Title:	**DATA PROTECTION POLICY**
Policy statement:	Tearfund is committed to compliance with the UK General Data Protection Regulation ("UK GDPR")[1], the UK Data Protection Act 2018 ("DPA") and all other relevant laws in respect of personal data and the protection of the rights and freedoms of individuals whose information Tearfund collects and processes. Compliance with the UK GDPR is described by 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 • Use of social media in high risk situations • Terms of Reference for Data Protection Group • Data Breach Incident Reporting • Subject Access Request procedure • Record of Processing Activities • 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

[1] The Brexit transition period ended on 31 December 2020. As part of the new trade deal the EU has agreed to delay transfer restrictions for at least four months, which can be extended to six months. The EU GDPR is an EU Regulation and it no longer applies to the UK. However, the GDPR has been incorporated into UK data protection law as the UK GDPR – so in practice there is little change to the core data protection principles, rights and obligations.

However, there are implications for the rules on transfers of personal data between the UK and the EEA. The UK government has stated that transfers of data from the UK to the EEA are permitted. The UK government is currently seeking an adequacy decision from the EEA. If this is granted it would allow the free flow of personal data from the EU/EEA to the UK to continue without any further action. If it is not granted, other appropriate safeguards such as standard contractual clauses will be required.

	perform their functions
Person responsible:	Finance Director reporting to the Board of Directors
Visability:	Public
Approval date:	February 2021

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 Training is available and compulsory for **all** staff regardless of location within Tearfund.

Tearfund has a data protection group which is formed of representatives from across the organisation and meets regularly to review our compliance with data protection.

The Data Protection Principles

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:
- Contractual necessity:
- Compliance with legal obligations:
- Legitimate business interests:

Less commonly, we may be able to rely upon:

- Public Interests
- 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.** There are lots of different ways we might explain to a data subject how we will use their personal data. These include:

  - Privacy policies on our website
  - Staff privacy notice
  - Express wording on paper consent forms or online webforms (i.e. beneficiary consent form, event application forms, online forms etc)
  - Verbal explanations
  - Contractual wording

In more detail….

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.*
- ★ *All supporter consent must be logged on Affinis.*
- ★ *Consent does not last indefinitely and we will need to take steps to ensure that we renew consent.*
- ★ *Standard wording for data collection from supporters is available from the Global Fundraising Group and any deviation from this wording must be signed off by the Fundraising Compliance Officer. If other groups within Tearfund are drafting consent wording this should be reviewed by legal.*
- ★ *There is some helpful guidance on beneficiary data in cash programming, which although drafted pre GDPR may still be helpful and can be found by staff*

Legitimate Business Interest
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.

Contractual Necessity *the individual must be the other party to the contract in order to rely upon this legal basis.*

Privacy Notices *- Tearfund currently has privacy notices for supporters and website users which can be found on www.tearfund.org. Tearfund's privacy notice for staff is linked at Appendix 1. You must ensure that any supporter data or employee data is gathered in a way which is consistent with these privacy notices. For other categories of data subject (beneficiaries, contractors etc) you must ensure that you use the data in a way that is consistent with the privacy disclosure made: whether in the contract, on online forms or given verbally.*

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 legal 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: Personal data may only be collected for specific, explicit and legitimate 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*

Examples:

1. *Beneficiary data is collected in South Sudan as part of the implementation of a project. The processing of this data would be classified as being processed for Administration: Business purposes. We may be processing this on the basis of a legitimate business interest or the consent of the beneficiary depending upon the circumstances. We would not then be able to use the beneficiary data to send marketing materials or carry out market research as this would not be in line with the original purpose.*

2. *A supporter signs up to receive further information about Tearfund at a Tearfund event. We would be processing the supporter's data for the purpose of Direct Marketing. We would not then be able to use the supporter's details to send out information about Tearfund job vacancies unless they have also subscribed to job alerts.*

3. *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: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

We need to be able to justify why all of the information that we are collecting is necessary for the purpose. 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.

Examples:

1. *Tearfund asks a website user to fill in details of their interests when making a donation. This information is not required to process the donation and sits on the record for 'information' only. It would be difficult for us to justify why the collection of this data was necessary or relevant for the purposes of processing the donation. In contrast, if an individual was volunteering overseas with Tearfund we may be able to demonstrate that this information is relevant for making decisions about the location or the team that the*

individual would be placed with.

2. *For safety and security purposes, Tearfund requests that staff or volunteers working overseas provide detailed information about their medical history in a medical form. For staff working only in the UK this procedure may not be relevant and therefore Tearfund would not collect this information from them.*

3. *For monitoring and evaluation purposes Tearfund may collect feedback from a pool of beneficiaries to measure impact. The survey asks for sensitive medical information. It does not, however, need them to provide any personal information such as their name or address and the survey can therefore be anonymous. 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 beneficiary.*

Principle 4: Personal data shall be accurate, and where necessary, kept up-to-date

The GDPR requires us to take 'every reasonable step' to ensure that personal data that is inaccurate is erased or rectified without delay. We are responsible for ensuring that the data we hold on individuals is accurate and up-to-date wherever possible. Individuals have the right to complain to the ICO if we fail to amend our records when requested to do so. In certain instances, such as when a spouse has recently died, it can be distressing to continue to receive mail addressed to them.

Wherever possible, staff should use central sources to record and gather data (Affinis, Select HR, IBIS etc) as this should be up to date and accurate. Staff should not create unnecessary copies (such as their own contact list) as this will quickly become out of date. Any location where personal data is stored should 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.

Examples

1. *If a supporter contacts Tearfund to inform us that they have moved house we should update Affinis as soon as possible. The previous address may be required to remain on the record for accounting purposes, but it should be made clear that no further correspondence will be sent to that address.*

2. *Tearfund staff will be reminded annually to keep their own details, including emergency contacts and next of kin, up to date via the Select HR portal. The annual reminder is Tearfund's 'reasonable step' but the onus is then on the staff member to ensure details are accurate and up-to-date.*

Principle 5: Personal data processed for any purpose shall be kept in a form which permits identification of individuals for no longer than is necessary for those purposes

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: 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

Personal information must be kept safe from unauthorised access and processing, and from accidental loss, damage and destruction. 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 organisation 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.

Sensitive/Special Category Personal Data

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

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

(The characteristics highlighted in bold are data that Tearfund would most commonly collect

An individual's criminal background is treated the same way as GDPR special category data under the DPA. In order to lawfully process special category data, you must identify both a lawful basis under Principle 1 **and** also identify a separate condition for processing special category data under Article 9.

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. Religious NGO exception (processing carried out in the course of our legitimate activities, with appropriate safeguards, so long as the processing relates solely to the members and former members of Tearfund with whom we have regular contact with and the personal data is not disclosed outside of Tearfund).
4. 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.

There are other conditions in Article 9 but these relate to information being necessary for the substantial public interest, reasons of occupational health or public interest in the sphere of public health or scientific/historical research purposes and it is therefore highly unlikely that Tearfund would be able to establish one of these conditions.

Other Key Issues

Personal Data Breaches

In a large organisation working globally there will be occasions whether personal data is unlawfully or accidentally 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 beneficiary consent forms 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 the data breach team (*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 the incident reporting team who will notify the data breach team 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.

Scope of GDPR

The GDPR applies to the"*processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not"* (Article 3.1).

Put in plain English this means that the GDPR applies to:

- UK nationals, EU nationals and non-EU nationals; IF
- The processing is carried out in the context of Tearfund's activities.

We have received external legal advice which indicates that as our Tearfund Country Offices do not have a separate legal entity and do share personal data for the purposes of Tearfund it is likely that the GDPR applies to this processing. The GDPR would therefore apply to beneficiary data collected in Country, personnel files of national staff etc. and that is why all staff must comply with this policy.

Oxfam has developed a Responsible Data Management toolkit, available on its website which may be useful in considering how to apply GDPR in different local contexts: https://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management

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. Tearfund's use of Google Drive amounts to a transfer of personal data to the U.S. (as this is where Google Drive's servers are located). If you send an email with personal information to a Partner in Nigeria this is a transfer of personal data to Nigeria.

The GDPR states that it is only permissible to transfer personal data outside of the EEA if:

1. There is a legal ground for the transfer (see above); and
2. There is an 'adequate level of data protection'

The EEA countries are those in the EU and Norway, Iceland & Liechtenstein. Other countries that the European Commission has decided have an adequate level of protection for personal data are Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay. The Commission has made partial finding of adequacy about Japan and Canada. Following the end of the transition period there are provisions which permit the transfer of personal data from UK to the EEA and to any countries which, as at 31 December 2020, were covered by a European Commission 'adequacy decision'. This is to be kept under review by the UK Government.

The UK government has the power to make its own 'adequacy decisions' in relation to third countries and international organisations. In the UK regime these are now known as 'adequacy regulations'.

There are also provisions which allow the continued use of any EU Standard Contractual Clauses ('SCCs'), valid as at 31 December 2020, both for existing restricted transfers and for new restricted transfers

Therefore, any staff who intend to enter new arrangements for transferring data outside the EEA and are unsure whether the transfer is adequately protected should email the legal team. Examples of when this may be required include:

- Emailing personal data to an overseas person or organisation
- Entering a contract with an overseas person or organisation, under which personal data will be transferred
- Procurement of a new supplier that will process personal data for Tearfund (and may store or process the data overseas), e.g. procurement of a new IT system or service involving personal data

See here for more details from the UK Information Commission

Exceptions to the above restrictions on international transfers, are if (a) an individual provides their informed consent, or (b) the transfer is necessary for the performance of a contract between the individual and Tearfund and is at the individual's request, then an international transfer may also be made.

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) without a contract being put in place and assurance that the third party has appropriate technical and organisational measures in place to safeguard the personal data. Legal have standard GDPR compliant data protection clauses for inclusion in your contracts. Please email the legal team 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.

Key Definitions

Anonymisation	A method of modifying Personal Data so that there is no connection of that data with an individual. If anonymisation is used so the individual cannot be identified at all then GDPR does not apply *e.g. a fully anonymous survey with no identifiable factors.* However, if the Data Controller can use or restore the anonymised information to identify individuals this is still classified as Personal Data under GDPR *e.g. a spreadsheet which contained personnel numbers only and no names would still be considered Personal Data if Tearfund is able to use the HR System together with the spreadsheet to identify individuals. This is not effective anonymisation.* *Similarly, an anonymous survey which asked individuals to include details of their team, age, location would not be effective if a specific individual could be identified using this and other information held by Tearfund.*
Categories of Data Subject	Within Tearfund we have identified the following categories of data subject about whom we may process personal data: 1. Attendees 2. Ambassadors 3. Beneficiaries 4. Contractors/Consultants 5. Employees 6. Former Employees 7. Journalists 8. Partners 9. Suppliers 10. Supporters 11. Trustees, and Board Committee Members who are not Trustees 12. Visitors 13. Volunteers
Data Breach	A breach of security that leads to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data Controller	The person (including organisations or government bodies) who determines the purposes and means or processing the personal data. Tearfund will usually act as the Data Controller.
Data Processor	A person (including organisations or government bodies) who process personal data on behalf of Tearfund.
Data Protection Clause	Wording that complies with GDPR and the Data Protection Act 2018 **must** be used in all arrangements with third parties where Personal Data is shared. Please email the legal team if you require assistance with this.

Data Protection Group	A cross-team working group who meet regularly to discuss data protection issues within Tearfund. The group may be contacted at any time with data protection queries.
Data Subject	Any living individual who is the subject of personal data held by Tearfund. This will include employees, donors, next of kin, partners, referees, supporters, volunteers and beneficiaries.
Data Subject Rights	The rights of an individual: 1. To be informed 2. Of access 3. To rectification 4. To erase 5. To restrict processing 6. To data portability 7. To object 8. In relation to automated decision making and profiling.
DPA	The UK Data Protection Act 2018, which implements UK-specific aspects of the GDPR
DPIA	A data protection impact assessment which must be used if an intended processing activity (in particular using new technologies) is likely to result in a high risk to the rights and freedoms of Data Subjects. A template DPIA can be found by staff.
Electronic Processing	Processing of Personal Data involving electronic means (i.e. emails, Google drive, databases)
GDPR	General Data Protection Regulation which came into force on 25 May 2018, replacing the Data Protection Act 1998.
ICO	The Information Commissioner's Office which is the regulatory for data protection legislation in England and Wales
Manual Processing	Processing of Personal Data entirely by people (i.e. paper records)
Personal Data	Data which relates to an identified or identifiable *living* individual. If a person can be identified directly or indirectly from the data (i.e. if there is a named individual, or an identification number such as personnel number of national insurance number, location data or other online identifiers).
Processing	Any operation which is performed on personal data. Basically any treatment of data will be treated as processing including, but not limited to: collecting, recording, organising, structuring, storing, adapting, altering, disclosing, erasing or otherwise making available.
Profiling	Any automated processing of personal data which is intended to evaluate certain aspects relating to the data subject. This would include automated analysis of an individual's work performances, personal preferences,

	behaviour, health etc
Pseudonymisation	The processing of Personal Data in such a manner that the personal data can no longer be attributed to a Data Subject without the use of additional information. This is often achieved by replacing the name or other characteristics with a pseudonym. Pseudonymised data falls within GDPR but is a safeguard to decrease the risk to the Data Subject. Please refer to the Corporate Hub for Tearfund's policy on using pseudonyms in connection with Beneficiary data.
Record of Processing Activities	A high-level, centralised record of the processing activities which Tearfund carries out.
Sensitive or Special Personal Data	Personal information which reveals something about an individuals: ● Racial or ethnic original ● Political opinion or trade union memberships ● Religious beliefs ● Physical or mental health condition ● Sexual life/sexual orientation ● Criminal background
Territorial Scope	The GDPR relates to all personal data processed by Tearfund both in relation to individuals based in the UK and individuals overseas.