



CHRISTIAN RELIEF AND EDUCATION FOR THE SOUTH SUDANESE (CRESS)

DATA PROTECTION POLICY – September 2018

Introduction – taking personal data protection seriously

CRESS needs to collect and use certain types of information about the individuals, contributors and sponsors who come into contact with the organisation in order to carry on its work. CRESS regards the lawful and correct treatment of personal information as very important to successful working, and to maintain the confidence of those with whom it deals.

CRESS Data Protection Policy Statement

This policy seeks to ensure that CRESS undertakes its responsibilities with regard to the protection of the personal data which it collects, stores and uses.

The CRESS data protection policy sets out how CRESS is compliant not only with current data protection legislation under the Data Protection Act (DPA) 1998 but also with the new regulations, supplementary to the DPA, as given in the General Data Protection Regulations (GDPR) 2018.

In compliance with the DPA (1998) CRESS has obtained and stores personal information given only by consent and processes that data only for legal purposes of the organisation.

CRESS understands and upholds the principles of data protection as given under the DPA (1998) and are listed in Appendix 1. The DPA (1998) also sets out five key areas which encompass best practice for good data governance and which CRESS endeavours to follow. These are accountability, visibility, consent, access and stewardship.

The GDPR (2018) extends these principles and seeks to strengthen data protection through more rigorous data security provision and through extended rights. CRESS understands and upholds all data protection rights given under the DPA (1998), and also those rights extended under the new legislation GDPR (2018). These are given in Appendix 2.

The aim of this policy is to ensure also that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures as set out in this document.

Data Collection

CRESS collects personal data only from those who have filled in, signed and returned their CRESS Data Protection Consent form.

The personal data that CRESS stores consists of: name, postal address, telephone number, email address and the record of any contributions. This data is used and processed only for contact about CRESS people, activities and projects, and to enable Gift Aid tracking and for accounts.

In compliance with GDPR (1998), CRESS uses a data protection consent form which has to be filled in by all current and new donors. This consent form also gives the privacy statement and options for opting in or out of contact by email, phone and post.

Data Storage & Security

CRESS takes steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

CRESS ensures personal data is stored securely and uses ChurchBuilder as their cloud storage provider. ChurchBuilder is a church management system and provides people based databases. This is a secure on-line tool and stores all the personal data which CRESS collects and uses. ChurchBuilder complies with all relevant legislation and owns their own servers which are based in the UK. Access to the CRESS ChurchBuilder database is controlled by usernames and passwords with password strength checking built in. Connections between ChurchBuilder and a user are encrypted.

There are also two office copies of the data which are stored on different hardware drives, accessed by strong passwords, by different CRESS staff members and kept in different places.

CRESS recognises the possibility of data breaches. It relies primarily on the high level of security given by ChurchBuilder. It protects the office copies with strong passwords, office alarms and checks carefully any staff member who is trusted with access.

Data Access & Responsibility

Under the Data Protection Guardianship Code, overall responsibility for personal data in CRESS rests with the governing body of trustees. These then delegate to a designated Data Protection Officer (DPO) who then is responsible for all other staff understanding the requirements of efficient implementation of this policy.

The DPO for CRESS is **Caroline Lamb (CEO)**.

All key CRESS staff have been informed and understand the legal responsibilities under DPA (1998) and GDPR (2018).

Training and awareness of all staff who collect and process personal data is done within CRESS at the time of induction, through reading, understanding and the signing of this policy and through on the job awareness.

CRESS ensures that everyone managing and handling personal information is trained to do so and that they are contractually responsible for following good data protection practices. Also that any disclosure of personal data is in line with CRESS procedures and that queries are dealt with swiftly and politely. Staff should be aware that any unauthorised disclosure of personal information will result in disciplinary procedures.

Continued monitoring of this policy will take place at regular intervals by CRESS senior managers.

A formal review with CRESS senior managers and all trustees will take place every three years to ensure that this policy is fit for purpose and reflects up to date legislation and work practices.

By operating internationally, CRESS is aware that these data protection issues may also apply to the delivery partners in Uganda (Dioceses of Liwolo and DOKK), international funded staff and project beneficiaries.

Signatories

The CRESS data protection officer and all CRESS senior managers and trustees should read and agree to this policy by signing a copy of the policy. Appendix 3 gives the signatory form.

APPENDIX 1 – Principles of the Data Protection Act 1998 will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specific and lawful purpose.
- Be adequate, relevant but not excessive.
- Be accurate and kept up to date.
- Not be held longer than necessary.
- Be processed in accordance with the rights of data subjects.
- Be subject to appropriate security measures.
- Not to be transferred outside the European Economic Area (EEA).

APPENDIX 2 – Data rights of individuals specified under the DPA (1998) and extended under GDPR (2018):

Rights of people under the DPA (1998):

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information.
- The right to prevent processing in certain circumstances.
- The right to correct, rectify, block or erase information which is regarded as wrong information.

Rights of people extended under GDPR (2018):

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to process restriction.
- The right to restrict portability.
- The right to object.
- The right to deny automated decision-making.

APPENDIX 3 - Data Protection Signatory Form:

I CONFIRM THAT I HAVE READ AND UNDERSTOOD CRESS'S DATA PROTECTION POLICY AND WILL ACT IN ACCORDANCE WITH IT.

I AM CONNECTED WITH CRESS IN MY CAPACITY AS A:

- MEMBER OF STAFF
- VOLUNTEER
- SENIOR MANAGER
- TRUSTEE

NAME CATHERINE CHAPMAN

SIGNATURE C. Chapman

DATE 25 SEPT 2018