CROSSREACH

Care you can put your faith in

DATA PROTECTION

POLICY

Policy Statement

In order to operate and provide care and support for children and vulnerable adults across Scotland, CrossReach is required to collect and use information about the people with whom it works. These data subjects may include members of the public, congregations, current, past and prospective employees, people who use a CrossReach service, volunteers, financial supporters and suppliers.

CrossReach will ensure that personal and special category information is collected, stored, transferred, shared, and processed appropriately and in line with the Data Protection Act 2018, UK General Data Protection Regulations (UKGDPR) and Data Use and Access Act (DUA) 2025, for both manual and electronic data.

Purpose of the Policy

The purpose of this policy is to provide guidance which employees must adhere to when any personal data belonging to or provided by data subjects is collected, stored or transmitted.

It is therefore imperative that all those who should know about this policy comply with the 6 Data Protection Principles. These are detailed in Appendix 1, Glossary of Terms,

Who is Affected by this Policy

All individuals for whom CrossReach collects, stores, transfers and shares personal or special category data. Employees and volunteers who handle data as part of their voluntary role.

Who Should Know About this Policy

All CrossReach employees (including relief workers), volunteers, Social Care Council members and students on placement Agency workers and all such persons for the purposes of the policy are referred to when the term “employees” is used.

Definitions

Please see Appendix 1 – Glossary of Terms

Core Principles

As an organisation, CrossReach will adhere to the core principles detailed below. The specific responsibilities of individuals will vary dependent on role.

1. Fully adhere to the 6 Principles detailed in the Data Protection Act
2. Through privacy notices, specify to Data Subjects the purpose for which information will be used and use the information for that purpose;
3. Ensure that there is a legal basis to collect, process and share personal or special category data and this has been recorded;
4. If the legal basis depends on legitimate interest, identify which particular interest applies. The most relevant are necessary processing that is covered by a privacy statement, the prevention or detection of crime, and the safeguarding of vulnerable individuals.
5. Ensure that all data, particularly personal and special category data, is held securely and is only accessible to those who require it to undertake their role, i.e. is held in locked storage (for paper records) or for electronic records, being held

on a secure server with sufficient additional security measures, authentication for users, and restrictions on access;

6. Only collect and process information to fulfil operational needs or to comply with any legal requirements and in line with permission from the Data Subject. Exemptions may be applied in Child/Adult Protection and safeguarding matters;
7. Take the appropriate steps to ensure that information used is accurate and relevant and up to date. Where it is identified that data is not accurate, steps are taken immediately to rectify this;
8. Will retain information in line with retention schedules and then securely destroy it;
9. Ensure that personal information is not transferred, internally or externally, without suitable safeguards and in line with CrossReach Policy;
10. If relevant data is lost, inappropriately shared or transferred then steps will be taken in line with the CrossReach Breach Management Plan to report the breach and, as far as possible, secure the data;
11. Ensure that information is available to Data Subjects to understand how to make a Subject Access Request;
12. CrossReach will comply with all Subject Access Requests, ensuring the rights of the Data Subject are met. This will involve ensuring that information is not shared until identification has been verified and references to other individuals have been removed. Where appropriate support will be offered to the Data Subject. This must be completed within 30 days unless an exemption applies for complexity or volume of information, in which case a 60-day extension is permitted; the QCI team should be contacted for support.
13. Where a Data Subject requests for their data to be erased, steps will be taken within one month to respond to the Data Subject on whether CrossReach can meet the request or if there is a justifiable legal basis for retaining the data: the QCI team should be contacted for support.
14. Where children are accessing the service directly and personal data is being processed, steps must be taken to verify their date of birth. If online services are likely to be accessed by children directly, any data collection must be done with child protection in mind;
15. Where new systems or processes are being developed in relation to personal or special category data, then privacy by design should be incorporated from the outset. The QCI team should be contacted for support.
16. Where a Data Subject requests for the processing of their personal data to be restricted. CrossReach will immediately, where possible, stop processing the Data Subject's data until an impact assessment is undertaken. This must be concluded within one month.
17. Ensure that if a Data Subject wishes to make a complaint relating to the processing of their data, this is managed in line with the CrossReach Complaints Policy and Procedure.
18. Will not transfer personal data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data or if an exemption applies. This also includes the transfer to cloud storage held outwith the EEA. This includes the use of third-party apps unless they employ specific measures to comply with GDPR requirements, such as storage in an appropriate country. QCI and IT must be contacted prior to any data being transferred outwith the European Economic Area.

Responsibilities

All employees and volunteers of CrossReach and Social Care Council members have responsibilities under the CrossReach Data Protection Policy

CMT – will ensure that this Policy meets legislative requirements and is fit for purpose.
SMT must lead by example and follow the policy in all situations involving personal and special category data. Through routine audits, Heads of Service must ensure that managers are monitoring implementation and compliance.
SMT members are responsible for ensuring that the appropriate training is in place for staff, volunteers and Social Care Council Members on the Data Protection Act and CrossReach Policy and Data Protection Guidance.
SMT members must ensure that any potential or actual breaches of Data Protection are immediately reported to the Business Partner, Quality, Compliance and Improvement who will undertake to report to the Data Protection Compliance Officer.

Business Partner – Quality, Compliance and Improvement – is responsible for ensuring that Retention Schedules are in line with any statutory requirements. They will provide assistance and guidance to Service Managers where a Data Subject makes a complaint, requests access to the data held on them, wishes data held to be removed or requests a restriction to their data being processed. As detailed above they are responsible for notifying the Data Protection Compliance Officer of any potential breaches. They are also responsible of advising the DPCO of any categories of Data not detailed in the ICO registration.

Service/Departmental Managers – are responsible for ensuring that all staff members understand and comply with this policy in their service, escalate any Data Protection issues or risks to their Head of Service and the Business Partner – Quality, Compliance and Improvement at the earliest opportunity and that staff complete/attend the Data Protection training provided.

Where a Data Subject requests for their data to be erased or processing to be restricted, the Business Partner – Quality, Compliance and Improvement should be contacted immediately, and they will provide support throughout that process. If the subject access request is complex or the service requires assistance with the subject access request, they should contact the archivist.

All employees, relief workers, volunteers and students on placement – are responsible for reading, understanding and applying the Data Protection Policy and shall follow scrupulously the Core Principles. Employees who have any queries regarding the policy should seek clarification from their line manager at the earliest opportunity.

Failure to comply with this policy could constitute gross misconduct under the Council's Disciplinary Policy and Procedure.

All employees are responsible for completing/attending and actively engaging in Data Protection training.

Any employee who breaches the policy or witnesses a breach should report this to their line manager or the Business Partner – Quality, Compliance and Improvement immediately.

Social Care Council Members – are responsible for ensuring that Senior Management are complying with the Data Protection Act and CrossReach policy.

Council members are personally responsible for ensuring that they adhere to the policy with any personal or special category data they receive as a result of their role as a Council member.

References to other Policies/Documents

Other policies and documents which should be read in conjunction with this policy are:

- CrossReach Data Protection Guidance
- GDPR Compliant Communications
- AC and OPS retention schedule
- C&F retention schedule
- Mobile Devices Policy
- Church of Scotland Data Protection Policy
- Records Policy
- Service User Records Policy
- IT Access Policy
- Data Protection Breach Management Plan
- CrossReach Disciplinary Policy and Procedure
- Subject Access request process
- Data protection Hints and Tips
- Subject Access Request – DSR Guidance and Standard Responses
- Gathering Data for a SAR – Guidance
- Privacy Notice for Employees
- Privacy Policy – Community
- Privacy Policy – Residential
- Redaction Guidelines
- Complaints and Compliments Policy 2026
- Interim AI Guidance

Ethics and Legislation

The Data Protection Policy will be followed in line with the legal requirements and principles of the Data Protection Act 2018, General Data Protection Regulations and Data Use and Access Act 2025 and will be applied through the Ethos and Values of CrossReach.

Monitoring and Auditing

Service Managers/Departmental Managers will be responsible for the ongoing monitoring of application of the Data Protection Policy.
Heads of Service will audit Managers undertaking this monitoring through routine service audits throughout the year.

The Data Protection Policy will be reviewed on a 3 yearly basis, or sooner in the light of any legislative or other developments. Any substantive changes will only be introduced with the approval of the Data Protection Compliance Officer.

Appendix 1 – Glossary of Terms

Breach Management Plan - sets out the course of action to be taken to reduce the risk of a data protection breach and aims to mitigate the damage caused if a breach does occur. The plan defines what constitutes a breach and provides a step-by-step process that should be followed when an incident occurs. The current Breach Management Plan can be found here: Breach Management Plan - May 2018

Data Controller - is the organisation that determines the purposes for which and the manner in which personal data is processed. The General Assembly of the Church is the official Data Controller for CrossReach but day to day operational control and resulting responsibilities rest with CrossReach itself.

Data Processing – means obtaining, recording or holding the information or data or carrying out any operation on the information or data (such as altering, consulting, organising, destroying, making available etc)

Data Protection Compliance Officer – The Solicitor of the Church of Scotland is the Data Protection Compliance Officer for CrossReach and provides advice to CrossReach in relation to data protection law.

Data Protection Principles – These state that personal data must:

1. Be processed fairly and lawfully and transparently;
2. Be collected and processed only for specified, explicit and legitimate purposes;
3. Be adequate, relevant and limited for the purposes for which it is processed;
4. Be kept accurate and up to date. Any inaccurate data must be deleted or rectified without delay;
5. Not be kept for longer than is necessary for the purpose for which it is processed and
6. Be processed securely.

Data Subject – is a person about whom personal data is stored in electronic or paper form in a structured filing system.

Information Commissioners' Office (ICO) - The 'Act' requires every organisation that processes personal information to register with the ICO and file annual reports. The notification is made in the name of the General Assembly of the Church of Scotland by the Data Protection Compliance Officer, the Solicitor of the Church. The CrossReach registration can be viewed at:
http://ico.org.uk/ESDWebPages/DoSearch?reg=155161

Type/classes of information processed
CrossReach is registered to process the following types/classes of information including:

- personal details
- family, lifestyle and social circumstances
- financial details

- employment and education details
- goods or services provided

In addition, CrossReach may process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- trade union membership

Should employees become aware of any processing of data not covered in the registered entry or amendments required to it, they must raise this immediately with the Business Partner – Quality, Compliance and Improvement, who will contact the Data Protection Compliance Officer. Failure to do so, or to knowingly process data other than in accordance with the registered entry, may constitute an offence under the Act.

Legal Basis for Processing – in order to collect, process and share information, CrossReach must ensure that it is clear legal basis to do so. GDPR sets out 6 legal bases for processing personal and special category data:

1. Consent,
2. Contractual,
3. Legal Obligation,
4. Vital Interests,
5. Public Task,
6. Legitimate Interest.

The legal basis should be assessed and recorded. For current key record types this has been done centrally.

Personal Data - is data which relates to any living individual identifiable from that data itself or in combination with other information which is or may be held by the Data Controller (see below), in electronic form or in a relevant filing system (including emails and other electronic messages). This includes any opinions expressed about the Data Subject and any indication of the intentions of any other person in respect of the Data Subject. It does not include anonymised data.

A significant amount of information held by CrossReach will be Personal Data (this includes personal and special category data) as it could refer to a person's health (physical or mental) and/or religious beliefs. Employees must therefore take additional care when dealing with any Personal Data.

Such data must be processed under strict conditions, ensuring there is a legal basis for processing such data. Legal Bases which are most relevant to CrossReach are Contractual Obligation, Legitimate Interest and Explicit Consent.

Personal or Special Category data processed by CrossReach is likely to fall into one of these categories, none of which are exhaustive:

- Data relating to People who use a CrossReach service
    - This could include name, address, contact details, next of kin, bank details, medical history, medications, care history, care/support needs, dietary

information, religious belief etc. It could be held in Care/Support plans, medication records, emergency contact lists, financial records etc. See the relevant privacy notice.

- Data relating to CrossReach employees and volunteers as Data Subjects
    - This could include name, address, contact details, emergency contact details, bank details, employment history, qualifications, disciplinary sanctions, sickness information, ethnic origin, religious belief etc. It could be held on the HR system, personnel files, supervision records, application forms etc. See the relevant privacy notice.
- Data about contacts such as Council/Committee members and other church members
    - This could include names, address, phone number, e-mail address, bank details etc. It is likely to be held in Church/CrossReach databases. See the relevant privacy notice.
- Data provided by contacts about their own contacts or other data subjects e.g. CrossReach givers, supporters and shoppers,
    - This could include names, address, phone number, e-mail address, bank details etc. It is likely to be held in Church/CrossReach databases, mailing lists etc. See the relevant privacy notice.

Privacy Impact Assessments - is a process which assists organisations in identifying and minimising the privacy risks of projects or policies.

Privacy Notices - detail the types of data held for the category of people the privacy notice covers. They detail how information will be held, shared and destroyed.

Records Retention Schedule - is a document that lists the types of records produced by the service area or department, along with the agreed length of time each record will be retained for and the final disposition methods. A retention schedule applies to both paper and electronic/digital records and will be an appendix to the Records Retention Policy. Current Retention schedules can be found here: Retention Guidelines

Special Category Data - is information that refers to racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, genetic or biometric data, and criminal convictions and offences. CrossReach will only hold Special Category Data to fulfil our purposes and will do so in line with processing conditions specified in the Data Protection Act and Data Use and Access Act.

Subject Access Requests – the Subject Access Requests process can be found here: Subject Access Request Process 2018

Organisational Policy - Version Control. This Version:		
CROSSREACH	Policy:	**Data Protection**
	Policy Family:	QCI, Data Protection
	Original CMT Date:	2014
	Most Recent Update:	August 2026
	Type of Update:	Full Review