HUMAN RELIEF
MISSION
المـواسـات

Data Protection Policy

Policy Name	Data Protection Policy
Policy Number	HRM-DPP

	Print Name	**Role**	**Signature**
Quality Reviewed By	Mr. Siraj Mudjahed Mr. Kashif Rehman Mr. Aziz Ul Haq Mujahid	SMT SMT ABM	S.M. K.R. A.M.
Reviewed and Approved By (BoT*) & (SMT)	Mr. Sami Ul-Haq Mujahid Dr. Salman Momin Mr. Khalid Habib Mr. Anwarlhaq Mudjahed	BoT BoT BoT SMT	S.M. S.M. K.H. A.M.

Policy Owners	HRM Compliance Team
Key Responsibilities	- Chairman - Trustees - Managers - Staff and Volunteers

1. Introduction

Human Relief Mission (HRM) recognises the fundamental importance of protecting the privacy and confidentiality of personal information. As a non-profit organisation dedicated to humanitarian efforts, HRM is committed to upholding the highest standards in data protection in accordance with the laws and regulations of the United Kingdom. This Data Protection Policy reflects our dedication to ensuring the responsible and transparent handling of personal data collected in the course of our operations.

In an era where information is a valuable asset, HRM acknowledges the need for robust measures to safeguard the personal information entrusted to us by employees, volunteers, donors, partners, and other individuals associated with our mission. This policy serves as a guide for our staff, volunteers, and senior management to understand the principles and practices that govern the collection, processing, storage, and protection of personal data within HRM.

The importance of data protection is not only a legal requirement but also integral to maintaining trust and confidence among our donors and partners. HRM is committed to treating personal data with the utmost respect and ensuring that it is handled with the highest standards of integrity and security. By adhering to this policy, HRM aims to demonstrate its unwavering dedication to respecting individual privacy rights while fulfilling its humanitarian mission.

This policy outlines the principles that underpin our data protection practices, emphasising transparency, fairness, and accountability. We encourage all individuals associated with HRM to familiarise themselves with this policy and actively participate in promoting a culture of data protection within our organisation.

As part of our commitment to continuous improvement, this policy will be regularly reviewed and updated to reflect changes in legislation, technology, and organisational practices. HRM is dedicated to staying at the forefront of data protection, ensuring that our policies and practices evolve in tandem with the dynamic landscape of information security.

Through the implementation of this Data Protection Policy, HRM reaffirms its pledge to be a responsible steward of personal information, respecting the rights of individuals and fulfilling its humanitarian objectives with the highest ethical standards.

2. Scope

This Data Protection Policy applies comprehensively to all personal data processed by Human Relief Mission (HRM), irrespective of the format in which it is collected or stored. The scope of this policy extends to all individuals whose personal data is processed by HRM, including but

not limited to employees, volunteers, donors, partners, and any other individuals with whom HRM engages.

2.1 Types of Personal Data Covered

The personal data covered by this policy includes, but is not limited to, names, addresses, contact details, financial information, identification numbers, and any other information that can be directly or indirectly associated with an individual.

2.2 Data Processing Contexts

This policy governs the processing of personal data in all contexts within HRM, whether it be in the course of administrative tasks, fundraising activities, program implementation, recruitment processes, or any other organisational function. It applies to personal data collected through HRM's website, mobile applications, paper forms, email communications, and any other means of data collection.

2.3 Inclusion of Third Parties

Where HRM engages third-party processors to handle personal data on its behalf, those entities are contractually bound to comply with this Data Protection Policy and the relevant data protection laws and regulations.

2.4 International Application

While HRM is based in the United Kingdom, the scope of this policy extends to the processing of personal data internationally if HRM engages in activities or collaborations that involve the transfer of personal data outside the United Kingdom. In such cases, HRM is committed to ensuring that international data transfers comply with applicable data protection laws and regulations.

By establishing a broad and inclusive scope, HRM aims to ensure that all individuals associated with the organisation understand the importance of protecting personal data in various organisational contexts and that the principles outlined in this policy apply consistently across different functions and activities.

3. Principles of Data Protection

Human Relief Mission (HRM) is dedicated to upholding the following principles in the collection, processing, and management of personal data:

3.1 Lawfulness, Fairness, and Transparency

HRM is committed to processing personal data lawfully, ensuring fairness in its processing activities, and maintaining transparency with individuals about how their data

will be used. All data processing activities will be guided by a legitimate basis as defined by applicable data protection laws.

3.2 Purpose Limitation
HRM will collect personal data for specific, explicit, and legitimate purposes and will not process it in ways that are incompatible with these purposes. The organisation will communicate the intended purpose of data collection to individuals and will not use the data for any purpose other than what was initially disclosed.

3.3 Data Minimisation
HRM will only collect and process personal data that is necessary for the intended purpose. Unnecessary or excessive data will not be collected, and efforts will be made to ensure that the data collected is relevant, adequate, and limited to what is essential for the stated purpose.

3.4 Accuracy
HRM recognises the importance of maintaining accurate and up-to-date personal data. The organisation will take reasonable steps to ensure that the data it processes is accurate, and individuals have the right to request corrections to their data.

3.5 Storage Limitation
HRM will retain personal data only for as long as necessary to fulfil the purposes for which it was collected. Regular reviews of stored data will be conducted to identify and securely dispose of data that is no longer required.

3.6 Integrity and Confidentiality
HRM is committed to processing personal data in a manner that ensures its security, integrity, and confidentiality. Appropriate technical and organisational measures will be implemented to protect against unauthorised or unlawful processing and to prevent accidental loss, destruction, or damage to personal data.

These principles guide HRM in creating a data protection culture that values individual privacy, promotes responsible data stewardship, and ensures compliance with relevant data protection laws and regulations. Employees and volunteers are expected to adhere to these principles in their day-to-day activities involving personal data.

4. Data Collection and Processing
HRM will inform individuals about the purpose and legal basis for collecting and processing their personal data. HRM will not use personal data for purposes other than those for which it was collected without obtaining explicit consent, unless required by law.

4.1 Collection of Personal Data

HRM collects personal data through transparent and lawful means, clearly communicating the purpose of the data collection to the individuals involved. Whether it is through online forms, physical documents, telephone conversations, or other channels, HRM ensures that individuals are informed about the nature of the data being collected, the purposes for which it will be processed, and any third parties involved in the processing.

4.2 Legal Basis for Processing

All data processing activities carried out by HRM are founded on a valid legal basis as defined by applicable data protection laws. Whether it is the necessity of processing for the performance of a contract, compliance with a legal obligation, protection of vital interests, consent, the performance of a task carried out in the public interest or in the exercise of official authority, HRM ensures that the legal basis for processing is identified and documented.

4.3 Consent

Where required, HRM obtains explicit consent from individuals before processing their personal data. Consent is sought for specific purposes, and individuals are informed of their right to withdraw consent at any time. HRM maintains records of consent to demonstrate compliance with data protection laws.

4.4 Data Processing for Specific Purposes

HRM processes personal data only for the purposes for which it was collected. Any subsequent processing that is incompatible with the original purpose requires further consent from the individuals involved or must be justified on another legal basis as defined by applicable data protection laws.

4.5 Data Quality and Accuracy

HRM is committed to maintaining the quality and accuracy of personal data. Efforts are made to ensure that the data collected is up-to-date and relevant for the intended purpose. Individuals have the right to request corrections to their data, and HRM responds promptly to such requests.

4.6 Data Security Measures

HRM implements appropriate technical and organisational measures to ensure the security of personal data. This includes protection against unauthorised or unlawful processing, as well as accidental loss, destruction, or damage. Access controls,

encryption, and regular security assessments are among the measures employed to safeguard the confidentiality and integrity of personal data.

4.7 Third-Party Processing

When engaging third-party processors to handle personal data on behalf of HRM, contractual agreements are established to ensure that these entities adhere to the same high standards of data protection. Such agreements include provisions for data security, confidentiality, and compliance with applicable data protection laws.

Through these practices, HRM strives to ensure that personal data is collected and processed in a manner that respects individuals' rights, complies with legal requirements, and upholds the organisation's commitment to responsible data management.

5. Consent

HRM will obtain explicit consent from individuals before collecting and processing their personal data. Consent will be sought for each specific purpose, and individuals have the right to withdraw consent at any time.

5.1 Explicit Consent

HRM recognises the importance of obtaining explicit and informed consent from individuals before processing their personal data. Explicit consent is sought for each specific purpose of data processing, and individuals are provided with clear and accessible information regarding the nature of the data being collected, the purposes for which it will be processed, and any third parties involved in the processing.

5.2 Consent Process

The consent process at HRM is designed to be transparent, straightforward, and easily understandable. Individuals are informed of their right to withdraw consent at any time without facing any negative consequences. The consent request includes details about how to withdraw consent and the implications of doing so.

5.3 Purpose-Specific Consent

Consent is sought for specific and defined purposes, and HRM ensures that personal data is processed only in accordance with the purposes for which consent was obtained. If there is a need to process the data for additional purposes, HRM seeks fresh consent or relies on an alternative legal basis as defined by applicable data protection laws.

5.4 Records of Consent

HRM maintains records of the consents obtained, documenting the details of when, how, and what individuals were told at the time of providing consent. These records serve as

evidence of compliance with data protection laws and are periodically reviewed and updated.

5.5 Right to Withdraw Consent

Individuals have the right to withdraw their consent at any time. HRM respects this right and ensures that the withdrawal process is as simple as the initial consent process. Withdrawal requests are processed promptly, and individuals are informed of the implications of withdrawing consent, if any.

5.6 Consent for Minors

When collecting and processing personal data of minors, HRM seeks the consent of parents or legal guardians in accordance with applicable laws and regulations. Efforts are made to ensure that the information provided to parents or legal guardians is clear, accessible, and easily understandable.

5.7 Ongoing Communication

HRM maintains open lines of communication with individuals regarding the processing of their personal data. This includes periodic reminders of the purposes for which consent was obtained, any changes to data processing activities, and the availability of options to update or withdraw consent.

Through the careful and considerate management of consent, HRM aims to build and maintain trust with individuals, demonstrating a commitment to respecting their autonomy and privacy rights in the processing of personal data.

6. Data Subject Rights

Individuals have the right to access, rectify, erase, and restrict the processing of their personal data. HRM will respond to such requests within the timeframe specified by applicable laws.

6.1 Right to Access

Individuals have the right to obtain confirmation as to whether or not their personal data is being processed by HRM. Upon request, HRM provides individuals with access to their personal data, including information about the purposes of processing, the categories of data being processed, and any third parties involved in the processing.

6.2 Right to Rectification

HRM acknowledges the right of individuals to request the rectification of inaccurate or incomplete personal data. Requests for rectification are processed promptly, and efforts are made to ensure that the corrected data is updated across all relevant systems.

6.3 Right to Erasure
Individuals have the right to request the erasure of their personal data under certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected or if the individual withdraws consent. HRM ensures that requests for erasure are handled in compliance with applicable data protection laws.

6.4 Right to Restriction of Processing
HRM recognises the right of individuals to request the restriction of processing in certain situations, such as when the accuracy of the personal data is contested or when processing is unlawful. During the period of restriction, HRM ensures that the data is only processed with the individual's consent or for limited purposes.

6.5 Right to Data Portability
Where applicable, individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another data controller. HRM facilitates the exercise of this right, providing individuals with their data in a portable format upon request.

6.6 Right to Object
Individuals have the right to object to the processing of their personal data in certain situations, including processing based on legitimate interests or for direct marketing purposes. HRM respects individuals' objections and ceases processing unless there are compelling legitimate grounds for the processing that override the individual's interests, rights, and freedoms.

6.7 Automated Decision-Making and Profiling
HRM is transparent about any automated decision-making processes, including profiling, that significantly affect individuals. Where such processes are in place, individuals have the right to obtain information about the logic involved, the significance, and the envisaged consequences. HRM ensures that individuals can express their point of view and contest automated decisions.

6.8 Communication and Response
HRM has established clear procedures for receiving and responding to requests related to data subject rights. Individuals are provided with information on how to exercise their rights, and HRM ensures that responses to requests are provided within the timelines prescribed by applicable data protection laws.

Through the recognition and facilitation of data subject rights, HRM aims to empower individuals to have control over their personal data and to contribute to a culture of transparency and accountability in data processing.

7. Data Security

HRM will implement appropriate technical and organisational measures to ensure the security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

7.1 Information Security Policy

HRM maintains a comprehensive Information Security Policy that outlines the organisation's commitment to safeguarding personal data. This policy serves as a foundation for establishing and maintaining robust information security practices throughout the organisation.

7.2 Access Controls

Access to personal data within HRM is restricted based on the principle of least privilege. Access controls are implemented to ensure that only authorised individuals have access to specific types of data, and permissions are regularly reviewed and updated in accordance with changes in roles and responsibilities.

7.3 Security Training and Awareness

All employees and volunteers at HRM undergo security training to raise awareness about information security best practices. This training covers topics such as password management, recognising phishing attempts, and the importance of data protection. Regular awareness campaigns reinforce the significance of individual responsibility in maintaining data security.

7.4 Incident Response and Management

HRM has established an incident response and management framework to address security incidents promptly and effectively. This includes procedures for identifying, reporting, and responding to data breaches or security vulnerabilities. The organisation is committed to learning from incidents to continuously improve its security posture.

7.5 Physical Security

Physical access to areas where personal data is processed or stored is restricted to authorised personnel. Measures such as secure entry systems, surveillance, and restricted access zones are in place to prevent unauthorised physical access and to protect against theft, damage, or other physical threats.

7.6 Data Backup and Recovery

HRM implements regular data backup procedures to ensure the availability of personal data in the event of data loss or system failures. Backup copies are stored securely, and recovery procedures are tested periodically to verify their effectiveness.

7.7 Vendor and Third-Party Security

When engaging third-party vendors or processors, HRM ensures that they adhere to high standards of data security. Contracts with vendors include provisions for data protection, security measures, and compliance with applicable data protection laws.

Through these comprehensive data security measures, HRM aims to instil confidence in individuals whose data is processed, demonstrate its commitment to protecting privacy, and mitigate the risks associated with unauthorised access, loss, or misuse of personal data.

8. Data Breach Response

In the event of a data breach, HRM will promptly assess and mitigate the impact of the breach and report it to the Information Commissioner's Office (ICO) and affected individuals as required by law.

8.1 Definition of a Data Breach

HRM defines a data breach as any unauthorised access, disclosure, alteration, or destruction of personal data. This includes incidents where there is a risk to the confidentiality, integrity, or availability of the data.

8.2 Incident Reporting Procedures

Employees and volunteers at HRM are educated about the importance of promptly reporting any incidents or suspicions of a data breach. Clear and accessible reporting procedures are in place to facilitate the timely identification and reporting of potential breaches.

8.3 Incident Identification and Assessment

Upon receiving a report or detecting a potential incident, HRM initiates a swift and thorough investigation. The organisation assesses the nature and scope of the breach, identifying the categories of individuals affected, the type of data involved, and the potential impact on individuals.

8.4 Communication Protocols

HRM has established clear communication protocols for notifying affected individuals, regulatory authorities, and other relevant stakeholders in the event of a data breach. The organisation complies with the legal obligations for reporting breaches to the

Information Commissioner's Office (ICO) and communicates transparently with affected individuals about the nature of the breach and the steps being taken to mitigate its impact.

8.5 Mitigation and Remediation
Immediate action is taken to mitigate the impact of a data breach. This may include securing systems, disabling unauthorised access, and taking steps to prevent further unauthorised disclosure or access. HRM also considers and implements remediation measures to prevent similar incidents in the future.

8.6 Data Breach Notification
In accordance with data protection laws and regulations, HRM notifies affected individuals without undue delay when a breach is likely to result in a high risk to their rights and freedoms. The notification includes information about the nature of the breach, the types of data involved, and the measures taken to address the breach.

8.7 Record-Keeping
HRM maintains detailed records of all data breaches, including the incident's nature, the response actions taken, and the outcomes of the breach assessment. These records serve as evidence of compliance with data protection laws and are used to inform future incident response planning.

8.8 Continuous Improvement
HRM views data breaches as opportunities to learn and improve. After each incident, a thorough analysis is conducted to identify root causes, assess the effectiveness of the response, and implement changes to policies, procedures, or security measures to enhance the organisation's overall resilience to data breaches.

8.9 Collaboration with Authorities
HRM collaborates with regulatory authorities, such as the ICO, and other relevant entities to ensure compliance with reporting requirements and to contribute to a collective effort to address and prevent data breaches within the broader community.

By maintaining a robust data breach response framework, HRM aims to minimise the impact of incidents on individuals, uphold its commitment to transparency, and continuously enhance its data protection practices.

9. International Data Transfers
HRM will only transfer personal data outside the UK and the European Economic Area (EEA) if adequate safeguards are in place, as required by applicable data protection laws.

9.1 Definition of International Data Transfers
International data transfers refer to the transmission of personal data from the United Kingdom or the European Economic Area to countries or organisations outside these regions. HRM recognises the importance of safeguarding personal data even when it is transferred internationally.

9.2 Legal Basis for International Transfers
HRM ensures that international data transfers are conducted in compliance with applicable data protection laws. The organisation identifies a lawful basis for such transfers, which may include obtaining the explicit consent of the individuals, entering into standard contractual clauses, ensuring the existence of an adequacy decision for the destination country, or utilising other legally recognised mechanisms.

9.3 Standard Contractual Clauses (SCCs)
Where required, HRM uses standard contractual clauses approved by the Information Commissioner's Office (ICO) or other relevant authorities. These clauses establish a legal framework for the protection of personal data during international transfers and outline the responsibilities of both HRM and the receiving entity.

9.4 Adequacy Decisions
HRM reviews and considers adequacy decisions issued by the ICO or the European Commission for the destination country. Adequacy decisions recognise that the data protection laws and practices in the destination country provide an adequate level of protection for personal data, facilitating lawful transfers.

9.5 Binding Corporate Rules (BCRs)
In the event that HRM operates within a multinational group, the organisation may consider implementing Binding Corporate Rules, a set of internal rules for the international transfer of personal data within the group. BCRs are subject to approval by the relevant data protection authorities.

9.6 Data Subject Information
Individuals are informed about international data transfers as part of HRM's transparency commitment. The organisation communicates the transfer mechanism used, the purposes of the transfer, and any additional safeguards in place to protect their data during the transfer.

9.7 Monitoring and Compliance

HRM establishes mechanisms for ongoing monitoring and compliance with international data transfer regulations. Regular reviews are conducted to ensure that the legal basis for transfers remains valid, and any changes in the legal landscape or data protection practices of the destination country are promptly addressed.

9.8 Documentation and Record-Keeping

HRM maintains documentation of the legal basis, safeguards, and risk assessments associated with international data transfers. This documentation serves as evidence of compliance with data protection laws and is available for review by regulatory authorities if required.

By carefully considering the legal requirements and implementing appropriate safeguards, HRM aims to ensure that international data transfers are conducted in a manner that upholds the privacy rights of individuals and complies with the principles of data protection.

10. Training and Awareness

HRM will provide training to staff and volunteers to ensure they are aware of their responsibilities under this policy and are knowledgeable about data protection laws and regulations.

10.1 Importance of Training and Awareness

Human Relief Mission (HRM) recognises that fostering a culture of data protection requires informed and vigilant employees, volunteers, and stakeholders. Training and awareness initiatives are fundamental to ensuring that all individuals associated with HRM understand their responsibilities, recognise the significance of data protection, and actively contribute to maintaining high standards in the handling of personal data.

10.2 Data Protection Training Programs

HRM conducts regular and comprehensive data protection training programs for all employees and volunteers. These programs cover essential topics such as the principles of data protection, legal obligations, the organisation's data protection policies and procedures, and the potential consequences of non-compliance.

10.3 Tailored Training for Roles and Functions

Recognising that different roles within the organisation involve distinct data protection responsibilities, HRM tailors training content to the specific needs of different departments and functions. This ensures that individuals understand how data protection principles apply to their daily activities and responsibilities.

10.4 New Employee and Volunteer Onboarding

As part of the onboarding process, new employees and volunteers receive specific training on data protection policies and practices. This orientation ensures that individuals are immediately aware of their role in safeguarding personal data and contributing to HRM's commitment to data protection.

10.5 Scenario-Based Training

HRM incorporates scenario-based training modules that simulate real-world situations. These exercises allow individuals to apply their knowledge in practical contexts, improving their ability to identify and respond to data protection challenges effectively.

10.6 Leadership Training

Leadership and management personnel receive specialised training to ensure they have a deep understanding of data protection requirements. This training covers their additional responsibilities in overseeing data protection practices within their teams and promoting a culture of compliance.

10.7 Reporting and Escalation Procedures

Training programs emphasise the importance of reporting and escalation procedures in the event of potential data breaches or non-compliance. Individuals are educated on how to recognise and report incidents promptly, ensuring swift and appropriate responses.

10.8 Collaboration with External Experts

HRM collaborates with external experts, consultants, or data protection authorities to provide specialised training or workshops. This collaborative approach ensures that HRM remains informed about the latest developments in data protection and enhances the knowledge and skills of its workforce.

10.9 Continuous Monitoring and Evaluation

HRM continuously monitors the effectiveness of its training initiatives through assessments, surveys, and feedback mechanisms. The organisation uses this information to refine training programs, address specific needs, and continuously improve the overall data protection education strategy.

By investing in comprehensive training and awareness programs, HRM aims to empower its workforce with the knowledge and skills necessary to protect personal data, mitigate risks, and uphold the highest standards of data protection throughout the organisation.

11. Policy Review

This Data Protection Policy will be reviewed regularly to ensure its continued relevance and compliance with applicable laws. Any updates will be communicated to staff, volunteers, and other relevant parties.

11.1 Purpose of Policy Review

Human Relief Mission (HRM) recognises the dynamic nature of data protection landscapes, including changes in legislation, technology, and organisational practices. The purpose of policy review is to ensure that HRM's Data Protection Policy remains current, effective, and aligned with the latest legal and industry standards.

11.2 Scheduled Reviews

HRM conducts regular and scheduled reviews of the Data Protection Policy to assess its relevance and effectiveness. These reviews are conducted at least annually, and more frequently if there are significant changes in data protection laws, organisational structure, or processing activities.

11.3 Involvement of Key Stakeholders

Policy reviews involve collaboration with key stakeholders, including legal experts, data protection officers, IT professionals, and representatives from different departments. This collaborative approach ensures a comprehensive and well-informed assessment of the policy's adequacy.

11.4 Legislative Compliance Checks

During policy reviews, HRM conducts thorough checks to ensure that the Data Protection Policy complies with the latest data protection laws and regulations, with a particular focus on updates to the General Data Protection Regulation (GDPR) or any relevant UK legislation.

11.5 Technology and Security Assessments

As technology evolves, HRM assesses whether the policy adequately addresses the organisation's technological infrastructure and security measures. This includes evaluating the effectiveness of existing controls and considering updates or enhancements to address emerging risks.

11.6 Risk Assessments

HRM conducts risk assessments to identify and evaluate potential risks to data protection within the organisation. These assessments consider internal and external factors that may impact the security and privacy of personal data.

11.7 Feedback Mechanisms

HRM establishes feedback mechanisms to gather input from employees, volunteers, and other stakeholders regarding their experiences with data protection practices. This feedback helps identify areas for improvement and ensures that the policy is responsive to the needs of the individuals it is designed to protect.

11.8 Documenting Changes

Any updates or revisions resulting from the policy review are documented meticulously. This includes detailing the nature of the changes, the reasons for the modifications, and the specific sections of the policy that are affected. Documenting changes ensures transparency and accountability.

11.9 Communication of Updates

Upon completing a policy review and implementing changes, HRM communicates the updates to all relevant stakeholders. This communication may include training sessions, internal memos, or other channels to ensure that individuals are aware of the revised policy and any new expectations or procedures.

11.10 Continuous Improvement

Policy review is not a one-time event but an ongoing process of continuous improvement. HRM remains vigilant in monitoring developments in data protection, regularly evaluating its practices, and adapting the Data Protection Policy to reflect the organisation's commitment to best practices and compliance.

11.11 Legal Compliance Certification

Following a comprehensive review and taking into consideration the financial circumstances, HRM may consider obtaining legal compliance certification from relevant data protection authorities or third-party certifying bodies. This certification serves as external validation of HRM's commitment to adhering to the highest standards of data protection.

By actively engaging in regular policy reviews, HRM aims to ensure that its Data Protection Policy remains a robust and effective framework for safeguarding personal data, promoting privacy, and upholding the trust and confidence of all individuals associated with the organisation.