

## Document Control

<b>Policy Owner:</b>	Inclusive Church Network Board of Trustees
<b>Approved by:</b>	Board of Trustees
<b>Date Approved:</b>	23/02/26
<b>Review Date:</b>	February 2027
<b>Version:</b>	1.0
<b>Data Protection Officer:</b>	Chantal Noppen, National Co-ordinator
<b>Data Protection Trustee:</b>	Yin-An Chen

## 1. Introduction

This Data Protection Policy sets out how Inclusive Church Network ("we", "us", "our") collects, uses, stores, and protects personal data in compliance with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

The Inclusive Church Network is committed to protecting the privacy and security of personal data. This policy applies to all personal data we process, whether it relates to members, volunteers, staff, donors, service users, or website visitors.

## 2. Scope

This policy applies to:

- All trustees, staff, volunteers, and contractors of Inclusive Church Network
- All personal data processed by or on behalf of Inclusive Church Network
- All data processing activities, whether manual or automated

## 3. Key Definitions

**Personal Data:** Any information relating to an identified or identifiable living individual.

**Special Category Data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation.

**Data Subject:** The individual to whom personal data relates.

**Data Controller:** The organisation that determines the purposes and means of processing personal data. Inclusive Church Network is the data controller for the personal data it processes.

**Data Processor:** Any organisation that processes personal data on behalf of the data controller.

**Data Protection Officer (DPO):** The person responsible for overseeing data protection compliance and acting as the point of contact for data subjects and supervisory authorities.

## 4. Data Protection Principles

We adhere to the six data protection principles set out in the UK GDPR. Personal data must be:

1. **Processed lawfully, fairly and transparently** – We only collect and use personal data where we have a lawful basis and we are transparent about our data processing activities.
2. **Collected for specified, explicit and legitimate purposes** – We only collect personal data for specific purposes and we do not use it in ways that are incompatible with those purposes.
3. **Adequate, relevant and limited to what is necessary** – We only collect the minimum amount of personal data needed for our purposes.
4. **Accurate and kept up to date** – We take reasonable steps to ensure personal data is accurate and we correct or delete inaccurate data without delay.
5. **Kept for no longer than necessary** – We delete or anonymise personal data when it is no longer needed, in accordance with our Data Retention Schedule (see Section 12).
6. **Processed securely** – We implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.

## 5. Lawful Basis for Processing

We process personal data only where we have a lawful basis. The lawful bases we rely on are:

### 5.1 Consent

We obtain explicit consent from individuals for:

- Marketing communications and newsletters
- Processing special category data (religious beliefs, sexual orientation) for service delivery



- Research and archiving purposes

### 5.2 Contract

We process personal data where necessary to enter into or perform a contract, including:

- Employment contracts with staff and volunteers
- Service agreements with members and participants

### 5.3 Legal Obligation

We process personal data where required by law, including:

- Employment law requirements (right to work, tax, pensions)
- Financial record-keeping and Gift Aid claims
- Safeguarding and child protection obligations

### 5.4 Legitimate Interests

We may rely on legitimate interests where appropriate, having balanced our interests against the rights and interests of individuals. This may include:

- Maintaining records of our activities and history
- Direct debits and payment processing
- Network security and fraud prevention

## 6. Special Category Data

Given our mission and values, we process special category data including information about:

- Religious or philosophical beliefs
- Sexual orientation
- Racial or ethnic origin (for diversity monitoring)
- Health information (for reasonable adjustments and safeguarding)

We only process special category data where we have both:

7. A lawful basis under Article 6 UK GDPR (as described in Section 5), and
8. An additional condition under Article 9 UK GDPR, including:
  - Explicit consent from the data subject
  - Processing necessary for reasons of substantial public interest (equality of opportunity monitoring)
  - Processing necessary for the purposes of carrying out our legitimate activities as a not-for-profit body with a religious aim

## **7. Data Subjects' Rights**

Individuals have the following rights under data protection law:

### **7.1 Right of Access**

Individuals can request copies of their personal data and information about how we process it. We will respond within one month.

### **7.2 Right to Rectification**

Individuals can request correction of inaccurate or incomplete personal data.

### **7.3 Right to Erasure ('Right to be Forgotten')**

Individuals can request deletion of their personal data in certain circumstances, though this right is not absolute and may be limited by other legal obligations.

### **7.4 Right to Restriction of Processing**

Individuals can request that we limit how we use their personal data in certain circumstances.

### **7.5 Right to Object**

Individuals can object to processing based on legitimate interests or for direct marketing purposes.

### **7.6 Right to Data Portability**

Individuals can request their personal data in a structured, commonly used, machine-readable format where processing is based on consent or contract.

### **7.7 Right to Withdraw Consent**

Where processing is based on consent, individuals can withdraw consent at any time.

### **7.8 Handling Rights Requests**

All requests to exercise data subject rights should be directed to the Data Protection Officer at [office@inclusive-church.org](mailto:office@inclusive-church.org). We will respond within one month (extendable by two further months for complex requests).



## 8. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected or to comply with legal, regulatory, or contractual requirements. Our Data Retention Schedule is set out in Section 12 of this policy.

## 9. Data Security

We implement appropriate technical and organisational measures to protect personal data, including:

- Access controls - limiting access to personal data on a need-to-know basis
- Encryption of sensitive data in transit and at rest
- Secure password policies and multi-factor authentication where available
- Regular software updates and security patches
- Secure disposal of physical records through shredding
- Secure deletion of electronic data
- Regular backups with appropriate security measures
- Staff training on data protection and security

## 10. Data Breach Management

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

### 10.1 Breach Response Procedure

9. **Containment:** Immediate steps to contain the breach and limit damage
10. **Assessment:** Evaluate the severity and impact of the breach
11. **Notification:** Report to the ICO within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms
12. **Communication:** Notify affected individuals without undue delay if there is a high risk to their rights and freedoms
13. **Documentation:** Record all data breaches, whether reportable or not
14. **Review:** Investigate root causes and implement preventative measures

Any suspected data breach must be reported immediately to the Data Protection Officer at [office@inclusive-church.org](mailto:office@inclusive-church.org).

## 11. Data Sharing and Third Parties



We may share personal data with third parties only where necessary and with appropriate safeguards. This includes:

### 11.1 Service Providers (Data Processors)

We use third-party service providers for functions such as:

- Email and communications platforms
- Website hosting and maintenance
- Payment processing
- Cloud storage and backup services

All data processors are required to sign written contracts (Data Processing Agreements) that include appropriate security measures and obligations under UK GDPR.

### 11.2 Legal and Regulatory Authorities

We may share personal data with:

- HMRC for tax and Gift Aid purposes
- The Charity Commission
- Law enforcement agencies where required by law
- Safeguarding authorities where there is a risk of harm

### 11.3 International Transfers

Where personal data is transferred outside the UK, we ensure appropriate safeguards are in place, such as Standard Contractual Clauses or adequacy decisions by the UK government.

## 12. Data Retention Schedule

The following Data Retention Schedule sets out how long we retain different categories of personal data. Retention periods are based on legal requirements, best practice guidance, and operational needs.

At the end of each retention period, data will be securely deleted or anonymised unless there is a legal requirement to retain it or the individual has consented to longer retention.

Data Category	Retention Period	Reason for Retention	Action
---------------	------------------	----------------------	--------



Staff/Volunteer Recruitment Records (Unsuccessful Applicants)	6 months from end of recruitment	Equality Act 2010 compliance	<b>Delete</b>
Staff/Volunteer Recruitment Records (Successful Appointees)	Duration of engagement + 6 years	Legal claims limitation period	<b>Delete</b>
Employment Contracts and Terms	Duration of employment + 6 years	Legal claims limitation period	<b>Delete</b>
Payroll and Tax Records	Current year + 6 years	HMRC requirements	<b>Delete</b>
Pension Records	Duration of employment + 6 years	Legal and regulatory compliance	<b>Delete</b>
DBS Checks and Safeguarding Records	6 months after check completed (certificate reference only retained)	DBS Code of Practice	<b>Delete</b>
Disciplinary and Grievance Records	Duration of employment + 6 years	Legal claims limitation period	<b>Delete</b>
Accident and Incident Reports	Date of incident + 6 years (12 years if involves a child)	Legal claims limitation period	<b>Delete</b>
Training Records	Duration of employment + 6 years	Evidence of competence and compliance	<b>Delete</b>
Membership Records (Active Members)	Duration of membership + 2 years	Operational need and relationship management	<b>Delete</b>
Membership Records (Lapsed Members)	2 years from lapse	Re-engagement opportunity	<b>Delete</b>
Event Registration and Attendance	Date of event + 2 years	Historical records and future planning	<b>Delete</b>

Consent Records	Duration of consent + 2 years	Evidence of lawful processing	<b>Delete</b>
Safeguarding Records	Indefinitely (or as advised by safeguarding authorities)	Child/adult protection obligations	<b>Review</b>
Donation Records	Date of donation + 6 years	HMRC Gift Aid requirements and financial audit	<b>Delete</b>
Gift Aid Declarations	Date of declaration + 6 years	HMRC requirements	<b>Delete</b>
Financial Transaction Records	Current year + 6 years	Legal and regulatory compliance, audit trail	<b>Delete</b>
Invoices and Receipts	Date of transaction + 6 years	Financial compliance and audit	<b>Delete</b>
Marketing Consent Records	Until consent withdrawn + 2 years	Evidence of lawful processing	<b>Delete</b>
Email Correspondence (General)	2 years from date of email	Operational reference	<b>Delete</b>
Email Correspondence (Significant Decisions/Contracts)	6 years from completion	Evidence and legal claims	<b>Delete</b>
Complaints Records	Date of resolution + 6 years	Legal claims limitation period	<b>Delete</b>
Website Analytics Data	26 months (or as configured)	Website improvement and user experience	<b>Auto-delete</b>
Cookie Consent Records	Duration of consent + 1 year	Evidence of compliance	<b>Delete</b>

User Account Data (Active)	Duration of account + 2 years	Service provision	<b>Delete</b>
User Account Data (Inactive >2 years)	2 years from last activity	Operational need	<b>Delete</b>
Trustee Records	Duration of trusteeship + 6 years	Governance and accountability	<b>Delete</b>
Board Meeting Minutes	Indefinitely	Permanent organisational record	<b>Archive</b>
AGM Records	Indefinitely	Legal requirement and organisational history	<b>Archive</b>
Policies and Procedures (Superseded)	Date of replacement + 6 years	Historical reference and compliance evidence	<b>Delete</b>
Research Consent Records	Duration of research project + 6 years	Evidence of ethical compliance	<b>Delete</b>
Anonymised Research Data	Indefinitely (subject to research protocol)	Research value and historical record	<b>Archive</b>
Historical Archives (Significant Events/Documents)	Indefinitely	Organisational heritage and public interest	<b>Archive</b>

## 13. Roles and Responsibilities

### 13.1 Board of Trustees

Ultimate responsibility for data protection compliance and approval of this policy.

### 13.2 Data Protection Trustee



The designated trustee responsible for oversight of data protection matters at Board level. Serious data protection concerns or escalations should be directed to the Data Protection Trustee.

### **13.3 Data Protection Officer (DPO)**

Chantal Noppen, National Co-ordinator, serves as the Data Protection Officer. The DPO is responsible for:

- Monitoring compliance with data protection law and this policy
- Handling data subject access requests and other rights requests
- Providing advice and guidance to staff and volunteers on data protection matters
- Managing data breach incidents and notifications
- Acting as the point of contact with the Information Commissioner's Office (ICO)
- Conducting data protection impact assessments when required
- Maintaining records of processing activities and consent
- Reviewing and updating data protection documentation

Contact: [office@inclusive-church.org](mailto:office@inclusive-church.org)

### **13.4 All Staff and Volunteers**

All staff and volunteers are responsible for:

- Following this policy and associated procedures
- Completing data protection training
- Reporting data breaches or concerns immediately to the DPO
- Only accessing personal data necessary for their role
- Keeping personal data secure and confidential

## **14. Training and Awareness**

All staff, trustees, and volunteers with access to personal data must:

- Complete data protection induction training
- Receive refresher training annually
- Be made aware of their responsibilities under this policy

The Data Protection Officer is responsible for coordinating and delivering training programmes.

## **15. Accountability and Monitoring**



**Inclusive  
Church**

## **DATA PROTECTION POLICY**

We maintain documentation to demonstrate compliance with data protection law, including:

- Records of processing activities
- Data Protection Impact Assessments (DPIAs) for high-risk processing
- Records of consent
- Data breach records
- Data Processing Agreements with third parties

This policy is reviewed annually by the Board of Trustees, with recommendations from the Data Protection Officer.

### **16. Complaints**

Individuals who have concerns about how we handle their personal data should contact the Data Protection Officer at [office@inclusive-church.org](mailto:office@inclusive-church.org).

If the matter cannot be resolved, concerns can be escalated to the Data Protection Trustee via the same contact address.

If concerns remain unresolved, individuals have the right to complain to the Information Commissioner's Office (ICO):

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire SK9 5AF  
Helpline: 0303 123 1113  
Website: <https://www.ico.org.uk/make-a-complaint>

### **17. Policy Review**

This policy will be reviewed annually or sooner if there are changes to:

- Data protection legislation
- Our data processing activities
- Best practice guidance

### **18. Related Documents**



**Inclusive  
Church**

## **DATA PROTECTION POLICY**

This policy should be read in conjunction with:

- Privacy Notice - Public
- Privacy Notice - Staff and Volunteers
- Information Security Policy
- Records Management Policy

---

*End of Data Protection Policy*