- Ofsted
- Disclosure and Barring Service
- HMRC
- Teachers' Pension Service
- Local Government Pension Service

Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies, HR Consultants, Occupational Health Services, Wellbeing Services, etc. When selecting companies and contractors to work with, the Trust will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with current data protection legislation
- Establish a data-sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data shared with them
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

The Trust requires these companies to keep personal data confidential and secure and to protect it in accordance with Data Protection law and the Trust's policies. They are only permitted to process the data for the lawful purpose for which it has been shared and in accordance with the Trust's instructions.

The Trust may also share personal data as is necessary and proportionate with emergency services and local authorities to help them to respond to an emergency that affects any of its pupils and staff. An emergency includes, but is not limited to:

- preventing serious physical harm to a person
- preventing loss of human life; protection of public health
- safeguarding vulnerable adults or children
- responding to an emergency.

The Trust may also share data with Law Enforcement agencies and Government bodies where it is legally required to do so for:

- for the prevention or detection of crime and/or fraud
- for the apprehension or prosecution of offenders;
- the assessment or collection of tax owed to HMRC
- in connection with legal proceedings
- where the disclosure is required to satisfy its safeguarding obligations
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

Transferring Personal Data Out of the UK

The Trust may, from time-to-time, transfer ('transfer' includes making available remotely), personal data to countries outside of the UK.

The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the Secretary of State has determined ensures an adequate level of protection for personal data
- The transfer is to a country (or international organisation) that provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the Information Commissioners Office; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made under exceptional circumstances and one of the derogations in Article 49 of the UK GDPR applies:
    - the transfer is made with the informed consent of the relevant data subject(s)
    - the transfer is necessary for the performance of a contract between the data subject and the Trust (or for pre-contractual steps taken at the request of the data subject);
    - the transfer is necessary for important public interest reasons
    - the transfer is necessary for the conduct of legal claims
    - the transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
    - the transfer is made from a register that, under UK law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Security

Everyone who works for, or on behalf of, the Trust has responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Trust's Data Security and Data Retention policies.

Data Security - Organisational Measures

The Trust shall ensure that the following measures are taken concerning the collection, holding, and processing of personal data:

- All staff, volunteers, contractors, service providers or other parties working on behalf of the Trust shall be made fully aware of their individual responsibilities and the Trust's responsibilities under the UK GDPR and this Policy, and shall have free access to a copy of this Policy
- Only those working for or on behalf of the Trust that require access to, and use of personal data to carry out their assigned duties shall have access to personal data held by the Trust
- Those working for or on behalf of the Trust who engage with the handling personal data will be appropriately trained to do so and adequately supervised
- Those working for or on behalf of the Trust shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed
- All personal data held by the Trust shall be reviewed periodically, as set out in the Trust's Data Retention Policy.

Data Security -Technological Measures

The Trust shall ensure that the following measures are taken concerning IT and information security:

- The Trust requires that any passwords used to access personal data shall have a minimum of 8 characters, composed of a mixture of upper- and lower-case characters, numbers and symbols. Passwords are not expected to be changed regularly, but users will be expected to change their password when instructed by the Trust:
- Passwords should not be written down or shared between any staff or other parties working for or on behalf of the Trust, irrespective of seniority or function. If a password is forgotten, it must be reset using the applicable method.
- All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Trust's IT staff shall be responsible for installing security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any Trust-owned computer or device without authorisation.
- Contravention of these rules may be treated as a disciplinary matter.

Data Security – Storage

The Trust shall ensure that the following measures are taken concerning the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption
- All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar
- All personal data relating to the operations of the Trust, stored electronically, should be backed up regularly
- Where any member of staff stores personal data on a mobile device (whether that be a computer, tablet, phone or any other device) then that member of staff must abide by the Trust's Acceptable Use Policy. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information

Data Security – Disposal

The Trust shall ensure that the following measures are taken concerning the disposal of personal data:

- When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted or disposed of. For further information on the deletion and disposal of personal data, please refer to the Trust's Data Retention Policy and Schedule

Data Security – Use of Personal data

The Trust shall ensure that the following measures are taken concerning the use of personal data:

- No personal data may be shared informally and if an employee, volunteer, processor, or other party working for or on behalf of the Trust requires access to any personal data that they do not already have access to. Such access should be formally requested from the Director of Operations.
- Personal data must always be handled with care and should not be left unattended or on view to unauthorised persons at any time
- If personal data is being viewed on a computer screen and the computer is to be left unattended, the user must lock the computer and screen before leaving it; and
- Where personal data held by the Trust is used for marketing purposes, appropriate checks to ensure consents for such processing are in place must be carried out before the data is used.

Data Breach Notification

All personal data breaches must be reported immediately to the Data Protection Officer.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure the Information Commissioner's Office is informed of the breach without delay, and within 72 hours after having become aware of it.

If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include, as a minimum, the following information:

- The categories and approximate number of data subjects concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the Trust's Data Protection Officer (or another contact point where more information can be obtained)
- The likely consequences of the breach.
- Details of the measures taken or proposed to be taken, by the Trust to address the breach including, where appropriate, measures to mitigate possible adverse effects.

For further information, please refer appendix 2.

Subject Access Requests (SARs)

Data subjects may make subject access requests ("SARs") at any time to access the personal data which the Trust holds about them, what it is doing with that personal data, and why. Data subjects are encouraged to approach the Trust directly to make a request.

Adhering to the data protection regulations is the responsibility of every staff member acting for or on behalf of the Trust, and the ability to identify and appropriately handle a request is considered to be part of every employee's role.

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implication of submitting a SAR, or have given their consent. Typically, children under 12 are considered unable to understand their rights, and parents can make SARs on their behalf, but this should be evaluated on a case-by-case basis and should not be applied in a blanket fashion.

Staff wishing to make a SAR may approach their line manager, the DPO or submit it directly to the Trust. Any staff member who receives a SAR must forward it to the DPO.

Subject access requests can be made verbally or in written form; however, the Trust would encourage requesters to document their request in written form.

The Trust must respond within one month unless the request is complex or numerous, in which case the response can be extended by a further two months. If such additional time is required, the data subject shall be informed without undue delay.

Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

There is no fee for making a SAR. However, if a request is unfounded or excessive the Trust may charge a reasonable administrative fee or refuse to respond to the request

When responding to SARs, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- May ask for clarification or specification

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of a pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interest
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

Subjects should also be aware there are exemptions to the regulation and some information will not be provided. If this is the case, the requester will be informed of the exemption that applies. We may also refuse to act on a request that is unfounded or excessive.

Data subjects have the right to complain to the ICO.

The Data Subject's Rights

All data subjects have the right to:

- information about the personal data the Trust process, how it is processed and on what basis it is processed, as set out in this policy.
- access their own personal data by way of a Subject Access Request (see above).
- correct any inaccuracies in their personal data.
- request that the Trust erase personal data where the Trust is not entitled under the law to process it, or it is no longer necessary to process it for the purpose it was collected.
- request the processing of personal data is restricted during the application for correction or erasure, or when contesting the lawfulness of the processing.
- object to data processing where the Trust is relying on a legitimate interest to do so and where it is considered the rights and interests of the data subject outweigh those of the Trust.
- object to the processing of personal data for direct marketing.
- receive a copy of their personal data, and transfer their personal data to another data controller, in certain circumstances.
- with some exceptions, not be subjected to automated decision-making.
- be notified of a data security breach concerning their personal data in certain circumstances.
- withdraw consent to processing where consent is the sole lawful basis for the processing.

Accountability & Record Keeping

The Trusts Data Protection Officer is Shard Business Services who can be contacted by emailing DPO@shardbusinessservices.co.uk

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Trust's other data protection-related policies, and compliance with the UK GDPR and other applicable data protection legislation.

The Trust shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Trust, its Data Protection Officer, and any applicable third-party data processors
- The purposes for which the Trust collects holds, and processes personal data:
- Details of the categories of personal data collected, held and processed by the Trust, and the categories of data subject to which that personal data relates
- Details of any transfers of personal data outside the UK, including all mechanisms and security safeguards
- Details of how long personal data will be retained by the Trust (please refer to the Trust's Data Retention Policy & Schedule); and
- Detailed descriptions of all technical and organisational measures taken by the Trust to ensure the security of personal data.

Data Protection Impact Assessments

The Trust shall carry out Data Protection Impact Assessments for all new projects and/or new uses of personal data which involve the use of new technologies/new service providers and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed
- The purpose(s) for which personal data is to be used
- The Trust's objectives
- How personal data is to be used
- The parties (internal and/or external) who are to be consulted
- The necessity and proportionality of the data processing related to the purpose(s) for which it is being processed
- Risks posed to data subjects
- Risks posed both within and to the Trust; and
- Proposed measures to minimise and handle identified risks.

Training and Awareness

Staff, Trustees, and other stakeholders who work for, or on behalf of, the Trust are provided with Data Protection training as part of the induction process.

Data Protection training forms part of continuing professional development within the Trust where changes to legislation and/or the Trust's processes make it necessary.

Monitoring Arrangements

The Trust's Data Protection Officer and the Data Controller's Representative are responsible for reviewing this policy and updating the Trust Board on the Trust's data protection responsibilities and any risks in relation to the processing of data. Any questions in relation to this policy or data protection should be directed to these persons.

The Data Controller's Representative, together with the Data Protection Officer, will check that the Trust complies with this policy by reviewing Trust records, policies, and procedures annually.

This policy will be reviewed and updated as and when necessary, in relation to any amendments to Data Protection legislation or guidance, or any internal concerns resulting from policy violations, data breaches, or on an annual basis.

At every review, the policy will be shared with the Trust Board.

Contacts

Any questions or concerns about how the Trust process personal information, or any requests to exercise data protection rights, should be submitted to the Trust in the first instance.

If the Trust is not able to address concerns and resolve them satisfactorily, please contact the Data Protection Officer at the address below.

Finally, concerns can be registered with the UK's data protection regulator, the Information Commissioner's Office, by following this link https://ico.org.uk/global/contact-us/email/

Contact Details

Data Controller:	The Sycamore Church of England Trust c/o Christ Church C.E. Primary School Church Street, Bury, BL8 3AX
Data Controller's Representative:	Ian Young. CEO
Data Protection Officer:	Shard Business Services DPO@shardbusinessservices.co.uk

Links With Other Policies

This Data Protection Policy is linked to:

- Appropriate Policy Document
- Data Retention Policy and Schedule
- Subject Assess Request Policy
- Privacy Notice for Parents
- Privacy Notice for Pupils
- Privacy Notice for Employees
- Privacy Notice for Trustees
- Privacy Notice for Job Applicants

Appendix 1: Appropriate Policy Document

For use when relying on specified conditions for the processing of special categories of personal data, and personal data relating to criminal convictions and offences

Introduction

1.1. This is the 'Appropriate Policy Document' required when The Sycamore Church of England Trust seeks to rely on any of the conditions specified in Schedule 1 to the Data Protection Act 2018, for the processing of special category and criminal convictions personal data.

1.2. The content of this Appropriate Policy Document meets the requirements of paragraph 39 of Schedule 1 of the Data Protection Act (2018), in that it –

- explains the Trust's procedures for securing compliance with the principles in Article 5 of the UK General Data Protection Regulation ('UK GDPR') - principles relating to the processing of personal data, in connection with the processing of personal data in reliance on the condition in question; and
- explains the Trust's policies as regards the retention and erasure of personal data processed in reliance on the condition, indicating how long such personal data is likely to be retained.

1.3. Under paragraph 40(1) of Schedule 1 of the DPA (2018), where the Trust processes personal data in reliance on a condition described in paragraph 38 of Schedule 1, they will, during the relevant period[1]

- retain the appropriate policy document,
- review and (if appropriate) update it from time to time, and
- make it available to the Information Commissioner, on request, without charge

Description of Data Processes

2.1. As part of its statutory and business functions, the Trust processes special category data related to stakeholders, including staff, Trustees, and volunteers, job applicants, pupils and parents/carers. This includes where relevant, information about health, disability and wellbeing, ethnicity, trade union membership, religious or philosophical beliefs, biometric data. Further information about this processing can be found in the relevant Privacy Notices.

2.2. Processing for reasons of substantial public interest relates to the data the Trust receives, obtains, or creates to fulfil our statutory obligations. For example, this may be related to the safeguarding of pupils, supporting staff with a particular disability or medical condition, for equal opportunities monitoring, safeguarding, etc.

2.3. A record of our processing activities is kept under Article 30 of the UK GDPR.

[1] The 'relevant period' begins when the data is collected and ends no less than 6 months following cessation of the processing

Schedule 1 Condition for Processing

3.1. The Trust processes special category data for the following purposes in Part 1 of Schedule 1 of the Data Protection Act (2018):

- Paragraph 1: Employment, social security and social protection.

3.2. The Trust may process special category data for the following purposes in Part 2 of Schedule 1 of the Data Protection Act (2018):

- Paragraph 6: Statutory, etc. purposes.
- Paragraph 8: Equality of opportunity and treatment.
- Paragraph 16: Support for individuals with a particular disability or medical condition
- Paragraph 17: Counselling
- Paragraph 18: Safeguarding of children and individuals at risk
- Paragraph 20: Insurance
- Paragraph 21: Occupational Pensions

Criminal Offence Data

4.1. The Trust processes criminal offence data for the following purposes in parts 1 and 2 of Schedule 1 of the Data Protection Act (2018).

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 18 (1) Safeguarding of Children and individuals at risk

Securing Compliance with the Data Protection Principles

5.1. The Trust's procedures for complying with Article 5 of the GDPR: Data Protection Principles are as follows:

Principle A: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Trust will:

- ensure that personal data is only processed where at least one of the conditions in Schedule 1 is met or the data subject has given their explicit consent for the processing.
- only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent (provision of privacy notices).
- where necessary carry out Data Protection Impact Assessments to ensure proposed processing is carried out fairly.

Principle B: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The Trust will:

- only collect personal data for specified, explicit and legitimate purposes and will inform data subjects what those purposes are through the provision of privacy notices.
- not use personal data for purposes that are incompatible with the purposes for which it was collected.
- before personal data is used for a new purpose that is compatible, the Trust will inform the data subject.

Principle C: Personal data shall be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

The Trust will:

- only collect the minimum personal data needed for the purpose for which it is collected.
- ensure the data is adequate and relevant to the purpose for which it is collected.
- apply Data Protection Impact Assessments to ensure proposed processing is not excessive.
- Where personal data is provided to, or obtained by the Trust but is not relevant to a stated purpose, it will be erased.

Principle D: Personal data shall be accurate and, where necessary, kept up to date.

The Trust will ensure that:

- personal data is accurate and kept up to date as necessary.
- when notified of inaccuracies personal data is corrected.
- Where the Trust become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, every reasonable step will be taken to ensure that data is erased or rectified without delay. If the Trust decides not to either erase or rectify it, for example, because the lawful basis relied upon to process the data means these rights don't apply, the decision not to erase will be documented.

Principle E: Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

The Trust will ensure that:

- personal data will only be kept in identifiable form only as long as is necessary for the purposes for which it is collected unless otherwise required by law.
- when no longer needed, personal data shall be securely deleted or anonymised.

- personal data is held and disposed of in line with the Trust's Data Retention Policy and Schedule.

Principle F: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Trust will ensure that:

- there are appropriate organisational and technical measures in place to protect personal data.
- data is processed in accordance with its Data Handling and Classification Procedure and Data Security Policy and Procedure.

Accountability Principle

6.1. Under GDPR Article 5(2), the Trust is responsible for and must be able to demonstrate compliance with the principles listed above.

6.2. The Trust has appointed a Data Protection Officer in accordance with Article 37 of the UK GDPR. The DPO provides independent advice and monitoring of personal data handling and has access to report to the highest management level.

6.3. The Trust will:

- ensure that records are kept of all personal data processing activities and that these are provided to the Information Commissioner on request (RoPA).
- carry out a Data Protection Impact Assessment for any high-risk personal data processing and consult the Information Commissioner if appropriate.
- have in place internal policies and procedures to ensure that personal data is collected, used or handled only in a way that is compliant with data protection law.
- Policies for Retention and Erasure of Personal Data
- The Trust will ensure, where special category or criminal convictions personal data is processed, that:
- there is a Record of Processing Activities (ROPA), and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data.
- where special category or criminal convictions personal data is no longer required for the purpose for which it was collected, it will be securely deleted or rendered permanently anonymous in accordance with the Trust's Data Retention Policy and Schedule.
- data subjects receive a Privacy Notice (sometimes called a fair processing notice) detailing how their data will be handled, including the period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period.

Additional Special Category Processing

7.1. The Trust processes special category personal data in other instances where there is not a requirement to keep an Appropriate Policy Document. Our processing of such data is in accordance with data protection legislation and respects the rights and freedoms of the data subjects.

7.2. The Trust will provide clear and transparent information about why personal data is processed including the lawful basis for processing in stakeholder Privacy Notices. Copies of Privacy Notices are available from the office.

Contact Information

8.1. If you have any questions or concerns about how the Trust process information or wish to exercise any data protection rights, please contact the Trust in the first instance.

8.2. If you have concerns that the Trust has not been able to resolve to your satisfaction you may contact the Data Protection Officer using the details below.

8.3. Alternatively, concerns can be registered the UK's data protection regulator, the Information Commissioner's Office by following this link https://ico.org.uk/make-a-complaint/

Contact Details

Data Controller:	The Sycamore Church of England Trust c/o Christ Church C.E. Primary School Church Street, Bury, BL8 3AX
Data Controller's Representative:	Ian Young. CEO
Data Protection Officer:	Shard Business Services DPO@shardbusinessservices.co.uk

Appendix 2 – Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. So, a data breach has occurred if personal data has been lost, stolen, destroyed (accidentally or in error), altered (accidentally or in error), disclosed accidentally or in circumstances where it should not have been or otherwise made available to unauthorised people.

Step 1: On finding or having caused a data breach, staff members or third-party data processors must notify the Data Protection Officer immediately.

Step 2: The DPO must notify the CEO immediately when notified of a breach.

Step 3: The DPO will take all reasonable steps to contain the breach and minimise its effects as far as possible, requesting action from staff members and any third-party data processors that may be required.

- Can the data be retrieved or safely deleted/destroyed by any unintended recipient(s)?
- Are we certain we have identified all the data that was lost/mistakenly disclosed or altered etc?

Step 4: At the earliest possible time, the DPO will assess the potential consequences of the breach. The DPO should consider;

- How could it affect the data subject(s) involved?
- How serious will these effects be for the data subjects?
- How likely is it that the data subjects could be affected in this way(s)?

Step 5: The DPO must decide whether or not the breach must be reported to the ICO. Breaches must be considered on a case-by-case basis; however, a breach must be reported to the ICO if it is likely to result in any physical, material or non-material damage such as;

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation

- damage to reputation
- or any other significant economic or social disadvantage to the individual(s) concerned

If the breach is likely to affect anybody in any of the ways described above, and cannot be successfully contained or rectified, it must be reported to the ICO.

Step 6: The DPO will document the decision taken as to whether or not the ICO are notified of the breach. The school should keep a record of this decision in case it is challenged at a later date by any of the individuals involved or by the ICO. The school should keep a record of breaches whether or not they are reported to the ICO. This record should include:

- A description of the breach and how it occurred
- Details of the data involved
- A description of the potential consequences of the breach
- Details of how likely it is any individuals could be affected
- A description of measures taken to contain or rectify the breach
- Actions taken to avoid any repeat of errors that lead to the breach

Step 8: In cases where the breach must be reported to the ICO, the DPO (or another member of staff if they are not available) must do so within 72 hours of becoming aware of the breach. Such breaches are reported via the relevant page on the ICO's website.

Step 9: The DPO must decide whether or not the individual's affected by the breach must be notified. Again, the potential risks to any affected individuals (described in Step 5), the severity of any affects and the likelihood of them being affected must guide this decision-making process. If there is a high risk the DPO will notify, in writing, all potentially affected individuals. This notification will include:

- Contact details for the DPO
- A description of how the breach occurred and the data involved
- A description of the measures taken to contain or rectify the breach
- Any advice it is possible to provide in terms of how the individuals could be affected

Step 10: The DPO must ensure records of breaches and decisions taken relating to them are stored and accessible in the event of any subsequent investigation by the school or the ICO.