

# **DATA PROTECTION POLICY**

## **Policy Statement**

In order to provide care and support for children and vulnerable adults across Scotland, CrossReach collects and uses 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 data protection legislation in force in the United Kingdom.

## **Purpose of the Policy**

The purpose of this policy is to provide guidance on data protection principals that all those acting on behalf of CrossReach 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, including employees and volunteers, comply with the 6 Data Protection Principles, summarised below.

“Personal Data” (information identifying a living person) should:

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

## **Who is Affected by this Policy**

All employees and volunteers of CrossReach as well as individuals for whom CrossReach collects, stores, transfers and shares personal or special category data.

## **Who Should Know About this Policy**

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

## **Why Do Employees Need To Know About this Policy**

Data protection legislation obliges all employees to take a proactive approach to data protection. In order to encourage best practice – and to avoid penalties from the Information Commissioner’s Office – all employees are required to read this policy and to treat others’ personal information with due care and consideration.

## **Definitions**

**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 paper form. 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.

**Special Category (Personal) 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 2018 Act and the GDPR.

**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.

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

**Privacy Impact Assessments** - is a process which assists organisations in identifying and minimising the privacy risks of projects or policies and large scale processing of information, payroll for example.

**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 current and historic paper and electronic/digital records and will be an appendix to the Records Retention Policy.

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

**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 personal data or carrying out any operation on the 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.

**Information Commissioners Office (ICO)** - The 'Act' requires every organisation that processes personal information to register with the ICO. CrossReach is registered under the General Assembly of the Church of Scotland. In the event of a notification needing to be made that will be done for CrossReach by the Data Protection Compliance Officer, the Solicitor of the Church.

**Legal Basis for Processing** – in order to collect, process and share information, CrossReach must ensure that it has a 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. In order to comply with legislation, the legal basis for processing information should be assessed and recorded.

## **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 (or “special categories”) 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

A significant amount of information held by CrossReach will be Special Category Data as it could refer to a person’s health (physical or mental) and/or religious beliefs. Such information must be treated as being confidential and processed in line with data protection requirements, ensuring there is a legal basis for processing such data.

The legal bases which are most relevant to CrossReach’s processing of information are: for the purposes of meeting contractual obligations; legitimate interests; performing a task in the public interest; where required to fulfil a legal obligation and explicit consent.

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

- Data relating to people who use a CrossReach services
  - This could include names, addresses, contact details, next of kin, bank details, medical history, medications, care history, care/support needs, dietary information, religious belief, photographs etc. It could be held in Care/Support plans, medication records, emergency contact lists, financial records etc. See the privacy notice for people who use a CrossReach service.
- Data relating to CrossReach employees and volunteers as data subjects
  - This could include names, addresses, contact details, emergency contact details, bank details, employment history, photographs, 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, addresses, phone numbers, e-mail addresses, bank details etc. It is likely to be held in Church/CrossReach databases. See the relevant privacy notice.

- Data provided by contacts as data subjects e.g. CrossReach givers, supporters and shoppers,
  - This could include names, addresses, phone numbers, e-mail addresses, bank details etc. It is likely to be held in Church/CrossReach databases, mailing lists etc. See the relevant privacy notice.

**Should employees become aware of processing of any data not covered by this policy or included in CrossReach's registration with the ICO, or become aware that amendments are required to the processing of data (for example if there are inaccuracies or in the event that someone wants their information to be deleted), they must raise this immediately with the Business Partner – Quality, Compliance and Improvement, who may require to 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.**

## **Core Principles**

CrossReach adheres to data protection legislation in the following ways:

1. By adhering to the 6 Principles detailed in the Data Protection Act.
2. Through privacy notices that specify to data subjects the purpose for which information will be used.
3. Ensuring that there is a legal basis to collect, process and share personal or special category data and that this has been recorded.
4. Ensuring 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 a locked room or in a locked cabinet and electronic records being password protected, portable devices encrypted or alternative approved security features being in place.
5. Only collecting and processing 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 matters.
6. Take 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.
7. Retaining information in line with retention schedules, securely destroying it when appropriate and maintaining a destruction log.
8. Ensuring that personal information is not transferred, internally or externally, without suitable safeguards and in line with CrossReach Policy.
9. 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.
10. Ensure that information is available to data subjects to understand how to make a Subject Access Request.
11. Complying with all Subject Access Requests, ensuring the rights of data subjects 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.
12. 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.
13. Where new systems or processes are being developed in relation to personal or special category data, privacy by design should be incorporated from the outset. The QCI team should be contacted for support.

14. 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.
15. 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 Apps such as DropBox and Evernote.
16. Will not share personal information with third parties without consent unless we are lawfully or contractually obliged to do so.

## **Responsibilities**

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

**SMT** – 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 data protection legislation and CrossReach Policy and Data Protection Guidance.

SMT members must ensure that any potential or actual data breaches are immediately reported to the Business Partner, Quality, Compliance and Improvement who will undertake to report to the 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 when a data subject requests access to the data held on them, they wish data held to be amended or removed or they request for the restriction of their data being processed.

**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.

**All employees, relief workers, volunteers and students on placement** – are responsible for reading, understanding and applying the Data Protection Policy and shall scrupulously follow 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 legislation 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 (to follow)
- CrossReach Data Protection Compliance (to follow)
- CrossReach Privacy Policy
- CrossReach Privacy Notices
- Portable ICT Devices Policy
- Church of Scotland Data Protection Policy
- Records Policy
- Service User Records Policy
- IT Access Policy
- Record Retention Policy
- Data Protection Breach Management Plan
- Data Subject Access Policy
- CrossReach Disciplinary Policy and Procedure

### **Ethics and Legislation**


The Data Protection Policy will be followed in line with the legal requirements and principles of the Data Protection Act 2018, the General Data Protection Regulation and any other data protection legislation in force in the United Kingdom 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.

	Policy	Version	Three	Approved by:	CMT
	Number:			Effective Date:	
	Approved:			Next Revision Date:	



The Church of Scotland

Social Care Council

Operating as CrossReach, Scottish Charity No: SC011353