General Data Protection Policy

What is GDPR:

The General Data Protection Regulation (GDPR) is an EU-wide regulation which will become effective in the UK on 25 May 2018. It replaces the existing law we have on data protection (the Data Protection Act 1998) and give individuals more rights and protection in how their personal data are used by organisations.

Key Principles of the General Data Protection Regulation:

Article 5 of the GDPR (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) contains the principles and requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Purpose

GDPR is a fundamental legal responsibility of every charity to ensure that they have the right policies and procedures in place so that they are being run properly and are taking individuals' rights seriously whilst processing personal data.

This policy applies to all personal data processed by UniTED. A Trustee shall take responsibility for UniTED's ongoing compliance with this policy. This policy shall be reviewed at least annually. UniTED shall register with the Information Commissioner's Office as an organisation that processes personal data.

Scope

This policy is mandatory for all UniTED employees worldwide. For the purposes of this policy, 'employee' is defined as anyone who works for or on behalf of UniTED, either in a paid or unpaid capacity. This therefore includes directly employed staff, trustees, contractors, employees and volunteers of sub-contractors, agency workers, consultants, volunteers, interns and all visitors to UniTED work programmes and offices.

It also covers youth-led ventures who are beneficiaries of our programs and implementing partners, and who we expect to work under the policy as a condition of their involvement with UniTED.

General Data Protection Policy

Individual Rights under GDPR:

An individual (All employees, volunteers, consultants, agency staff, sub-contractors, partner organisations, youth-led ventures) has the following rights with respect to their personal data gathered at UniTED:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object (including objecting to direct marketing)
- Rights in relation to automated decision making and profiling.

For more information on individual rights go to https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ individual-rights/.

Lawful, fair and transparent processing of Personal Data

- To ensure its processing of data is lawful, fair and transparent, UniTED shall maintain databases and data repositories
- Databases and data repositories shall be reviewed at least annually.
- Individuals have the right to access their personal data and any such requests made to UniTED shall be dealt with in a timely manner.

Lawful purposes

- All data processed by UniTED must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
- UniTED shall note the appropriate lawful basis in databases and data repositories.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in databases and data repositories.

Data minimisation

UniTED shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- UniTED shall take reasonable steps to ensure personal data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving / removal

- To ensure that personal data is kept for no longer than necessary, UniTED shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- The archiving policy shall consider what data should/must be retained, for how long, and why.

Security

- UniTED shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted this should be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

Designated Data Controllers:

Designated Data Controllers are responsible for handling reports or concerns, about the protection of vulnerable people, appropriately and in accordance with the procedures that underpin this policy.

Vanita Parmar, a UniTED trustee is the designated data controller.

They are responsible for:

- ensuring employees, volunteers, consultants, visitors and partner organisations are aware of the policy, are appropriately trained and are supported to implement and work in accordance with it
- creating a management culture that encourages reporting of data breaches
- acting immediately if they become aware of any data breaches and where appropriate based on a risk assessment, report these breaches to the ICO within 72 hours.
- ensuring monitoring and recording procedures are implemented

Accountability & Governance:

The Board of Trustees holds ultimate accountability for this policy UniTED will put into place proportionate governance measures, including reviewing and approving internal policies, documenting activity, keeping records of data processing, undertaking data protection impact assessments where necessary and maintaining records of investigations for data breaches.

Breach:

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, UniTED shall promptly conduct an investigation led by the Chair of the Board and assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website) and the individual concerned.

General Data Protection Policy

Glossary:

Personal data:	Any information relating to a living individual who can be directly or indirectly identified from it. This includes name, address, contact details but could also include two or more non-specific pieces of information that when combined could identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator and other descriptors
Special categories of personal data:	Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information, health and a natural person's sex life or sexual orientation.
Data controller:	A controller determines the purposes and means of processing personal data – organisations will be 'data controllers' (e.g. charities) when they hold and use the data of customers and clients. Charities will be 'data controllers' in a number of ways, including: – As an employer processing the personal data of employees, trustees and volunteers. – As a provider of personalised services to beneficiaries and clients – As a fundraising or campaigning organisation that has donors and supporters.
Processing personal data:	Means doing something with personal data – this includes keeping records, using data for direct marketing, carrying out a contractual obligation among others. A fuller definition of "personal data" can be found at https://ico.org.uk/

Date of Last Update: 20th May 2018

Responsible Owner: Chair of Trustees; CEO

Procedures:

Data responsibilities:

- All employees will be trained on this policy and procedures. They will know what would constitute a breach and how to report it.
- All business partners will be briefed on their responsibilities in relation to data protection.
- In every case consent will be requested from volunteers, interns, venture partnerships and employees for any data that is collected for legitimate business. These records of consent opt in will be stored in UniTED's Google shared fileshares. For social media, specific consent will be sought from the individuals concerned if they are happy to have their images and names to be used.
- An individual has the right to access, amend or revoke their data and this request must be made to the UniTED Data Controller in writing. These requests and their outcome will be stored for evidence in UniTED's Google shared fileshares. Certain exceptions may apply minimal personal data may need to be passed on to a specialised welfare or law enforcement agency in relation to a life threatening/safeguarding incident.
- UniTED will review the policy and procedures at least annually.
- UniTED will take every step to ensure data held is accurate and amended as per the request of the individual owner.
- All data will be held securely in password protected domains and will be destroyed in alignment with UniTED's data archiving policy.
- In the event of a breach, the data controller or the CEO will investigate the breach, document the investigation and depending on the risk of the breach, will report it to the ICO within 72 hours. If the breach involves an employee, the investigation will be conducted by the Chair of trustees and will document and report as required to the ICO.

Data Protection:

1. **Google Drive**

Access to the UniTED Google Drive will be limited to trustees and employees of UniTED – this will be ensured by a general password which all trustees and employees will use and that shall be changed every 6 months.

Certain parts of the Google Drive will be restricted further to certain trustees and employees through a different password to ensure there is a legitimate reason for access:

- Safeguarding incident reports will be accessed by designated safeguarding officers
- Job applications and references will be accessed only by the recruitment committee
- Log-ins spreadsheet will be accessed only by the CEO and Chair of Trustees

Other partners may be granted access to individual documents and/or folders containing information that pertains to them, provided that there is no inappropriate data within the document or folder and this type of access will be limited.

2. **Databases**

All documents with datasets will be password protected, to protect against computer theft.

General Data Protection Policy

Consent from Ventures and Volunteers:

The following statements will be implemented in documentation for Ventures, volunteer and Internship agreements to ensure data is collected only after explicit consent is obtained.

All Venture/Volunteer/Internship Agreements must have section on their consent to use data, to be signed separate from other clauses. These agreements will all be kept in the UniTED Google Drive securely via password protection.

This section shall read:

I, ……., consent to UniTED processing my data for the purposes of organising activities in Uganda, safeguarding, monitoring and evaluation. This includes permission for UniTED to use my image in photographs and video recordings in publications, including website entries, for any lawful purpose.

I understand that I have the right to access all data UniTED has about me at any time. And have the right to withdraw my consent for UniTED to process my data at any time, in accordance with the General Data Protection Regulation.

Signed….”

Mailing List

All newsletters to the UniTED mailing list will include a footnote giving recipients the option of removing themselves from the mailing list as well as the ability to request any information held about themselves at UniTED.