Please contact the Data Protection Officer at dpo@tearfund.org if you have any questions.

Title:	**DATA PROTECTION POLICY**
Policy statement:	Tearfund is committed to compliance with the UK General Data Protection Regulation ("UK GDPR"), the UK Data Protection Act 2018 ("DPA") and all other applicable regulations in respect of personal data and the protection of the rights and freedoms of individuals whose information Tearfund collects and processes. Tearfund's procedures for compliance with the UK GDPR and DPA are outlined in this policy and those policies and procedures listed below.
Procedures and other policies which relate to this policy	• Data Retention Policy • Information Security Policy • Guidelines on Handling Personal Data • Staff Privacy Notice • Personal Conduct Policy • Whistleblowing Policy • Content Gathering, Storage and Use Policy • Misconduct Policy • Affinis User Guides • Use of social media in high risk situations here • Key points to consider when sharing data with the Tearfund family All of the above documents are available on the Tearfund Policies Shared Drive, Corporate Hub, as an appendix to this policy, or on the affinis hub here, or on the global brand and photographic hub. • Terms of Reference for Data Protection Group • Data Breach Incident Reporting • Subject Access Request procedure • Record of Processing Activities The documents above are available, upon request, from the data protection officer - dpo@tearfund.org. • Data Storage Logs Each team has its own data storage log that it is responsible for keeping up to date.
Why the policy is needed:	Failure to ensure that the processing of personal data complies with legislation risks enforcement action, even prosecution, and compensation claims from individuals. There are also potentially serious reputational risk issues.
Who must follow this policy:	Everyone within Tearfund regardless of location or role. All employees of the Tearfund family, affiliates, volunteers, consultants or representatives of Tearfund who require access to Tearfund servers and platforms in order to perform their functions
Person responsible:	Finance Director reporting to the Board of Directors

Version:	Final
Approved by:	BOARD
Approval date:	July 2023
Next formal review:	July 2025

Introduction

Data protection is about safeguarding the fundamental right to privacy, which is enshrined in laws and regulations. All individuals need to have the means to exercise their right to privacy and protect themselves and their information from abuse. Tearfund works with a huge number of people across the world and needs to collect personal information to support the work that we do. Everyone within Tearfund will handle personal data at some stage in their role and it is therefore essential that we all understand the basic principles of data protection and our responsibilities in this regard.

Data Protection Training and Resources

Tearfund is committed to ensuring that all staff understand their obligations and responsibilities in connection with handling personal data. Data Protection e-learning is compulsory for **all** staff regardless of location within Tearfund. If you have any questions regarding data protection you should email: dpo@tearfund.org in the first instance.

Tearfund has a data protection officer and data protection groups which are formed of representatives from across the organisation and meet regularly to review our compliance with data protection.

WHAT IS PERSONAL DATA?

The data protection policy applies only when personal data is being processed

- Personal data only includes information relating to natural persons who:
    - can be identified or who are identifiable, directly from the information in question.
    - who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

WHAT IS PROCESSING?

- The UK GDPR applies to the processing of personal data that is:
    - wholly or partly by automated means; or
    - the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

- "Processing" is a very wide term - it includes collection, holding, storing and sharing.

WHAT IS SPECIAL CATEGORY DATA?

Special category (also referred to as sensitive) personal data is personal data which reveals or relates to an individual's:

- Racial or ethnic origin
- Political opinion or trade union memberships
- Religious or philosophical beliefs
- Genetics or biometrics
- Physical or mental health condition
- Sexual life/sexual orientation

In order to process special category data, we will usually need to rely on one of the following grounds:

1. Explicit consent of the individual;
2. Necessary to comply with our obligations and rights in the field of employment and social security;
3. processing is necessary for certain limited work-related health purposes;
4. Religious NGO exception processing carried out in the course of our legitimate activities, with appropriate safeguards;
5. The relevant information has already manifestly been made public.

Less commonly, we may seek to rely on:

1. Processing is necessary in connection with a legal claim;
2. Processing is necessary to protect the vital interests of the individual.

If you need to process special category data and are unsure whether you can rely on one of these grounds, seek advice from Tearfund's Legal team.

- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised then the anonymised data is not subject to the UK GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

DATA PROTECTION PRINCIPLES

What are they? Why must staff abide by them?

Tearfund commits to following the principles of Article 5 of the UK GDPR and sets out seven key principles which apply whenever personal data is being processed. Tearfund will keep a record on an ongoing basis of its personal data processing activities and the basis for processing it is relying on in

relation to each activity

Principle 1: Personal data must be processed fairly, lawfully and transparently

Fairly and lawfully: We need to have a legal basis on which to process the personal data that the individual is able to understand. Any personal data that is processed should be done on one of the following legal grounds:

- Consent
  Consent *needs to be:*
  - ★ *given by a* ***clear, affirmative*** *act which establishes a* ***freely given, specific, informed*** *and* ***unambiguous*** *indication that the data subject agrees to the processing of personal data for one or more* ***specific purposes****.*
  - ★ *We need to have evidence of the consent received where we rely upon this.*
- Contractual necessity
- Compliance with legal obligations(eg disclosing details to HMRC)
- Legitimate business interests (eg vetting)

If you are seeking to rely upon a Legitimate Business Interest as the legal basis for processing personal data you must first complete a Legitimate Business Interest Assessment. This is because Tearfund's legitimate business interest needs to be balanced against the interests or fundamental rights and freedoms of the individual. The template for this is linked in Appendix 1.

Less commonly, we may be able to rely upon:

- Public Interests (preventing or detecting unlawful acts)
- Vital Interests

Transparently: We need to communicate to data subjects in clear and plain language **how** we will use their personal data at the time of **collection.** This could be done by:

- Privacy policies on our website *www.tearfund.org*.
- Staff privacy notice linked at Appendix 1
- Express wording on paper consent forms or online webforms (i.e. Participant Permissions Template form, event application forms, online forms etc)
- Verbal explanations - which must be recorded
- Contractual wording

Data Privacy Impact Assessments - *a data privacy impact assessment must be completed before carrying out types of processing that are likely to result in a high risk to the rights and freedoms of the individuals. This would include where there is large scale use of sensitive data, data concerning vulnerable individuals or processing involving a new type of technology. A template DPIA can be found in Appendix 1 and these should be signed off by Tearfund's Legal team and Tearfund's Data Protection Officer. Once the DPIA is signed off, the outcomes must be integrated into the plan for processing the data. The DPIA must then be kept under review and revisited when necessary.*

Principle 2: Purpose Limitation

Personal data may only be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Tearfund must not obtain information for one purpose and then use it for another. We should be explicit about how we will use the personal data.

In more detail:

Tearfund has identified the following 'purposes' for which we collect data:

- *Administration:*
  - *Business purposes*
  - *Employees (inc. applicants, volunteers, consultants and freelancers)*
  - *Supporters*
- *Data Matching*
- *Direct Marketing:*
  - *Appeals and News Updates*
  - *Campaigning*
  - *Fundraising Events*
  - *Seeking Legacies*
  - *Volunteering Events*
- *Market Research*
- *Profiling*
- *Prospecting*
- *Provision of Services*

If you are collecting personal data for a purpose which you do not believe would fall into one of the above categories please email dpo@tearfund.org.

Example:

An individual applies for a job on Tearfund's website and provides personal information to be used for the purpose of the recruitment (which would fall within Administration: Employees). The email address they supplied should not then be used for sending marketing emails unless we had their express consent for this.

Principle 3: Data minimisation

We need to be able to demonstrate that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

This is a balancing exercise between collecting sufficient information for the intended purpose but also ensuring that we don't collect information 'just in case' it might be useful. This principle is relevant when designing things such as web forms or surveys. We should consider what information we are collecting and why we need it. We should also be careful about recording opinions or excessive information about individuals. Remember the individual can request to see any information we hold about them and you therefore need to be able to explain why you have the information.

Example:

For monitoring and evaluation purposes Tearfund may collect feedback from a pool of project participants to measure impact. The survey asks for family information which is personal data. However, there is no need for respondents to provide any further personal information such as their address so that additional information should not be sought. This would ensure that the information collected is only that which is necessary for the purposes of measuring impact. However, if Tearfund wanted to include a named case-study as part of the impact report we would need the explicit consent of that participant.

Principle 4: Accuracy

Personal data shall be accurate, and where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed is erased or rectified without delay

Wherever possible, staff should use central sources to record and gather data (Affinis, SelectHR, IBIS etc) as this should be up to date and accurate. Staff should not create unnecessary copies Any location where personal data is stored must be included in the team storage log.

Staff should make the necessary changes to data as soon as they are informed or when the errors are noticed. Out-of-date information should be destroyed.

Principle 5: Storage Limitation

Personal data must be kept for no longer than is necessary for the purpose for which it is processed.

We need to ensure that we can justify why it is necessary to continue to process (which includes storing) personal data either electronically or hard copy.

You should ensure data is being stored in accordance with the timescales set out in the Retention Policy and that you are familiar with the guidelines on handling personal data both of which are linked in Appendix 1.

In more detail

- *You should ensure that you name any Google documents with personal data in such a way that it is easy to understand (i) what the document is; and (ii) when it should be deleted and (iii) restrict access so there are not multiple copies of personal data in the Google drive.*
- *You should delete personal data from your email inbox and sent items as soon as it is no longer required.*
- *You should ensure that your team Data Storage Log is reviewed quarterly and kept accurate - consider adding this to your regular team meeting catch ups.*
- *You should ensure that you know how to delete and archive data.*
- *You should ensure that you regularly delete items from your 'download' folder.*
- *You should anonymise personal information if you would like to retain it for statistical or research purposes.*

Principle 6: Integrity and confidentiality (security)

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, or destruction of, or damage to, personal data

This is potentially the biggest source of risk for Tearfund with phishing and hacking a major risk for all international organisations. All employees at Tearfund are responsible for ensuring the data they access is kept safe and secure at all times and must ensure compliance with the Information Security Policy and that they have read and understand the Guidance on Digital Security.

In more detail

Tearfund has both organisational and technical measures in place. Examples of these include:

Organisational

1. *Staff training on data protection*
2. *Policies on Data Protection and Information Security*
3. *Guidance on Digital Security*
4. *Training and guidance on use of Google Documents*

5. *Provision of locked cupboards*

Technical

1. *System back-ups*
2. *Encryption*
3. *Database access permissions*
4. *Google Drive*
5. *Third party software*

Each of us has a part to play - from ensuring that we lock cupboards and computers, to ensuring that we do not send emails to incorrect addresses or give individuals access to personal information who do not need to see it. All staff must familiarise themselves with the Information Security Policy which is circulated annually and available at any time on the Corporate Hub.

Principle 7: Accountability

The accountability principle requires Tearfund to take responsibility for the personal data being handled and its compliance with the other six principles. Appropriate measures and records are also required to be in place as to demonstrate compliance. Tearfund provides mandatory induction data protection training and regular compulsory elearning revision for existing staff. The Core Data Protection Group meet regularly to review responses to any data breaches and the organisation's compliance with policies and procedures and the Wider Data Protection Group which has representatives from all teams at tearfund provides a further opportunity for reminders about best practice to be disseminated.

Tearfund has appointed a Data Protection Officer, who acts as the contact point with the Information Commissioner's Office and data subjects.

Other Key Issues

Privacy and Data Protection Rights of Individuals

Tearfund will respect the rights granted to individuals by data protection laws, including rights to:

- Access their data
- Restrict the use of their data
- Rectify inaccuracies in their data
- Erase their data
- Restrict unsolicited contact
- Be notified of data breaches
- Be informed of the criteria for any automated decision making about them
- Complain

Please email dpo@tearfund.org for more details

Personal Data Breaches

In a large organisation working globally there will be occasions - which may be accidental - where personal data is deleted, lost, altered without permission or disclosed or accessed by those who were not authorised to see or access the information. This is defined as a personal data breach. It will cover a huge variety of incidents such as:

★ accidentally emailing a supporter's details to the wrong email address;

- ★ paper participant permissions templates being misplaced during a trip;
- ★ a laptop being stolen which contained personal data;
- ★ a supplier notifying us that their systems have been unlawfully accessed;
- ★ the Tearfund system or network being hacked;
- ★ incorrect access being given to staff members of a document or database containing sensitive personal data.

Tearfund has in place a Data Breach Incident Response Plan to respond with Personal Data Breaches (and other security breaches). The key message for all staff members is that you **must report** any data breach you become aware of **immediately**, by emailing databreach@tearfund.org (*note: if the breach involves lost or stolen IT equipment, safety or security issues, or any other type of incident, you should instead submit an incident report to incident.reporting@tearfund.org, who will notify databreach@tearfund.org of the data breach*). This is because if we are required to notify the Information Commissioner's Office we need to do so without undue delay and if possible within 72 hours of becoming aware of the breach. We therefore have a very short timeframe. Please see the attached process for reporting a breach in more detail.

Privacy by design and default

Before adopting new data processing or activities that may present high risks to privacy and personal data Tearfund will conduct and document a data protection impact assessment.

Tearfund will use processes such as pseudonymisation (to reduce privacy risks to data subjects) or anonymisation to minimise the collection, use, storage or any other form of processing of personal data.

Scope of UK GDPR

As our Tearfund Country Offices are not separate legal entities, and do share personal data for the purposes of Tearfund we work on the basis that the UK GDPR applies to this processing. The UK GDPR is therefore applied to participant data collected in Country, personnel files of national staff etc. and that is why all staff must comply with this policy.

International Transfers

Any access of personal information in another country will amount to a 'transfer' to that country. For example, if a staff member opens up a google document which contains personal data in India, this amounts to a transfer of that data to India. Under the GDPR the default position is that personal data cannot be transferred or accessed outside the UK unless one or more or the following conditions are met: (i) the European Commission has declared the data importing country to be an 'adequate jurisdiction'; or (ii) appropriate safeguards have been put in place, for example, Binding Corporate Rules ("BCRs"), or Standard Contractual Clauses ("SCCs"). The UK has determined that the EU's data protection laws are adequate and the EU has determined the UK's data protection laws to be robust enough. This means data can safely flow from the UK to the EU and vice versa.

Tearfund has put in place data transfer agreements containing standard contractual clauses to enable data transfer between Tearfund family members together with a Guarantee Declaration ("Declaration") with respect to the transfer of personal data from Tearfund UK to other Tearfund country offices.

Local law

Alongside this policy the applicable laws in the countries where Tearfund operates must be followed when collecting and processing personal data. Where these applicable laws demand stricter protections for personal data Tearfund must comply fully and implement any additional policies and processes where needed.

Sharing Personal Data

Personal data (including basic information such as names) must not be shared with any third party outside of Tearfund (including contractors, suppliers, partners, donors etc) unless that sharing complies with the Data Protection Principles, there is a contract in place, and assurance (which should be in the contract) that the third party has appropriate technical and organisational measures in place to safeguard the personal data. Tearfund's Legal team have standard GDPR compliant data protection clauses for inclusion in your contracts. Please email legal@tearfund.org to obtain Tearfund's standard GDPR clause.

Children and Data Protection

Where we are relying upon consent as the ground for processing the personal data of children, only those children aged over 13 may consent (in the UK - this may be 16 in other EU jurisdictions). For children under 13 we will need the consent of the individual with parental responsibility for the child and reasonable steps must be taken to verify this.

Appendix 1

1. Staff Privacy Notice
2. Legitimate Business Interest Assessment
3. Retention Policy
4. Guidelines for Handling Personal Data
5. Data Privacy Impact Assessment