DATA PROTECTION POLICY

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 seeks to comply not only with current data protection legislation under the Data Protection Act (DPA) 2018 but also with the new regulations given in the General Data Protection Regulations (GDPR) 2018.

In compliance with the DPA (2018) CRESS has obtained and stores personal information given only by consent and processes that data only for legal purposes of CRESS.

CRESS understands and complies with the principles of data protection as given under the DPA (2018) and listed in Appendix 1. The DPA (2018) 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 (2018), and also those rights extended under the new legislation GDPR (2018). These are listed in Appendix 2.

The aim of this policy is to ensure also that everyone handling personal data is aware of these principles and rights 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 (2018), CRESS uses a data protection consent form which is completed 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 Xero as their cloud storage provider. Xero is a 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. Xero complies with all relevant legislation and owns their own servers which are based in the UK. Access to the CRESS Xero database is controlled by usernames and passwords with password strength checking built in. Connections between Xero 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 Xero. It protects the office copies with strong passwords, office alarms and checks carefully any staff member who is trusted with access.

CRESS recognises that in some cases legitimate interest may apply.

DATA ACCESS & RESPONSIBILITY

Under the Data Protection Guardianship Code, overall responsibility for personal data in CRESS rests with the governing body of trustees.

All CRESS employees, the Chief Executive Officer, trustees and designated volunteers ("key staff") have been informed of this Data Protection Policy and of the need to protect personal data under DPA (2018) and GDPR (2018).

Training and awareness of key 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 seeks to ensure that everyone managing and handling personal information is trained to do so and that they are responsible for following good data protection practices. Any use of personal data is consistent with CRESS procedures and that queries from individuals about their personal data are dealt with swiftly and politely. Key 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 trustees.

A formal review of this Policy with the Chief Executive Officer of CRESS and trustees will take place every three years to ensure that this policy is fit for purpose and reflects current legislation and work practices.

By operating internationally CRESS is aware that these data protection issues may also apply to the CRESS partners based in Uganda as well as project beneficiaries. We have requested their compliance and they are in receipt of a copy of this policy.

SIGNATORIES

The Chief Executive Officer of CRESS and CRESS' senior trustees should read and agree to this policy by signing a copy of the policy. Appendix 3 gives the signatory form.

Name:	Caroline Lamb
Position:	Chair of the Trustees
Date:	20/03/2020
Signature: