St Faith's Church of England Infant and Nursery School

West Parade, Lincoln, LN1 1QS

Data Protection Policy

Data Controller
St Faith's CofE Infant and Nursery School
Data Protection Officer
Mr Darrel Towndrow
Email: dpo@infotechdirect.co.uk

Policy information
Version: 2.0
Date adopted: January 2026
Next review: January 2027
ICO registration: [ZA/B XXXXXXX]
Approved by: Board of Governors
Policy owner: Data Protection Officer

Contents

1. Introduction and Purpose

St Faith's Church of England Infant and Nursery School collects, uses, stores, shares and disposes of personal data about pupils, parents and carers, staff, governors, and others who come into contact with the school. This data is processed to enable the school to provide education and carry out its statutory functions.

This policy sets out how the school will handle personal data lawfully, fairly and transparently, in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Privacy and Electronic Communications Regulations 2003 (PECR)
- Education (Pupil Information) (England) Regulations 2005
- Children Act 1989 and Children and Families Act 2014
- Keeping Children Safe in Education (current statutory guidance)

This policy applies to all personal data processed by the school, regardless of format — electronic or paper. All staff, governors, contractors and volunteers who process personal data on behalf of the school are required to read, understand and comply with it.

2. Key Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable living individual.
Special category data	Sensitive personal data including racial/ethnic origin, health, religion, biometrics, sexual orientation, political opinions, trade union membership. Attracts heightened protection under Article 9 UK GDPR.
Criminal convictions data	Data relating to alleged offences, proceedings, or sentencing. Processed only under Schedule 1 DPA 2018 conditions.
Processing	Any operation on personal data — collection, use, storage, disclosure, destruction.
Data controller	The school — determines the purposes and means of processing personal data.
Data processor	A third party that processes data on behalf of the school under a written Data Processing Agreement.
Data subject	The living individual to whom the personal data relates.
DPO	Data Protection Officer — responsible for overseeing data protection compliance.
ICO	Information Commissioner's Office — the UK independent data protection supervisory authority.
DPIA	Data Protection Impact Assessment — a structured assessment of high-risk processing activities.

3. Data Protection Principles

The school is committed to ensuring that all personal data is processed in accordance with the six data protection principles set out in Article 5 of the UK GDPR. All staff share responsibility for adherence to these principles.

Principle	Requirement
1. Lawfulness, fairness and transparency	Data is processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. Purpose limitation	Data is collected for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes.
3. Data minimisation	Data collected is adequate, relevant and limited to what is necessary for the purpose.
4. Accuracy	Data is accurate and, where necessary, kept up to date. Inaccurate data is erased or rectified without delay.
5. Storage limitation	Data is retained in identifiable form no longer than is necessary for the purpose.
6. Integrity and confidentiality	Data is processed with appropriate security, protecting against unauthorised access, loss, destruction or damage.

Accountability: The school is responsible for, and must be able to demonstrate, compliance with all six principles. This 'accountability' obligation underpins the policy framework as a whole.

4. Lawful Basis for Processing

The school only processes personal data where it has a lawful basis to do so under Article 6 UK GDPR. The basis relied upon for each category of processing activity is documented in the school's Article 30 Record of Processing Activities, maintained by the DPO. The most common bases used are:

Processing activity	Lawful basis
Pupil admissions and registration	Legal obligation (Education Act 1996; School Admissions Code)
Supporting learning, progress and reporting	Public task (statutory education function)
Pastoral care and pupil welfare	Public task; vital interests where safety is at risk
Safeguarding and child protection	Legal obligation (Children Act 1989; KCSIE)
Special educational needs provision	Legal obligation (Children and Families Act 2014); public task
Medical and health data	Vital interests; substantial public interest (DPA 2018 Sch. 1)

Processing activity	Lawful basis
School Census and statutory DfE returns	Legal obligation (Education (Pupil Information) Regulations 2005)
Attendance monitoring	Legal obligation (Education Act 1996)
Exclusions	Legal obligation (Education Act 2002)
Staff employment and HR	Legal obligation; contract of employment
Financial administration	Legal obligation; contract; legitimate interests
CCTV (if applicable)	Legitimate interests (security and safety)
Photographs — school publications and website	Legitimate interests; or consent where required
Equality monitoring	Legal obligation (Equality Act 2010); substantial public interest
Class card lists (first names only)	Consent

4.1 Special category data

In addition to a lawful basis under Article 6 UK GDPR, processing special category data also requires a specific condition under Article 9 UK GDPR. The school relies on the following conditions, as set out in Schedule 1 of the Data Protection Act 2018:

- Substantial public interest — safeguarding of children and vulnerable individuals; equality of opportunity monitoring
- Employment and social security law obligations
- Health and social care purposes
- Vital interests — where necessary to protect life

The DPO is responsible for ensuring that the appropriate Schedule 1 condition is identified and documented before any special category data is processed.

4.2 Consent

Where the school relies on consent as its lawful basis, the following requirements apply:

- Consent must be freely given, specific, informed and unambiguous
- The school will make clear at the point of collection what the data will be used for and how consent can be withdrawn
- Consent may be withdrawn at any time without detriment. Withdrawal does not affect the lawfulness of processing carried out prior to withdrawal
- The school will not rely on consent for processing that is required to fulfil its statutory functions — in those cases, a more appropriate basis applies

Records of consent and withdrawal are maintained by the school office.

5. Data Protection Officer (DPO)

The school has appointed a Data Protection Officer as required by Article 37 UK GDPR, given its large-scale processing of special category data relating to children.

DPO Contact Details
Name: Darrel Towndrow
Email: enquiries@st-faiths.lincs.sch.uk

The DPO is responsible for:

- Monitoring compliance with UK GDPR, the DPA 2018 and this policy
- Providing advice on Data Protection Impact Assessments (DPIAs)
- Acting as the primary contact point for the ICO and for data subjects exercising their rights
- Providing data protection training and guidance to staff
- Maintaining the Article 30 Record of Processing Activities
- Maintaining the Data Breach Register

The DPO operates independently and must not receive instructions regarding the exercise of their data protection tasks. The DPO's identity and contact details are published on the school's website and are available from the school office.

6. Privacy Notices

The school fulfils its transparency obligations under Articles 13 and 14 UK GDPR by issuing privacy notices to data subjects at or before the point at which their personal data is collected.

The school maintains the following privacy notices:

- Privacy Notice for Parents, Carers and Pupils — published on the school website and issued to parents on admission
- Staff Privacy Notice — provided to all employees at the point of recruitment
- Governor Privacy Notice — provided on appointment

Each privacy notice includes, as a minimum:

- The identity and contact details of the data controller and DPO
- The categories of personal data collected and the purposes for which it is used
- The lawful basis for each processing activity, including the specific Schedule 1 condition where special category data is processed
- Recipients and categories of recipients with whom data is shared
- Retention periods or the criteria used to determine them
- Details of any international data transfers and the safeguards in place
- A full description of data subjects' rights
- The right to withdraw consent and how this can be done
- The right to lodge a complaint with the ICO

Privacy notices are reviewed annually by the DPO and updated to reflect any changes to the school's processing activities or applicable guidance.

7. Record of Processing Activities (Article 30 Register)

The school maintains a Record of Processing Activities (ROPA) in accordance with Article 30 UK GDPR. This register documents all personal data processing activities carried out by the school as Data Controller. It contains:

- The name and details of the school and, where applicable, the DPO
- The purposes of each processing activity
- Categories of data subjects and personal data
- Categories of recipients, including data processors
- Details of any transfers to third countries and the safeguards in place
- Retention periods
- A description of technical and organisational security measures

The ROPA is maintained by the DPO, reviewed annually, and made available to the ICO on request. Any significant new processing activity must be added to the ROPA before it commences.

8. Data Protection Impact Assessments (DPIAs)

The school will carry out a Data Protection Impact Assessment before commencing any processing that is likely to result in a high risk to the rights and freedoms of individuals, in accordance with Article 35 UK GDPR.

8.1 When a DPIA is required

A DPIA is required where processing is likely to result in high risk, including — but not limited to — the following scenarios:

- Introduction of new technologies (e.g. AI-based learning platforms, biometric systems, learning analytics)
- Systematic monitoring of individuals (e.g. expanded CCTV, staff activity monitoring)
- Large-scale processing of special category data
- Processing that involves profiling or automated decision-making with significant effects
- Processing that involves children's data in new ways
- Significant changes to existing systems or new third-party data sharing arrangements

8.2 DPIA process

Where a DPIA is required, the following process will be followed:

- The DPO must be consulted before the DPIA commences, as required by Article 35(2) UK GDPR
- The DPIA will describe the processing, assess necessity and proportionality, and identify and evaluate risks
- Where risks cannot be adequately mitigated, the ICO must be consulted before processing begins (Article 36 UK GDPR)
- Completed DPIAs are retained by the DPO and reviewed if processing activities change

No new processing activity that meets the threshold for a DPIA may commence without a completed and approved DPIA on record.

9. Data Sharing

The school does not share personal data with any third party without a lawful basis to do so. Where sharing is required or permitted, the school will share only the minimum data necessary.

9.1 Data processors

Where the school engages third parties to process personal data on its behalf, it will:

- Carry out due diligence on the processor's data protection practices before engagement
- Ensure a written Data Processing Agreement (DPA) is in place that complies with Article 28 UK GDPR
- Include data protection requirements in all relevant contracts
- Review processor compliance periodically

Data Processing Agreements are maintained by the DPO. No new processor may be engaged without a DPA in place.

9.2 Sharing with third-party controllers

The school may share data with the following categories of third-party controller where there is a lawful basis to do so:

- Lincolnshire County Council — safeguarding, SEN, statutory returns
- Department for Education — School Census, statutory data collections, National Pupil Database
- Ofsted and other regulators — inspection functions
- NHS and health authorities — pupil health and medical needs
- Police, courts and tribunals — safeguarding and legal proceedings
- Social care and health and welfare organisations — safeguarding and welfare
- Receiving schools on pupil transfer — educational continuity
- Examination bodies — national assessments
- Professional advisers and legal counsel — advice and representation

9.3 International data transfers

Where the school transfers personal data to a country or territory outside the United Kingdom, it will do so only in accordance with UK data protection law. Transfers will be made only where:

- The destination country benefits from a UK adequacy decision; or
- Appropriate safeguards are in place, such as the International Data Transfer Agreement (IDTA) or UK standard contractual clauses; or
- A specific exemption under the DPA 2018 applies

The DPO is responsible for assessing and documenting any international transfers in the ROPA.

10. Retention and Disposal of Personal Data

The school retains personal data only for as long as is necessary for the purpose for which it was collected, or as required by law. Retention periods are set out in the school's Data Retention Schedule, maintained by the DPO and based on the Records Management Code of Practice for Schools and current DfE guidance.

Category of data	Retention period
Pupil educational records (general)	Until the pupil's 25th birthday
Safeguarding and child protection records	Until the pupil's 25th birthday as a minimum; some records indefinitely
Special educational needs (EHCP / statements)	Until the pupil's 35th birthday
Accident and injury records	Until the pupil's 21st birthday
Admissions records (unsuccessful)	1 year after the admissions round
Financial and accounting records	7 years after the financial year end
Staff personnel files	7 years after employment ends
Payroll and pension records	7 years after the employee leaves
DBS check records	6 months after the recruitment decision
CCTV footage (if applicable)	31 days unless retained for incident investigation

When data is no longer required, it is securely deleted or physically destroyed in accordance with the school's Secure Disposal Procedure. Paper records containing personal data are shredded using a cross-cut shredder; electronic records are permanently deleted or overwritten. A record of disposal is maintained.

11. Security of Personal Data

The school implements appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, or unauthorised access or disclosure, in accordance with Article 32 UK GDPR.

11.1 Technical measures

- Password protection and multi-factor authentication (MFA) on all school systems
- Role-based access controls — staff may only access data necessary for their role
- Encryption of all portable electronic devices and storage media containing personal data
- Secure, managed cloud storage with Data Processing Agreements in place
- Regular software updates and security patching
- Network security controls including firewall, filtering and monitoring

11.2 Organisational measures

- Annual data protection training for all staff, with records maintained
- Acceptable use policy for all school IT equipment and systems
- Clear desk and screen lock policy
- Confidentiality requirements included in all employment contracts and volunteer agreements
- Secure physical storage (locked filing cabinets) for paper records containing personal data
- Visitor sign-in procedures; visitors are accompanied at all times
- Personal data is not to be left unattended in vehicles
- Staff working remotely must ensure personal data is appropriately secured

11.3 Cloud-based services

Before adopting any cloud-based service that will process personal data, the school will carry out due diligence on the provider's data protection and security practices, ensure a Data Processing Agreement is in place, and consider whether a DPIA is required. The DPO must be consulted before any new cloud service is procured.

12. Individual Rights

Under UK GDPR, individuals have the following rights in relation to their personal data. All rights requests should be directed to the DPO. The school will respond within one calendar month, extendable by a further two months for complex requests (with notice given to the individual).

Right	Summary
Right of access (Subject Access Request)	Request a copy of personal data held. Responded to within one calendar month, free of charge for standard requests.
Right to rectification	Request correction of inaccurate or incomplete data.
Right to erasure	Request deletion of personal data where no lawful basis for retention exists. Does not apply to data retained under a legal obligation.
Right to restrict processing	Request limitation of processing while a dispute is resolved.
Right to data portability	Where processing is based on consent or contract, receive data in a portable, machine-readable format.
Right to object	Object to processing based on legitimate interests or public task, on grounds relating to the individual's particular situation.
Right not to be subject to automated decision-making	Not to be subject to decisions made solely by automated means that have significant legal or similar effects.
Right to withdraw consent	Withdraw consent at any time without detriment. Does not affect processing already carried out.

12.1 Subject Access Requests (SARs)

Requests for access to personal data must be made in writing (including by email) to the headteacher. The school will verify the identity of the requestor and, where the request relates to a child's data, will verify parental responsibility before disclosure is made.

There are two distinct rights of access to pupil data:

- A subject access request under Article 15 UK GDPR for access to personal data generally
- A request for access to the educational record under the Education (Pupil Information) (England) Regulations 2005 — to which a response is required within 15 school days

The school will redact any information relating to third parties where it is not possible to separate this from the requested information. Information may be withheld where disclosure would cause serious harm to the physical or mental health of the pupil or another person, or where it would reveal that a child is at risk of abuse.

13. Photographs and Electronic Images

The use of photographs and video recordings of pupils is addressed in the school's Online Safety Policy, which sets out the school's position on the use of images in school publications, the website, and by external organisations. Parental consent forms for photography are obtained on admission and reviewed annually.

For the purposes of data protection, photographs and video recordings of identified pupils constitute personal data. The school's lawful basis for using pupil images will depend on the context:

- Images used in school publications and internal communications — legitimate interests
- Images shared with external media or third-party organisations — consent

Parental consent to the use of images may be withdrawn at any time by contacting the school office in writing.

14. Biometric Data

The school does not currently use biometric data. If the school introduces or intends to introduce any biometric system (such as fingerprint or facial recognition technology), the following requirements will apply in accordance with the Protection of Freedoms Act 2012 and UK GDPR:

- The school will notify parents and pupils in advance, explaining the intended purpose and lawful basis for processing
- Written consent of at least one parent or carer with Parental Responsibility must be obtained before any biometric data is taken from a pupil
- A pupil may refuse to have their biometric data taken, regardless of parental consent
- The school must provide an alternative system for pupils who do not provide biometric data
- A DPIA must be completed before any biometric system is introduced
- The local authority must be notified as required

15. Staff Training and Awareness

All staff receive data protection training as part of their induction and at least annually thereafter. Training covers:

- The school's obligations under UK GDPR and this policy
- Staff responsibilities regarding the security and confidentiality of personal data
- How to recognise and report a personal data breach
- The handling of Subject Access Requests
- The appropriate use of school IT systems and devices

Training records are maintained by the school office and reviewed by the DPO. Additional role-specific guidance is provided to staff with access to sensitive data, including the SENCO, Designated Safeguarding Lead, and finance and HR staff.

Governors receive data protection awareness briefings in line with their governance responsibilities, at least annually.

16. Complaints

Complaints about how the school has handled personal data, or about the exercise of information rights, are dealt with under the school's Data Protection Complaints Procedure. This is a separate procedure from the school's General Complaints Procedure, which does not apply to complaints relating to data protection or information rights.

Complaints should be made by email to the Data Protection Officer at dpo@st-faiths.lincs.sch.uk.

The Data Protection Complaints Procedure, published on the school website, sets out how complaints are received, acknowledged and investigated, the timescales that apply, and the school's approach to complaints made on behalf of a child or by a third party.

Where a complaint is not resolved to the individual's satisfaction, or where the school's Data Protection Complaints Procedure has been exhausted, the individual has the right to lodge a complaint with the Information Commissioner's Office:

Information Commissioner's Office — Contact Details
Website: ico.org.uk/make-a-complaint
Telephone: 0303 123 1113
Post: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

17. Policy Review

This policy will be reviewed at least annually by the DPO and approved by the governing body. It will also be reviewed following any significant changes to legislation, ICO guidance, or the school's data processing activities.

Policy detail	
Policy owner	Data Protection Officer
Review frequency	Annual (or earlier if required)
Next review date	January 2027
Approval authority	Board of Governors

Approved by:

Role	Signature and date
Chair of Governors: Dr Emile Van Der Zee	
Headteacher: Mrs Amanda Konrath	
Data Protection Officer: Mr Darrel Towndrow	

Appendix A — Legislation and Guidance Reference

Instrument	Relevance
UK General Data Protection Regulation (UK GDPR)	Primary data protection framework post-Brexit
Data Protection Act 2018 (DPA 2018)	Supplements UK GDPR; Schedule 1 conditions for special category data
Privacy and Electronic Communications Regulations 2003 (PECR)	Electronic marketing and cookies
Education (Pupil Information) (England) Regulations 2005	Pupil records and educational record access rights
Children Act 1989	Safeguarding and welfare duties
Children and Families Act 2014	SEN and disability provisions
Equality Act 2010	Equality monitoring obligations
Protection of Freedoms Act 2012	Biometric data in schools
Freedom of Information Act 2000	Public authority information access obligations
Keeping Children Safe in Education (current)	Statutory safeguarding guidance
Records Management Code of Practice for Schools (ICO)	Retention schedule guidance
ICO Guidance for Education	ico.org.uk/for-organisations/education/

Appendix B — Key Contacts

Contact	Details
Data Protection Officer	Mr Darrel Towndrow
Headteacher	Mrs Amanda Konrath — 01522 888988
Chair of Governors	Dr Emile Van Der Zee — via School Office
Information Commissioner's Office	0303 123 1113 | ico.org.uk
NCSC (cyber incidents)	ncsc.gov.uk/section/about-ncsc/report-cyber-incident
Action Fraud (cybercrime)	actionfraud.police.uk | 0300 123 2040
Lincolnshire Safeguarding Children Partnership	[LSCP contact details]

Appendix C: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

1. Reporting a breach

On becoming aware of a personal data breach, or potential breach:

- The staff member or data processor must immediately notify the Headteacher (or a member of the Senior Leadership Team)
- The Data Protection Officer (DPO) must also be informed as soon as possible

2. Initial assessment and containment

The Headteacher (or delegated member of SLT) will:

- Take immediate steps to contain and minimise the impact of the breach, working with IT support or relevant staff as appropriate
- Establish the initial facts, including:
    - What has happened
    - What data is involved
    - Who may be affected

Examples of containment actions may include:

- Securing or disabling user accounts
- Recalling emails
- Recovering or remotely wiping devices
- Removing data from public access
- Restricting access to systems or files

3. Investigation

The school, as **Data Controller**, is responsible for investigating the breach.

This will typically involve:

- The Headteacher or SLT
- IT support (where relevant)
- Advice and support from the DPO

The investigation will determine whether personal data has been:

- Lost
- Stolen

- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Accessed by unauthorised individuals

4. Risk assessment

The school, with advice from the DPO, will assess:

- The **likelihood and severity of risk** to individuals
- Whether the breach could result in harm, including:
    - Loss of control over personal data
    - Identity theft or fraud
    - Financial loss
    - Damage to reputation
    - Loss of confidentiality
    - Safeguarding risks
    - Any other significant economic or social disadvantage

5. Notification to the ICO

The **Headteacher (on behalf of the Data Controller)** is responsible for determining whether the breach must be reported to the ICO.

The DPO will:

- Provide advice on whether the breach is reportable
- Support the preparation and submission of the report

Where required, the breach will be reported via the ICO reporting process **within 72 hours** of the school becoming aware of it.

The report will include, where possible:

- A description of the nature of the breach
- The categories and approximate number of individuals affected
- The categories and approximate number of personal data records affected
- The name and contact details of the DPO
- The likely consequences of the breach
- The measures taken or proposed to address the breach and mitigate its effects

Where full details are not yet known, an initial report will be submitted within 72 hours, with further information provided as soon as possible.

6. Notification to individuals

Where the breach is likely to result in a **high risk to individuals**, the school will notify affected individuals without undue delay.

This notification will include:

- A description of the breach
- The likely consequences
- The measures taken or proposed
- Contact details for further information (including the DPO)

7. Recording the breach

All personal data breaches, whether reportable or not, will be recorded by the school.

For each breach, the record will include:

- The facts and cause of the breach
- Its effects
- The action taken to contain it
- Any actions taken to prevent recurrence

Records will be retained securely in line with the school's data protection procedures.

The DPO will support and review breach records as part of their monitoring role.

8. Review and lessons learned

Following a breach:

- The Headteacher and relevant staff will review the incident
- Appropriate actions will be identified to prevent recurrence

This may include:

- Changes to processes or procedures
- Additional staff training
- Implementation of technical controls

The DPO will provide advice and may make recommendations as part of this review.

9. Actions to minimise the impact of specific breaches

The school will take appropriate steps to mitigate the impact of different types of data breach, particularly those involving sensitive personal data.

These examples are not exhaustive and will be considered on a case-by-case basis.

Sensitive information disclosed via email (including safeguarding records)

- The sender must attempt to recall the email immediately
- The incident must be reported to the Headteacher/SLT and DPO
- IT support will assist with recall or containment where possible
- The school will contact recipients and request deletion and confirmation
- Further steps will be taken if information has been publicly disclosed

Data published in error (e.g. on the school website)

- The data will be removed immediately
- The incident will be reported and assessed in line with this procedure

Confidential information shared inappropriately (e.g. exam results or staff data)

- Hard copies will be recalled and securely destroyed
- Access to electronic data will be restricted where possible
- The incident will be reported and assessed

Loss or theft of a device containing personal data

- The incident must be reported immediately
- IT support will take steps such as account disabling or remote wiping where possible
- The breach will be assessed in line with this procedure

Third-party data breach (e.g. supplier compromise)

- The supplier will be contacted immediately
- The school will assess the impact on its data
- The breach will be managed in line with this procedure

These examples are not exhaustive. Each incident will be assessed on its own merits by the school, with advice from the DPO.

This policy supersedes all previous versions of the school's Data Protection Policy. It is based on current UK GDPR and Data Protection Act 2018 requirements as in force at the date of adoption.