The Sycamore Church of England Trust

Grow together, Learn forever

Privacy Notice: Workforce

Applicable to:	All Trust Schools
Adopted By:	Trust Board
Date Adopted:	May 2018
Authorised Signatory:	
Mr Ian Young – Trust Leader and CEO	
Mr Mark Granby – Chair of Board of Trustees	
Review Period:	Annually
Last Update:	January 2026
Next Review:	January 2027

Contents

Introduction ____ 4
1. Data Protection Principles ____ 4
2. Categories of data we collect ____ 4
3. Collecting this information ____ 5
4. Why we collect and process workforce personal data. ____ 6
5. Automated Decision Making ____ 6
6. The Lawful Bases on which we Process Personal Data ____ 7
7. Criminal Proceedings/Convictions ____ 7
8. Consent ____ 7
9. Change of Purpose ____ 8
10. Storage and Retention of Personal Data ____ 8
11. CCTV ____ 8
12. Sharing Personal Data ____ 9
Third-party service providers ____ 9
13. Transferring Data Outside The UK ____ 10
14. Data Security ____ 10
15. Your Data Subject Rights ____ 10
Your Duty to Inform us of Changes. ____ 11
Subject Access Requests ____ 11
Fulfilling A Subject Access Request ____ 11
Fees ____ 11
Exercising Other Data Subject Rights ____ 11
The Right to Withdraw Consent ____ 11
16. Complaints ____ 12
17. Contact us ____ 12
18. Changes to this Privacy Notice ____ 12
How the Government uses your data ____ 14
Data collection requirements ____ 14
Sharing by the Department ____ 14
How to find out what personal information DfE hold about you ____ 14

Record of Policy Changes and/or Reviews

Date	Details	Reason for Review/Change
January 2026	Sentence added to complaints section: We will acknowledge your concern within 30 days and will respond without undue delay.	ICO advice following review

Introduction

Under data protection law, individuals have a right to be informed about how the Trust uses any personal data that we hold about them. We comply with this right by providing privacy notices (sometimes called fair processing notices) to individuals where we are processing their personal data.
This privacy notice explains how and why we collect, store, and use personal data about pupils.

We, The Sycamore Church of England Trust are the 'data controller' for the purposes of data protection law. The Trust is registered as a data controller with the Information Commissioners Office (ICO). Our registration number is ZA253323

This Privacy Notice relates to The Sycamore CE Trust, and its constituent Academies:

- Christ Church C.E Primary School
- St. John's C.E Primary School
- Radcliffe Hall C.E / Methodist Primary School
- St Stephen's C.E Primary School
- St Thomas's C.E Primary School
- Holy Trinity C.E Primary School

and any other Academy which joins the Trust in the future (hereafter referred to as the 'Trust').

Our data protection officer is Shard Business Services (see 'Contact us' below).

1. Data Protection Principles

Personal Data must be processed in accordance with the six Data Protection Principles. It must be:

- used lawfully, fairly and in a transparent way.
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- relevant to the purposes we have told you about and limited only to those purposes.
- accurate and kept up to date.
- kept only as long as necessary for the purposes we have told you about.
- kept securely.

2. Categories of data we collect

The categories of workforce personal data that we collect, process, hold, and share include but is not limited to:

- contact details including your name, address, email address and telephone number, date of birth and gender.
- other personal details including your date of birth, marital status, gender, next of kin and emergency contact numbers.
- the terms and conditions of your employment including position, annual leave entitlement, pension and benefits information, days of work and working hours.
- qualifications and employment records, including work history, job titles, working hours, training records and professional memberships, start date, post, roles including start and end dates, with previous employers and with the Trust.
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover.

- details of your bank account, payroll records, National Insurance number and tax status information, pension contributions, student loans and other deductions, and timesheets.
- information about your entitlement to work in the UK, DBS Checks and Children's Barred list information, Overseas check, Teacher status checks.
- information about your criminal record (see Section 7 below)
- details of periods of leave taken, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.
- assessments of performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence.
- Settlement agreements, COT3 agreements, and claims to an Employment Tribunal or Employment Appeal Tribunal
- details of driving licence, passport, and other relevant identity documents
- Photographs
- CCTV footage (where relevant)
- Data related to the use of the Trust's information and communications systems.
- Any other personal data we will inform you of from time to time.

We may also collect, store, and use information about you that falls into "special categories" of more sensitive personal data. This includes information about:

- medical or health conditions, including whether or not you have a disability for which the Trust needs to make reasonable adjustments.
- equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religious or philosophical beliefs.
- political opinion
- biometric data (where relevant)
- details of Trade Union Membership

3. Collecting this information

We collect workforce personal data from:

- either directly from individuals or indirectly via employment agencies and other bodies
- your passport, driving licence or other identity documents.
- third parties including references from previous employers; the Local Authority or other agencies (e.g., DBS Checks)
- forms you completed at the start of, or during your employment, such as Benefit Nomination forms, emergency contact, etc,
- health providers such as Occupational Health and Fitness to Work notifications.
- information generated during your employment including attendance records, sickness records, performance reviews and complaint/disciplinary/grievance investigations.

The majority of workforce data provided to us is mandatory, some of it is provided to us voluntarily. To comply with the UK General Data Protection Regulation, we will inform you whether you are required to provide certain information to us, if you have a choice in this and what the possible consequences of failing to provide this personal data would be.

4.Why we collect and process workforce personal data.

The Trust collects information to safeguard our users, promote the objects and interests of the Trust, facilitate efficient operations, and ensure that all relevant legal obligations are complied with. For example, we collect data to:

- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights.
- facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace.
- operate and keep a record of employee performance and related processes, to plan for career development, succession planning and workforce management purposes.
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled.
- obtain occupational health advice, to comply with duties concerning individuals with disabilities, to meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled.
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Trust complies with duties concerning leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled.
- ensure effective general HR and business administration.
- inform our recruitment and retention policies.
- allow better financial modelling and planning.
- provide references on request for current or former employees.
- enable equalities monitoring.
- respond to and defend against legal claims.

5.Automated Decision Making

Automated decision-making takes place when an electronic system uses personal information to make decisions without human intervention. We are permitted to use automated decision-making in limited circumstances.

We ***do not*** envisage that any decisions will be taken about you using automated means. However, we will notify you in writing if this position changes.

6.The Lawful Bases on which we Process Personal Data

We only collect and use personal data when the law and our policies allow us to do so. We process general category data where:

- the data subject, or a person with the lawful authority to exercise consent on the data subject's behalf, has given consent.
- the processing is necessary for a contract we have with you, or because it is necessary to take steps before entering into a contract with you.
- the processing is necessary for us to comply with a legal obligation.
- the processing is necessary to protect your vital interest or that of another person.
- the processing is necessary for us to perform a task in the public interest or for our official functions, and this task or function is lawful.

We process special category data where:

- the data subject, or a person with the lawful authority to exercise consent on the data subject's behalf, has given explicit consent.
- the processing is necessary for carrying out our obligations concerning employment law.
- the processing is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent.
- the processing relates to personal data which are manifestly made public by the data subject.
- the processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity.
- the 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.
- the processing is necessary, where applicable, for preventative or occupational medicine to assess the working capacity of the employee or to obtain a medical diagnosis.
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Some of the reasons listed above for collecting and using personal data overlap, and there may be several grounds that justify our use of this data.

7.Criminal Proceedings/Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our legal and safeguarding obligations and provided, we do so in line with data protection legislation.

We envisage that we will hold information about criminal convictions if information about criminal convictions comes to light as a result of your appointment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your time as an employee.

Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and/or the Police.

Such information will only be processed to the extent that it is lawful to do so, and appropriate measures will be taken to keep the data secure.

8.Consent

We may process personal information without your consent, in compliance with the above lawful bases (section 6), where this is required or permitted by law and our policies.

We will ask for consent to process general personal data where there is no other lawful basis for processing it. For example, where we wish to use your photographs on our website or social media channels for promotional/marketing purposes.

In limited circumstances, we may approach you for your written consent to allow us to process 'special category' data (e.g., to obtain an Occupational Health report). If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

Where we rely solely on consent as the lawful basis for processing, consent may be withdrawn at any time.

9.Change of Purpose

We will only use your personal information for the purposes for which it was collected unless we reasonably consider that we need to use it for another reason, and that reason is compatible with the original purpose.

If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so, or seek your consent if necessary, before the processing commences.

10.Storage and Retention of Personal Data

A significant amount of personal data is stored electronically. Some information may also be stored as hard copy.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including to satisfy any legal, accounting, insurance or reporting requirements.

Details of retention periods for different aspects of your personal information are available in our ***Data Retention Schedule.***

When your time as an employee with the Trust comes to an end, we will retain and securely destroy your personal information following our Data Retention Schedule.

11.CCTV

CCTV is used at some of our sites. The purpose of the system is to prevent crime and promote security and public safety.

If in the event of viewing CCTV for a specified purpose, disciplinary action is observed, the CCTV can and may be used to support a disciplinary investigation.

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

Images are retained for a maximum of 30 days. After this period images will be permanently deleted unless they are required and retained for an ongoing investigation, for example, if an incident or crime has been recorded. In such cases, the images will be retained until the conclusion of any actions or criminal proceedings arising from the incident.

Any enquiries about the CCTV system should be directed to office@thesycamoretrust.co.uk

12.Sharing Personal Data

We do not share workforce data with anyone without consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law), we routinely share workforce data with:

- The Local Authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

- The Department for Education - to fulfil our statutory reporting requirements. We are required to share information about our workforce with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls that meet the current government security policy framework. For more information, please see 'How Government uses your data' section, below.

We may occasionally also share workforce data with:

- Governors
- Disclosure & Barring Service
- Our regulators e.g., Ofsted
- Police forces or other law enforcement agencies, courts, tribunals
- Trade unions and associations
- Your family or representatives
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Professional bodies

Third-party service providers

Limited personal data is shared with third-party service providers who require access to the data to deliver contracted service. These service providers include: -

- Payroll
- Legal advisors
- Insurance providers
- IT providers
- Occupational Health provider
- Wellbeing Service provider
- Any other third-party service provider we will inform you of from time to time

These third-party service providers act as data processors on the Trust's behalf and are required to take appropriate security measures to protect your personal information in line with our policies and data protection legislation.

We authorise these service providers to use personal data only as necessary to perform services on our behalf, or to comply with legal obligations if necessary.

13. Transferring Data Outside The UK

We do not routinely share data with organisations outside the UK. Where this may be necessary, we may transfer data with your explicit consent and with appropriate safeguards.

We will not transfer personal data outside the UK unless such transfer complies with the UK GDPR. This means that we cannot transfer any personal data outside the UK unless:

- The Secretary of State has decided that another country or international organisation ensures an adequate level of protection for personal data
- One of the derogations in the UK GDPR applies (including if an individual explicitly consents to the proposed transfer).

14. Data Security

We have put in place appropriate organisational and technological security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

In addition, we limit access to your personal information to those employees, consultants, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

15. Your Data Subject Rights

You have the right to:

- Make a Subject Access Request (SAR) (see below)
- Withdraw your consent to processing based solely on consent, at any time.
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it (in certain circumstances)
- Prevent use of your personal data for direct marketing
- Challenge processing which has been justified based on public interest.
- Request a copy of agreements under which your personal data is transferred outside of the UK.
- Trust does not use automated decision-making and/or profiling in any of its processes and procedures.
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

For more information about your data subject rights please see here.

Your Duty to Inform us of Changes.
The personal information we hold about you must be accurate and current. Please keep us informed if your personal information changes during your time with us.

Subject Access Requests
Under data protection legislation, individuals have the right to request access to their personal data held by the Trust. Subject Access Requests ***may be*** made in writing or verbally.

If you would like to make a SAR concerning your personal data it would be helpful if this could be made in writing to the Trust, including:

- name and contact address
- email address and telephone number
- details of the information required.

Fulfilling A Subject Access Request
The lawful time scale for the Trust to respond to a Subject Access Request is one calendar month from receipt of a '**valid**' SAR.
A SAR is only considered '***valid*** when we are fully satisfied regarding the identity of the requester and their entitlement to the data requested. If in any doubt we will request confirmation of identity to ensure your personal data is not inadvertently released to a third party who is not entitled to it.

The Trust has limited administrative resources outside of term time, we encourage employees to submit Subject Access Requests during term time and to avoid sending a SAR just before or during term breaks. This will assist us in responding to your request as promptly as possible.

If the SAR is complex or numerous, the period in which we must respond may be extended by a further two months. You will be notified of any delays in actioning the SAR and provided with a timeframe in which you can expect to receive the requested data.

Fees
You will ***not*** have to pay a fee to access your personal information (or to exercise any of your other data subject rights). However, we may charge a reasonable fee if your access request is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Exercising Other Data Subject Rights
If you wish to review, verify, correct, or request the erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Trust the first instance (details below).

The Right to Withdraw Consent
Where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, and there is no other applicable lawful basis for processing the data, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Trust directly.

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another lawful basis for doing so.

16.Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading, or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. We will acknowledge your concern within 30 days and will respond without undue delay.

If you have any concerns that we are not able to resolve to your satisfaction, you can contact our Data Protection Officer at the address below.

Alternatively, you can register your concern with the UK's data protection regulator - the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/make-a-complaint/your-personal-information-concerns/
- Call 0303 123 1113
- Or write to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

17.Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:

Data Protection Officer: Shard Business Services
Email: DPO@shardbusinessservices.co.uk

Data Controller: The Sycamore CE Trust
Email: office@thesycamoretrust.co.uk
Phone: 0161 723 1078 (option 3)
Address: C/o Christ Church CofE Primary School
Church Street, Walshaw, Bury, BL8 3AX

Data Controllers Representative: Ian Young – Trust Lead
Email: office@thesycamoretrust.co.uk

18.Changes to this Privacy Notice

This Notice will be reviewed annually or as necessary in response to changes in Data Protection legislation or our processing activities

We reserve the right to update this Privacy Notice at any time, and we will provide you with a new Privacy Notice when we make any substantial updates.

We may also notify you in other ways from time to time about the processing of your personal information.

Effective Date:	May 2018
Last update:	January 2026
Review Date:	January 2027

How the Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce.
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy.

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice, or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data?
- the purpose for which it is required.
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data, they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below: https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: https://www.gov.uk/contact-dfe