DATA PROTECTION POLICY

Policy ID: HA/POL/DPP

Author: Ihsan Al-Jafri

Owner: CEO

Sign off: Ihsan Al-Jafri

Version: 2

Last updated: July 2026

Next review: End of July 2026

Data Protection Policy

1. Introduction

Human Appeal is an incorporated UK charity working across the globe to strengthen humanity's fight against poverty, social injustice and natural disaster, through the provision of immediate relief and establishment of self-sustaining development programmes. Our vision is to contribute to a just, caring and sustainable world, free of poverty. Human Appeal does this by raising money to fund immediate and long-term sustainable solutions, and empower local communities.

2. Policy Statement

Human Appeal is obliged to comply with all relevant UK and EU information legislation. This requirement to comply is devolved to all stakeholders, who may be held personally accountable for any breaches of personal data security for which they may be held responsible.

Human Appeal supports the objectives of the Data Protection Act 2018 and other legislation relating to data processing and information access, including the General Data Protection Regulation (GDPR), The Privacy and Electronic Communications Regulations (PECR), the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and the Environmental Information Regulations 2004. This policy aims to assist staff or individuals working on behalf of Human Appeal, with meeting their statutory and other obligations which covers the issues of information governance and risk.

3. Policy Objective

The policy is intended to establish and maintain the security and confidentiality of personal data,and provide a framework for maintaining the normal business activities of Human Appeal by:

3.1 Creating and maintaining within the organisation a level of awareness of the need fordata protection as an integral part of the day to day business.
3.2 Ensuring that all data users are aware of and fully comply with the relevant legislation as described in policies and fully understand their own responsibilities;
3.3 Ensuring that all data users are aware of the rights of data subjects in accessing andcorrecting their personal data under the Data Protection Act 2018;
3.4 Protecting sensitive personal data from unauthorised disclosure, unlawful processing or storing etc.;
3.5 Safeguarding the accuracy of information;
3.6 Protecting against unauthorised modification of information;
3.7 Storing, archiving and disposing of sensitive and confidential information in anappropriate manner;
3.8 Lawful use or sharing of Human Appeal information.

3.9 **Human Appeal will achieve this by ensuring that:**

- Setting up appropriate systems and controls according to Human Appeal's riskappetite.
- Ensuring the confidentiality of personal data and exempt information is assured;
- Regulatory and legislative requirements are met;
- All transmission and essential sharing of information internally or with partners, inmanual or electronic format, is properly authorised and effected within agreed sharing protocols.
- Data protection training is provided;
- All losses of personal data, actual or suspected, are reported, investigated and any resulting necessary actions taken;

- Standards, guidance and procedures are produced to support this policy.
- Processing personal information when it is absolutely necessary for organisational purposes;
- Ensuring that the least possible amount of personal data is collected, and that personal datais never processed unduly;
- Informing individuals of how their personal data is or will be used and by whom;
- Processing only pertinent and adequate personal data;
- Processing personal data in a lawful and fair manner;
- Keeping a record of the various categories of personal data processed;
- Ensuring that all personal data is kept as accurate and up-to-date as possible;
- Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes;
- Giving individuals the right of 'subject access', as well as all other individual rights pertainingto their personal data;
- Ensuring that all personal data is maintained securely;
- Transferring personal data outside of the EU only in situations where it shall be appropriatelysecured;
- Applying various statutory exemptions, where appropriate;
- Identifying personnel that are responsible and accountable for GDPR Compliance.

4. Scope

4.1 This policy applies to all employees of Human Appeal. Breaches of the GDPR policy shall be dealt with according to Human Appeal's Disciplinary Policy. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

All third parties working with or for Human Appeal who have or may have access to personal data are required to read, understand and fully comply with this policy at all times. All aforementioned third parties are required to enter into a data confidentiality agreement prior to accessing any personal data. The data protection obligations imposed by the confidentiality agreement shall be equally onerous as those to which Human Appeal has agreed to comply with. Human Appeal shall at all times have the right to audit any personal data accessed by third parties pursuant to the data sharing agreement. **Please see Appendix 1 Data Sharing Agreement**

4.2 This policy applies to all information and personal data held by Human Appeal. Information and personal data can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically. All electronic and communication devices owned, administered, controlled or sanctioned for use by Human Appeal.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Recordings.
- Photographs

- Information and data in test, training and live environments, however it is hosted.
- All staff of Human Appeal including temporary and contract staff, volunteers and third-parties accessing or using the charity's information, data and/or network.

- All donors / supporters, beneficiaries and members of the public whose personal information is held by Human Appeal in order to provide its services.
- Locations from which Human Appeal systems are accessed (including home use or other remote use). Where there are links to enable partner organisations to access Human Appeal information, prior assurance must be obtained that information security risks have been identified and suitably controlled.

5. Definition of terms

5.2 **Personal data** – is information that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number or could include other identifierssuch as an IP address or a cookie identifier, or other factors. If it is possible to identify an individualdirectly from the information you are processing, then that information may be personal data.

5.3 **Data subject** - refers to any living person who is the subject of personal data held by an organisation. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social.

5.4 **Data subject consent** - refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a specific written or oral statement or by clear, unambiguous, affirmative action and must be given freely at all times, without duress, with the data subject being properly informed.

5.2 Controllers - are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they arenot joint controllers if they are processing the same data for different purposes.

5.3 Processors - Processors act on behalf of, and only on the instructions of, the relevant controller.

5.4 Processing - refers to any action taken in relation to personal data, including but not limited to collection, adaptation or alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise.

5.5 Establishment - refers to the administrative head office of the 'data controller' in the EU, wherethe main decisions regarding the purpose of its data processing activities are made. 'Data controllers' based outside of the EU are required to appoint a representative within the jurisdictionin which they operate to act on its behalf and liaise with the relevant regulatory and supervisory authorities.

5.6 Filing system - refers to any personal data set which is accessible on the basis of certain benchmarks or norms and can be centralised, decentralised or dispersed across various locations.

5.7 Personal data breach - refers to a security breach which results in the disclosure, alteration, destruction or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully. All personal data breaches must be reported to relevant regulatory authority by the 'data controller' at all times, whereas the data subject need only be informed of a data breach when it is likely that the breach will have an adverse effect on his or her privacy or personal data.

5.8 Special categories of personal data - refers to personal data covering such matters as racial or ethnic origin, beliefs - whether religious, political or philosophical, trade union membership, biometric identification, health, sexual orientation and sex life.

5.9 Territorial scope the GDPR applies to all EU based 'data controllers' who engage in the processing of data subjects' personal data as well as to 'data controllers' located outside of the EUthat process data subjects' personal data so as to provide goods and services, or to monitor EU based data subject behaviour.

5.10 Third party - is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the controller or processor

6. Data Protection Principles

- All organisations that 'process' 'personal data' are data controllers and are required to be registered with the Information Commissioner's Office (ICO) as defined in the Digital Economy Act 2017. Human Appeal has registered with the ICO as a "data controller" that engages in processing personal information of data subjects. The Systems & Development Team will ensure that this is completed annually.
- Appointed employees of Human Appeal with managerial or supervisory responsibilitiesare responsible for ensuring that good personal data handling practices are developed, reviewed and encouraged within Human Appeal, as per their individual job descriptions. All members of Human Appeal who process personal data are responsible for ensuring compliance with data protection laws. Human Appeal provides annual GDPR Training for all employees as well as for general members of Human Appeal.
- Human Appeal will adopt a "best practice" approach at all times based on the ICO' guidelines, and, where appropriate, professional codes of practice.
- Any data controller must observe the Data Protection principles which govern the manner in which data is collected, held and processed. Human Appeal is committed to ensuring that all information held is necessary, used fairly and responsibly and in compliance with the principles as follows:

7. Processed fairly and lawfully

- Information will only be held where it is justified to do so and processing may be carried out where one of the following conditions has been met as per Human Appeal's Privacy Policy /Notice (https://humanappeal.org.uk/privacy), namely where:-
- The individual has given their consent to the processing
- The processing is necessary for the performance of a contract that was/will be concluded with the data subject
- The processing is required as part of a legal obligation
- The processing is necessary to protect the vital interests of an individual (protecting someone's life).
- The processing is necessary in order to pursue our legitimate interests

7.1 Processed only for the specified lawful purposes and not processed in any way incompatible with those purposes

Human Appeal is one data controller. Personal data held by Human Appeal can be used within Human Appeal as permitted by the charity's Privacy Policy / Notice to carry out the functions of the charity. This however must be on a 'need to know' basis and appropriate security and access controls implemented where necessary so only staff that need access tothe personal data are allowed it.

- All requests for information from other public bodies, including the police, are tobe in writing except in an emergency.
- When receiving requests for personal data, clarification must be obtained as to who the requesting party is, the reason why information is requested and if there is authority to give the personal data. However, additional information might be required on a case by case basis, depending on the particular details of the request.
- Where consent is used as the legal basis for processing personal data, Human Appeal will ensure that consent is unambiguous, specific, freely given and an affirmative action or statement, with an audit trail to demonstrate consent was gained. Consent must be explicit.
- If Human Appeal plan to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, we will ensure the new use is fair, lawful and transparent. We will require, therefore your new consent if this was the legal basis we relied on for the initial processing. If other grounds were used, according to Art. 6 (4) GDPR, we will make sure the new purpose is compatible with the previous one, by analysing the context, the link between the two of them, possible consequences, etc.

7.2 Adequate, relevant and not excessive in relation to the purpose(s) for which personal data is processed

Human Appeal will ensure that the personal data we are processing is sufficient to properly fulfil our stated purpose, relevant to that purpose and we will only hold the minimum personal information necessary to enable us to perform our functions.

7.3 Accurate and kept up-to-date

All efforts will be made to ensure that information is periodically assessed for accuracy;and is kept up to date. If Human Appeal discovers that the personal data is incorrect or misleading, we will take reasonable steps to correct it as soon as possible. We do also encourage data subjects to exercise their right to rectification any time they acknowledge data about them is inaccurate.

7.4 Processed no longer than is necessary for the purpose(s)

Information must be erased securely once it is no longer required and kept in line with Human Appeal's Retention and Disposal Schedule.

Human Appeal will not retain personal data for longer than is necessary and once an employee has left Human Appeal, it may no longer be necessary for Human Appeal to retain all of the personal data held in relation to that individual. Some data will be kept longer than others, in line with Human Appeal's data Retention and Disposal Schedule.

7.5 Processed in accordance with the rights of the data subject

Human Appeal recognise the rights given to people under the General Data ProtectionRegulation (Articles 12-22).

7.6 Protected by appropriate and organisational measures

Human Appeal has systems in place to keep information secure. Staff must refer to theInformation Security Policy

7.6.1 Transfer of personal data to non-EU member states must show the necessary organisational and technical measures have been put in place to protect data e.g. Adequacy assessment, EU modelclauses.

7.6.2Access to personal data shall only be granted to those who need it and only according to the principles of Human Appeal's Information Security Policy.

7.6.3 Before being granted access to any organisational data, all staff of Human Appeal must understand the Information Security Policy.

7.6.4 Computer screens and terminals must not be visible to anyone other than staff of Human Appeal with the requisite authorisation.

7.6.5 No manual records may be accessed by unauthorised employees of Human Appeal and may not be removed from the business premises in the absence of explicit written authorisation.

7.6.6 Manual records must be removed from secured archiving when access is no longer needed on a day-to-day basis. All deletion of personal data must be carried out in accordance with Human Appeal's Retention and Disposal Schedule Manual records which have passed their retention date must be shredded and disposed of as 'confidential waste' and any removable or portable computer media such as hard drives or USB sticks must be destroyed as per Human Appeal's Information Security Policy prior to disposal.

7.6.7 Personal data that is processed 'off-site' must be processed by authorised Human Appeal staff,due to the increased risk of its loss, damage or theft.

7.6 Consent

7.6.3 The individual has given clear, specific, explicit consent for Human Appeal to process their personal data for a specific purpose.

7.6.4 Consent is freely given and should never be given under duress, when the data subject is inan unfit state of mind or provided on the basis of misleading or false information.

7.6.5 Provided either in a statement or by unambiguous affirmative action.

7.6.6 Demonstrated by active communication between the data controller and the data subject and must never be inferred or implied by omission or a lack of response to communication.

7.6.7 Consent requires a positive opt-in for electronic mediums.

7.6.8 Human Appeal must name any third party controllers who will rely on the consent.

7.6.9 Human Appeal must make it easy for people to withdraw consent and tell them how.

7.6.10 Human Appeal must keep evidence of consent – who, when, how, and what you told people. In addition, consent must be kept under review.

7.7.1 Withdrawal of consent

- Withdrawal of consent is defined as any indication on the part of the data subject that he orshe withdraws consent for the processing of their personal data. Withdrawal of consent must be specific and without ambiguity and shall be provided by the data subject either by way of a statement or through clear, affirmative action on his or her part (such as ticking the opt-out box from our website).

- Withdrawal of consent by the data subject covers all processing activities carried out for a specific purpose or purposes, for which that data subject provided consent in the first place.Withdrawal of consent shall not make unlawful any processing of personal data engaged in by Human Appeal prior to the withdrawal of consent.

- As a data controller, Human Appeal is responsible for administering the withdrawal of consent on the part of the data subject, under the oversight of the Donor Care Team and System's and Development Team. Withdrawal of consent is indicated via emailing customercare@humanappeal.org.uk and telephoning the Donor Care Team and Human Appeal must be able to demonstrate that the data subject has withdrawn consent, by producing the email and / or evidence of the telephone call, if required. If Human Appeal was processing the data for multiple purposes, Human Appeal must be able to show that consent has been withdrawn for all purposes.

8. Contract

The processing is necessary for a contract Human Appeal has with the data subject, or because we havebeen asked to take specific steps before entering into a contract.

9. Legal obligation

The processing is necessary for you to comply with the law (not including contractual obligations).

10. Vital interests

The processing is necessary to protect someone's life.

11. Public task

The processing is necessary for Human Appeal to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

12. Legitimate interest

The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

13. Special category personal data and data about offences and criminal convictions

There are additional requirements placed upon the data controller where the holding of 'special category personal data' is concerned. The definition of 'sensitive personal data' isdata in respect of: -

- racial or ethnic origin
- political affiliations
- religious belief
- union membership
- physical/mental health
- sexual life
- Biometric
- Genetic

If disclosing special category personal data (even if required to do so by law) consent of the data subject must be obtained unless a specific exemption applies.

Additionally, if special category personal data is held, security measures for holding such data will need to be considerably higher than that for other service areas holding less sensitive data.
Moreover, data relating to criminal convictions and offences or related security measures must benefit from additional data protection safeguards, compared to personal data. Their regime resembles the one for special categories of personal data.

14. Subject Access Requests (SAR) and other data subject rights

Under the Data Protection Act 2018/ General Data Protection Regulation, data subjects have the right to know what information is held about them. This is known as a SubjectAccess Request (SAR). **See the Data Subject Access Request Handling and Data SubjectRights Policy for more information.**

15. Exemptions

The rights of data subjects are subject to certain statutory exemptions. Human Appeal willdisclose personal information, without the data subject's consent in accordance with the Data Protection Act 2018. This includes but is not limited to: -

- On production of a court order for disclosure.
- In the interests of assessing or collecting a tax duty.
- In the interests of crime prevention and detection, which includes theapprehension and prosecution of offenders.
- In the interests of discharging various regulatory functions.
- Where information is required for research purposes providing such data is general and does not cause damage or distress to the data subject.
- In the interests of protecting the vital interests of the data subject e.g. only in a life ordeath situation.
- In the interests of safeguarding national security.

16. Privacy Notices / Policy

Under the Data Protection Act 2018, data subjects have the right to know what Human Appeal will use their personal data for. This is called a Privacy Notice / Policy. It should be added on all Human Appeal forms, where personal data is collected, or on the charity's web based forms. Human Appeal will publish its Privacy Notice / Policy on the website and update and inform people of the changes periodically.

17. Use of personal data in marketing

- Human Appeal will comply with the Privacy and Electronic Communications Regulations (PECR).
- Personal data collected by Human Appeal will only be used for marketing purposes where customers have been told this will happen via a Privacy Notice / Policy or where customers have opted-in (consented) to receive such information.
- All emails and SMS's sent to customers for marketing purposes will include a 'how to opt-out' message.
- Post and telephone calls do not require a positive opt in due to the use of legitimate interest, but we must inform the individual of their right to opt out.
- Databases used by Human Appeal for marketing purposes will be 'cleansed' at least every two years to determine customers still wish to receive marketing information and to verify the accuracy of the data.

18. Complaints

All complaints about Human Appeal's processing of personal data may be lodged by a data subject directly with the Donor Care Team by calling the dedicated complaints line on 0161 536 2020 or emailing customercare@humanappeal.org.uk, providing details of the complaint. The data subject must be provided with a Privacy Policy / Notice at this stage. All complaints in relation to how a complaint has been handled and any appeals following the submission of a complaint shall be dealt with by the Donor Care Team.

However, you have the right to address to the ICO in order to express your dissatisfaction with how we handled your requests/complaints regarding data protection.

19. Accountability and governance

According to the GDPR accountability principle, the data controller is responsible both for ensuring overall compliance with the GDPR and for demonstrating that each of its processes are compliant with the GDPR requirements. To this extent data controllers are required to:

- Maintain all relevant documentation regarding its processes and operations;
- Implement proportionate security measures;
- Carry out Data Protection by Design and Default and Data Protection Impact Assessments (DPIAs). **See Appendix 2 Data Protection by Design and Default and Data Protection Impact Assessments (DPIAs).**

20. Information sharing

20.1 Data processing by external suppliers

- Human Appeal shall only engage with third party data processors that are able to provide security, including technical, physical or organisational security, to all personal data that theyprocess on Human Appeal's behalf.
- Before entering into any agreement with a third-party data processor, Human Appeal; must carry out an information security risk assessment. Taking into consideration the basis of thenature of the personal data to be processed and the specific circumstances of the data processing, the Systems and Development Team may deem it necessary that an additional audit of the third-party data processor's security arrangements may be carried out before entering into any agreement.
- Human Appeal shall only engage a third-party processor pursuant to a written contract which expressly sets out the service to be provided. The third-party processor is also required to provide suitable security for the personal data to be processed, which must alsobe confirmed in the written contract ("the data processing agreement"). **See Appendix 1 Data Sharing Agreement.**

The GDPR sets out what needs to be included in the data processing agreement:

- the subject matter of the processing;
- the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data involved;
- the categories of data subject;
- the controller's obligations and rights.Human Appeal is required to carry out regular audits of the third-party data processor's security arrangements throughout the duration of the contract, when the third party hasaccess to personal data held by Human Appeal.
- The data processing contract must contain a clause preventing third-party data processors from hiring subcontractors for the processing of personal data in the absence of express, written approval by Human Appeal.

- Human Appeal will only approve contracts with second-tier data processors, if the subcontractors of the third-party data processor agree to provide the same level of security and protection to the rights and freedoms of the data subject as those afforded by Human Appeal. In addition, the contract between the third-party data processor and the second-tierdata processors must contain a clause requiring that all personal data will be either destroyed or returned to Human Appeal upon the termination of the contract.
- Managers responsible for procurement of services must ensure that a Data Protection by Design and Default and Data Protection Impact Assessment is carried out (**See Appendix 2 Data Protection by Design and Default and Data Protection Impact Assessments (DPIAs),** potential bidders are compliant with data protection requirements and the necessary data processing agreements are put in place when contracts are awarded. **See Appendix 1 Data Sharing Agreement**
- Managers responsible for services which share personal data with outside partnersand agencies on a regular, organised basis must ensure that a written data sharing agreement is in place. **See Appendix 1 Data Sharing Agreement**
- The data sharing agreement must be signed by the relevant departmental director for single service agreements and the Chief Operating Officer for cross service agreements.

21. Documentation

- The GDPR contains explicit provisions about documenting our processing activities.
- We must maintain records on several things such as processing purposes, data sharing and retention.
- We may be required to make the records available to the ICO on request.
- Records must be kept up to date and reflect our current processing activities.

See Appendix 3 Human Appeal's documentation record (in progress)

22. Data Protection by Design and Default and Data Protection Impact Assessments

- It is vital that Human Appeal is aware of all risks associated with personal data processing and it is via its risk assessment process that Human Appeal is able to assess the level of risk. Human Appeal is also required to carry out assessments of the personal data processing undertaken by other organisations on its behalf and to manage any identified risks, so as tomitigate the likelihood of potential non-compliance with this policy.
- The General Data Protection Regulation requires Human Appeal to implement appropriate technical and organisational measures:
- which are designed to implement the data protection principles; and
- for ensuring that, by default, only the minimum quantity of personal data are processed for each purpose.

These measures are referred to as Data Protection by Design and Default.

- The GDPR also requires data protection impact assessments (DPIAs) to be carried out on processing activities which are likely to result in a high risk to the rights and freedoms of individuals. A DPIA helps Human Appeal to identify and minimise any data protection risks involved with a project or initiative. They also play a key role in implementing data protection by design and default.

- These legal obligations apply to the processing of personal data by Human Appeal and all aspects of designing appropriate privacy protection into Human Appeal's activities includingproposals, new developments and/or significant changes that involve the access, potential access or processing of personal data. High risk initiatives relate to processing which affects the rights and freedoms of data subjects.

- Activities include, for example:

    - Projects involving physical infrastructure where personal data may be processed;
    - Non-IT Services developed or acquired software and/or cloud services;
    - New IT Services developed or acquired systems, software and/or services and/or;
    - Changes to existing IT systems, software and/or services;
    - Policy change.

- Compliance is mandatory for staff involved in purchasing or designing new physical infrastructure, or updated systems or processes which require the processing of personal data.

- It is not permitted to procure software and/or services which will process personal data without adherence to data protection by design and default and data protection impact assessments.

- Anyone considering commissioning or changing personal data processing systems must complete the data protection privacy by design and default and privacy impact assessment during discovery or feasibility. A decision to introduce a new or updated Human Appeal system that processes personal data must not be made without completing the data protection privacy by design and default and privacy impact assessment. Projects and change initiatives must have a nominated project manager who is responsible for ensuring that this is followed.

The project manager must:

- assign an agreed information security classification to the proposed Human Appeal process, IT system, software and/or service;
- submit and receive approval from the Board of Directors for their personal data processing activity;
- obtain the required sign-off from the key stakeholders; and
- ensure that the data protection principles listed in this policy are met.
- Managers must submit a Data Protection Impact Assessment (DPIA) to the Board of Directors for all new projects, procurement, commissioning or services they undertake at the start of any such proceeding.
- If the outcome of a DPIA points to a high risk that Human Appeal's intended personal data processing could result in distress and/or may cause damage to data subjects, the Board of Directors will then decide whether Human Appeal ought to proceed. In turn, Human Appeal may escalate the matter to the regulatory authority if significant concerns have been identified. It is the responsibility of the Project Manager and the Board of Directors to

ensure that appropriate controls are in place to ensure that the risk level associated with personal data processing is kept to an acceptable level, as per the requirements of the GDPR.

(**See Appendix 2 Data Protection by Design and Default and Data Protection Impact Assessments (DPIAs)**

23. Information security

- Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Human Appeal which must be managed with care. All information has a value to the organisation. However, not all of this information has an equal value or requires the same level of protection. Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use. Formal procedures must control how access to information is granted andhow such access is changed.
- Personal data will only be kept for as long as the service provided to the data subjectis in existence or is as required by law. If there is no legal requirement to keep the records, they will be removed / erased as soon as is practicable in line with Human

Appeal's Retention and Disposal Schedule.

- Personal data should be handled in accordance with the Human Appeal's Information Security Policies.
- In the event that employees take home manual or computerised files containing data, it is the employee's responsibility to ensure that such data is made secure.
- All employees of Human Appeal are personally responsible for keeping secure any personal data held by Human Appeal for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless Human Appeal has provided expressauthorisation and has entered into a data processing agreement with the third party.
- Human Appeal must take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the Police.

24. Encryption and passwords to online services

- Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.
- A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least eight characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Do not use the 'remember password' function.
- Never write your passwords down or store them where they are open to be viewed by anyone.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password for systems inside and outside of work.
- Human Appeal currently adopt a strong password policy with multi factor authentication.
- Microsoft Office 365 UK and EU offices have multi factor authentication available.
- All Human Appeal devices across the UK and EU Offices have Windows Bitlocker encryption installation.
- Microsoft Enterprise Mobility Security Suite has been installed to protect our Office 365 Cloud Environment with additional security features, including advanced threat protection (ATP) and Azure Information Protection (AIP) across our UK and EU Offices.
- Advanced threat protection (ATP) is installed across all Human Appeal devices to scan all emails and block any malicious attachments or URLs within email correspondence, emails are blocked from countries with known threats and the latest enterprise anti-virus protection is installed.
- Azure Information Protection (AIP) is currently in progress to help Human Appeal label, classify and protect corporate emails and documentation on Human Appeal devices, whilst on the move.
- User access rights are reviewed at regular intervals by the Systems and Development Team to ensure that the appropriate rights are still allocated.

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to the organisations systems by:

- Following the Password Policy Statements outlined above.
- Ensuring that any PC / laptop they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords, this includes not writing passwords down or saving them electronically elsewhere.
- Informing the System and Development Team of any changes to their role and access requirements.
- The use of USB's and portable devices on Human Appeal owned devices can seriously compromise the security of the network, therefore they are blocked. The normal operation of the network must not be interfered with. Specific approval must be obtained from IT before connecting any portable equipment to Human Appeal's network. An encrypted USB

or portable device will be provided on a case by case basis by the Systems and Development Team.

25. Disposal of removable storage media

It is the responsibility of Human Appeal to manage the secure disposal of all storage mediathat is no longer required. All owners of removable storage media are responsible for disposing of removable storage media utilising the below procedure:

1. Hard disks must be formatted and cleaned of all data and software before beingreused for another Human Appeal owned device.
2. PC hard drives that are no longer needed are locked in a safe space until we sourcea hard drive shredding service for the safe disposal and destruction of our hard drives.
3. Removable storage media devices that contain confidential information must be destroyed only after a risk assessment has been carried out and must never be reused. Removable storage media devices no longer needed are internally crushedand disposed of by the Systems and Development Team.
4. Removable storage media devices that contain confidential information are cleanedof all data before being reused in another Human Appeal owned device.
5. Documents that contain confidential and restricted information should be shredded by their owners prior to being destroyed. Shredders are located on the ground, first and second floors at Human Appeal Head Office and available across our other UK and EU offices. The shredded waste must be removed by an approved service provider, Shred – It.

26. Personal data breach

A personal data breach occurs against the following events:

- A personal data breach pursuant to Article 33 'Notification of a personal databreach to the supervisory authority'
- A personal data breach pursuant to Article 34 'Communication of a personal databreach to the data subject' of the GDPR.

There is a distinction under the GDPR between a 'data controller' and a 'data processor'. This is because different organisations involved in processing personal data have varying degrees of responsibility. An organisation can be a data controller or a data processor, depending on its rights and obligations.

All users, including temporary employees of Human Appeal and third parties, and HumanAppeal must be aware of the following procedure and are required to follow it should a personal data breach incident occur.

26.1 Breach Notification – data processor to data controller

All personal data breaches by Human Appeal must be notified to the appropriate datacontroller immediately. The Systems and Development Team must record the communication of the breach in line with our Serious Incident Policy, stating how the notification was made (whether by email, telephone call etc.), to whom and how the confirmation of receipt was provided.

26.2 Data controller to supervisory authority

If a risk is considered likely to result in a risk to the rights and freedoms of natural persons, Human Appeal is required to report the personal data breach tothe supervisory authority immediately and in any event, no later than 72 hours after they have been aware about the breach. If the notification is made outside of the 72-hour window, Human Appeal is required to provide reasons for the delay.

Human Appeal is required to provide the following to the supervisory authority:

26.2.1 A description of the nature of the personal data breach;
26.2.2 The categories of personal data that have been affected by the breach;
26.2.3 The number, which may be approximated if necessary, of data subjects affected by the breach;
26.2.4 The number, which may be approximated if necessary, of personal data records affected by the breach;
26.2.5 The name and contact details of the responsible officer;
26.2.6 The likely outcomes of the personal data breach;
26.2.7 Any measures taken by Human Appeal to address and/or mitigate the breach; and
26.2.8 All other information regarding the data breach.

26.3 Data controller to data subject

If it is likely that there will be a high risk to the affected data subject's rights and freedomsunder the GDPR, Human Appeal is required to provide immediate notification to the relevant data subjects. The notification to the data subject must be made in clear and plainlanguage and must include the following:

26.3.1 A description of the nature of the personal data breach;
26.3.2 The categories of personal data that have been affected by the breach;
26.3.3 The number, which may be approximated if necessary, of data subjects affected by the breach;
26.3.4 The number, which may be approximated if necessary, of personal data records affected by the breach;
26.3.5 The name and contact details of the DPO;
26.3.6 The likely outcomes of the personal data breach;
26.3.7 Any measures taken by Human Appeal to address and/or mitigate the breach; and
26.3.8 All other information regarding the data breach.

Human Appeal must use appropriate measures, such as encryption, to ensure that all personal data is secure and cannot be accessed by those without the requisite authority. Human Appeal must also take subsequent measures to ensure that the risk to the rights and freedoms of the data subject are no longer an issue. If notification would require Human Appeal to implement a disproportionate amount of effort, a public communication or other similar measure may suffice, so long as all data subjects are effectively informed. Itis possible that the supervisory authority may require Human Appeal to communicate the personal data breach to the data subject, should there be an element of high risk involved.

27. Duties and Responsibilities

Human Appeal is registered as a data controller. The Data Protection Officer is responsible for monitoring the fair and lawful processing of personal and/or sensitive personal information, whilst the Chief Executive Officer might be held liable on behalf of Human Appeal as a whole, in cases of non-compliance.

However, it is the responsibility of all employees and elected members to handle information and data correctly. As an individual representing, working for, or on behalf of, Human Appeal it is essential that you understand and abide by the following:

- Organisational and/or departmental policy, procedures and guidance on the collection and use of personal/sensitive information and data;
- Only process personal/sensitive personal information in accordance with the data protection legislation
- Be clear why you are using personal/sensitive information;
- Tell people why their information is being collected, what it will be used for and how it will be managed from collection to destruction;
- Collect only the minimum amount of personal/sensitive data needed, and use it only for thepurposes specified or in line with legal requirements;
- Ensure the personal/sensitive information is input correctly and accurately
- Ensure personal/sensitive information is destroyed / erased securely when it is no longer required;
- If you receive a request from an individual for information held by Human Appeal about them please forward the request to the Donor Care Team if they are about a donor / supporter customercare@humanappeal.org.uk, the Programmes Team if they are about a beneficiary and the People & Culture Team if they are regarding current, former or prospective employees.
- Handle all personal information in accordance with the charity's security policies and procedures;
- Do not send personal/sensitive personal information outside of the EU without referring to the Systems and Development Team.
- Understand and undertake the mandatory training relating to Information Security and DataProtection in a timely manner.
- **Human Appeal will ensure that;**
- Employee training needs are identified and training provided to ensure that those managingand handling personal/sensitive information understand their responsibilities and follow good practice.
- All current and future users of Human Appeal information are instructed in their data protection responsibilities and have access to and have read the data protection and information security guidance.
- Anyone who makes a request regarding their personal information to the charity is responded to.
- Any breach of this policy, real or suspected, is reported as required in the Serious Incident Reporting Policy.
- Any breach investigation is undertaken as a priority and resources are committed to any investigation in order to conclude the investigation in a timely manner.

- They will develop, implement and maintain the corporate data protection and relevant information governance and risk policies, procedures and standards that underpin the effective and efficient creation, management, dissemination and use of personal data;
- Provision of data protection support and advice to staff and managers.
- The production, review and maintenance of data protection policies and their communication to the whole of the charity;
- Provision of professional guidance on all matters relating to data protection.
- Oversight management of all information data protection breaches and suspected breach investigations.
- Provision, via the intranet, of data protection awareness briefing materials and, through online and offline training.
- Oversight management of all information requests under the Data Protection Act 2018 and Environmental Information Regulations 2004, and any subsequent appeals and complaints to the ICOs Office;
- Management and recording of information sharing processes and agreements;

28. Compliance with the legislation

Human Appeal recognises the need to make the contents of this policy known and ensurecompliance by every employee.

All staff will be mandatorily trained in basic data protection principles and made aware of this policy. Data protection awareness will be included in the induction process. Training updates for staff will also be provided annually. The Audit and Compliance Team will notify staff of changes to data protection legislation, how these changes will affect them, when they will occur and what is needed to stay within the law.

Human Appeal must pay the annual data protection fee to the ICO's Office and notify the ICO's Office annually what personal data it intends to process. An internal review of these notification requirements will be undertaken by the Board of Directors annually. The ICO will be informed ofany changes required to the notification.

Human Appeal expects all employees to comply fully with this policy, the data protection principles and other information legislation and Human Appeal's procedures. Disciplinary actionmay be taken against any Human Appeal employee who knowingly breaches any instructions contained in, or following from this policy.

Individual employees are affected in the same way as Human Appeal as a whole. Anyonecontravening the Data Protection Act 2018 could be held personally liable and face courtproceedings for certain offences which may result in a fine and / or a criminal record.

Service areas which are causing concern over data protection compliance will be forwarded to Internal Audit for further investigation.

29. Policy Review

This will be reviewed on a bi-annual basis to ensure continuing appropriateness.

Appendix 1

Data Sharing Agreement

STANDARD DEFINITIONS

Party: a Party to this Agreement

Agreement: this contract;

Law: means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of arelevant court of law, or directives or requirements with which the Contractor is bound to comply;

Contractor Personnel: means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-Contractor engaged in the performance of its obligations under this Agreement **]**

GDPR CLAUSE DEFINITIONS:

Data Protection Legislation: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy;

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer and Data Protection Impact Assessment take the meaning given in the GDPR.

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach**.**

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018: Data Protection Act 2018

GDPR: the General Data Protection Regulation (for EU data subjects – *Regulation (EU) 2016/679, for UK data subjects – the UK General Data Protection Regulation as EU retained legislation*)

LED: Law Enforcement Directive (*Directive (EU) 2016/680*)

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.

Sub-processor: any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement

1. DATA PROTECTION

1.1 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor. The only processing that the

Contractor is authorised to do is listed in Schedule [X] by the Customer and may not be determined by the Contractor.

1.2 The Contractor shall notify the Customer immediately if it considers that any of the Customer'sinstructions infringe the Data Protection Legislation.

1.3 The Contractor shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistancemay, at the discretion of the Customer, include:

(a) a systematic description of the envisaged processing operations and the purpose ofthe processing;
(b) an assessment of the necessity and proportionality of the processing operations inrelation to the Services;
(c) an assessment of the risks to the rights and freedoms of Data Subjects; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule [X], unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Customer before processing the Personal Data unless prohibitedby Law;

(b) ensure that it has in place Protective Measures, as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Contractor Personnel do not process Personal Data except in accordancewith this Agreement (and in particular Schedule X);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure thatthey:

(A) are aware of and comply with the Contractor's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of theCustomer has been obtained and the following conditions are fulfilled:

(i) the Customer or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LEDArticle 37) as determined by the Customer;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Datathat is transferred (or, if it is not so bound, uses its best endeavours to assistthe customer in meeting its obligations); and

(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the Agreement unless the Contractoris required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, the Contractor shall notify the Customer immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);
(b) receives a request to rectify, block or erase any Personal Data;
(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
(f) becomes aware of a Data Loss Event.

1.6 The Contractor's obligation to notify under clause 1.5 shall include the provision of further information to the Customer in phases, as details become available.

1.7 Taking into account the nature of the processing, the Contractor shall provide the Customer with full assistance in relation to either party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 (and insofar as possiblewithin the timescales reasonably required by the Customer) including by promptly providing:

(a) the Customer with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set outin the Data Protection Legislation;

(c) the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Customer following any Data Loss Event;

(e) assistance as requested by the Customer with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office.

1.8 The Contractor shall maintain complete and accurate records and information to demonstrateits compliance with this clause. This requirement does not apply where the Contractoremploys fewer than 250 staff, unless:

(a) the Customer determines that the processing is not occasional;

(b) the Customer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(c) the Customer determines that the processing is likely to result in a risk to the rightsand freedoms of Data Subjects.

1.9 The Contractor shall allow for audits of its Data Processing activity by the Customer or the Customer's designated auditor The Customer is entitled, on giving at least three days' notice to the Contractor, to inspect or appoint representatives to inspect all facilities, equipment, documents and electronic data relating to the processing of Personal Data under this Agreement by the Contractor. The requirement to give notification in advance will not apply if the Customer believes that the Contractor is in breach of any of its obligations under this Agreement. The Contractor shall designate a data protection officer if required by the Data Protection Legislation.

1.10 Before allowing any Sub-processor to process any Personal Data related to this Agreement,the Contractor must:

(a) notify the Customer in writing of the intended Sub-processor and processing;
(b) obtain the written consent of the Customer;
(c) enter into a written agreement with the Sub-processor which give effect to the termsset out in this clause [X] such that they apply to the Sub-processor; and
(d) provide the Customer with such information regarding the Sub-processor as theCustomer may reasonably require.

1.11 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

1.12 The Contractor may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.13 The parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Contractor amendthis agreement to ensure that it complies with any guidance issued by the Information Commissioner's Officer.

1.14 The Contractor shall undertake all of the above processing activities at its own expense and at no extra cost to the Customer.

1.15 The Customer retention and disposal schedule as provided will be followed by the Contractor where appropriate and relevant; no decisions on retention or disposal are to be made by the Contractor unless it is part of detailed Processing under this Agreement.

1.16 The Contractor shall without undue delay inform the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Contractor will make regular backups of the Personal Data and will restore such Personal Data at its own expense.

Schedule of Processing, Personal Data and Data Subjects

Schedule [X] Processing, Personal Data and Data Subjects

1. The Contractor shall comply with any further written instructions with respect to processing by the Customer.

2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	
Duration of the processing	
Nature and purposes of the processing	
Type of Personal Data	
Categories of Data Subject	
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law topreserve that type of data	
Signatories	_____(signed) _____(name) _____(name of company)

	_____(address) _____ _____ _____ (position) _____ (date)

Appendix 2

Data Protection by Design and Default and Data Protection Impact Assessment Form

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA

Step 2: Describe the processing:

Describe the nature of the processing: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? Add a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: What do you want to achieve? What is the intended effect on individuals? What are the benefitsof the processing for you, and more broadly?

Step 3: Consultation process:

Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your

processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality:

Describe compliance and proportionality measures, in particular: What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks:

Describe the source of risk and nature of potential impact on individuals	Likelihood of harm (Remote, possible or probable)	Severity of harm (Minimal, significant or severe)	Overall risk (Low, medium or high)

Step 6: Identify measures to reduce risk:

Risk	Options to reduce or eliminate risk	Effect on risk (Eliminated, reduced or accepted)	Residual risk (Low, medium or high)	Measure approved (Yes/no)