General Data Protection Regulation (GDPR) & Data Protection

Policy and procedures

Aug 2025-27

Document control

Document information	Details
Title	Data Protection policy
Number	2
Version	6
Status	Draft / Under Review/ Exec Approved / Pending Trustee review / Approved
Effective date	September 2025
Next review date	September 2027
Owner	Executive Team
Approved by	Hannah Lashley (Director of Services)
Approval date	HL - November 2025

Version History

Version	Date	Modified by	Notes of Changes
1			Draft
2	January 2023	Jordan Ignatius and Maria Khan	Reaching Higher Data Protection Policy has been reviewed by Jordan Ignatius. This document will be put through to Approval by the Trustees Board, before it is formally published.
3	January 2023	Jordan Igantius	Approved by Jordan Ignatius (MD) and Marvin Rufus (trustee)
4	8th April 2024	Hannah Lashley	Updated by Hannah Lashley (DoS) Added as new Data Protection Officer
5	May 2025	Hannah Lashley	Hannah reviewed – changed record keeping duration.
6	11th August 2025	Hannah Lashley	Policy review and updates. Removal of clause regarding employee or volunteer retention records of 12 months.
7	30th September 2025	Robert Davis	Trustee review and feedback. Flagged key missing information from previous procedures sent.
8	4th November 2025	Hannah Lashley	Updates procedures and added missing GDPR policy. Added contents and data protection schedule table.

Related documents

- Confidentiality policy; Complaints policy; Safeguarding policy; Privacy policy; Retention Policy; Social Media policy

Contents

1. Purpose and Principle of policy and procedure

This policy is intended to cover the Data Protection responsibilities of Reaching Higher towards those who work for and with us in our work.

Details of the charity's Data Protection Officer are provided at the end of the policy.

The Data Protection Act 2018 (previously The Data Protection Act 1998) regulates the processing of information relating to individuals. This includes the obtaining, holding, using or disclosing of this information, and covers computerised records as well as paper filing systems. Data users must comply with the data protection principles of good practice which underpin the Act.

Everyone has rights regarding the way in which their personal data is handled. During the course of our activities, we will collect, store and process personal data about our staff, young people, partners and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful charity operations.

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

The types of personal data that we may be required to handle include information about current, past and prospective staff, young people, partners and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and other regulations.

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2. Introductions

This policy has been designed based on legislation, policy and guidance that seek to protect enforce Data Protection law in England.

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

Data Protection meaning and terms:

DATA	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
DATA SUBJECTS	For the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
PERSONAL DATA	Data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.
DATA CONTROLLERS	The people or charity who determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the GDPR. We are the data controller of all personal data used in our charity for our own commercial purposes.
DATA USERS	Employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
DATA PROCESSORS	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include partners which handle personal data on our behalf.
PROCESSING	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
SENSITIVE PERSONAL DATA	Information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings, genetic data and biometric data where processed to uniquely identify a person (for example a photo in an electronic passport). Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3. Data Protection Principles

The data controller is responsible for and must be able to demonstrate compliance with these principles. Personal data must be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes).

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation).

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay .

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

It is the policy of Reaching Higher that all personal data will be held in accordance with the principles and requirements of data protection and other relevant legislation, and that procedures will be put in place to ensure the fair processing of data subjects.

Reaching Higher and all staff and volunteers who process or use personal data must ensure that they abide by these principles at all times. Relevant data protection issues will be included in all induction and training. Reaching Higher will ensure that staff and volunteers know enough about how information held about them is used or disclosed. Information held about staff and volunteers and young people will only be collected and recorded with good reason. It will be stored securely and for only as long as required. Relevant data protection issues will be included in all induction and training.

- Information no longer required will be disposed of appropriately.
- Inform staff/volunteers and young people, parents/carers why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Ensure our staff are aware of and understand our policies and procedures

Reaching Higher will not give out information about any individual over the telephone or by e-mail unless it is satisfied that the individual knows that this type of disclosure may be made and/or the information is already in the public domain (or that there is an over-riding reason for the disclosure such as safeguarding the wellbeing of a child, young person, employee or volunteer).

No details of individuals will be passed to other organisations for marketing, fundraising or circulating information unless consent has been obtained and the individual given the opportunity to opt-in or opt-out.

4. Fair and Lawful Processing

- The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

- For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our charity, we will ensure that those requirements are met.

5. Specified, Explicit and Legitimate Purposes

- In the course of our charity, we may collect and process the personal data set out in the Schedule. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, charity partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

- We will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the GDPR. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

6. Notifying Data Subjects

If we collect personal data directly from data subjects, we will inform them about their rights under the GDPR including:

a) The purpose or purposes for which we intend to process that personal data and the legal basis for the processing.
b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.
c) The means, if any, with which data subjects can limit our use and disclosure of their personal data including the right to object to processing.
d) The right of subject access.
e) The right to be forgotten.
f) The right to withdraw consent, where processing is based on consent.
g) The right to rectification if data is inaccurate or incomplete.

h) Rights related to automated decision making and profiling.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

7. Data Minimisation

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

8. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9. Storage Limitation

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10. Processing in line with Data Subject's rights

We will process all personal data in line with data subjects' rights, in particular their right to:

a) Request access to any data held about them by a data controller.
b) Object to processing, including in particular to prevent the processing of their data for direct-marketing purposes.
c) Ask to have inaccurate data amended.
d) Request the deletion or removal of personal data where there is no compelling reason for its continued processing.
e) Prevent processing that is likely to cause damage or distress to themselves or anyone else.
f) Obtain and reuse their personal data for their own purposes (where that right applies)

11. Data Security

We will process all personal data in line with data subjects' rights, in particular their right to:

- We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. If there is a data security breach which will result in a risk to the data subject we will report that breach to the regulator without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

- We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a) **Confidentiality** means that only people who are authorised to use the data can access it.
b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept clear and locked if they hold confidential information of any kind. **(Personal information is always considered confidential.)**

c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

12. Transferring Personal Data to a country outside the EEA

We will only transfer any personal data we hold to a country outside the European Economic Area ("EEA") where the conditions of transfer provided for in the GDPR apply.

13. Disclosure and Sharing of Personal Information

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

We may also disclose personal data we hold to third parties:

a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

c) If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, young people, non-paid workers, partners or others. This includes

exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

d) We may also share personal data we hold with selected third parties for the purposes set out in the **Error! Reference source not found.**.

14. Dealing with Subject Access Requests (SAR)

- Data subjects must make a formal request for information we hold about them. This must be made in writing (email or paper letter). Employees who receive a written request should forward it to their line manager immediately.

- When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:
  a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
  b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Our employees will refer a request to their line manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

15. Staff records

- The names and posts held by staff and trustees within Reaching Higher are considered to be in the public domain and may be made freely available in any format to anyone.
- Contact details of Trustees are made available to staff only for the purpose of making contact in furtherance of Reaching Higher's governance.
- The work mobile numbers of staff are available to all staff and Trustees.
- Staff contact numbers shall be made available to other staff members for the purpose of making contact in an emergency.
- All information required for the purposes of payroll is confidential and made available only to the Treasurer of the Board of Trustees, Jordan Ignatius (MD), Lisa Harrison (ED) and external payroll provider who oversees finance. Information will be passed to statutory bodies if a legal requirement, such as in connection with tax and national insurance.
- All other information within staff records is confidential and can only be made available to Reaching Higher Executive Team. Personnel records are only used for matters connected with the individual's employment at Reaching Higher or to help with references Reaching Higher might write in future at the staff or volunteer's request.
- Information about age, gender, geographical location, ethnicity, sexual orientation, marital status and disability of staff, volunteers and Board members is kept for the purposes of monitoring our equal opportunities policy.
- Staff will be given full open access to their complete personnel records.
- Databases containing information about individuals (including children and young people) shall be confined to contact details and information directly relevant to the reason for their inclusion on Reaching Higher's databases.

- Information about age, gender, geographical location, ethnicity and disability of staff members, volunteers and young people will be kept anonymous and is collected only for the purposes of monitoring equal opportunities and reporting back to funders.
- Data about individuals shall be deleted on the request of the individual when the data is no longer used or required for legal, financial or contractual reasons.

16. Photographs and Videos

- Reaching Higher heavily relies on and uses photographs and videos within sessions, group work, events and activities and for promotional purposes.

- The Reaching Higher website will not contain any personal data that is not absolutely necessary. Where information is captured on the website, a clear policy statement will be provided, and no personal data will be captured without the knowledge of the data subject. Photographs, recordings, videos or DVDs in which any children or young people can be identified will only be used with explicit written consent from parents/carers.

17. Parental Inclusion and Permission

For all events, activities, trips and residentials, parental inclusion is necessary. Young people under the age of 18 years of age must have parental consent. On all forms, Reaching Higher require the name, address, date of birth and contact details (phone and/or email) of the young person involved. We require that both the parent/carer and young person must sign forms to agree to terms and conditions of the event as well as permission for Reaching Higher to use their personal information.

Reaching Higher Data Protection Officer

Name: Hannah Lashley
Job Role: Director of Services
Contact: info@reachinghigher.org.uk
Appointed Since: April 2024

Policy last updated: 4th November 2025

Schedule for Data Processing activities

Type of data	Type of data subject	Type of processing	Purpose of processing	Type of recipient to whom personal data is transferred	Retention period	Security Measures
Contact information (name, address, phone, email)	Young people (service users), parents/carers/guardians, volunteers, donors	Collection, storage, updating, communication	To manage participation in programmes, send updates, contact in emergencies	Staff, authorised volunteers, CRM/email platform providers	Minimum 6 years after last contact (or 6 years for donors)*	Password-protected systems, encrypted databases, restricted staff access
Emergency contact and medical information	Young people (service users)	Collection, storage, limited sharing in emergencies	To ensure participant safety during activities or events	Emergency services, authorised staff and delivery leaders	Minimum 6 years after last contact*	Encrypted storage, limited access, paper forms kept in locked cabinets
Volunteer and staff records (ID, DBS checks, training, references)	Volunteers, employees	Collection, verification, storage, updating	To ensure safeguarding compliance and manage volunteer engagement	HR staff, DBS disclosure service, Line managers	Minimum 6 years after last contact*	Secure HR software, access logs, locked filing cabinets
Donation and financial records (bank details, gift aid forms)	Donors, supporters	Collection, storage, transmission to financial institutions	To process donations and claim Gift Aid	Bank, HMRC (for Gift Aid claims), accounting software, contracted accountant	7 years (in line with HMRC requirements)	Encrypted transmission, financial software with role-based access

Photographs and videos	Young people, volunteers	Collection, storage, publication (with consent)	To promote activities and report to funders	Website visitors, social media platforms, funders	Until consent withdrawn or minimum 6 years after event*	Consent forms stored securely, minimal identifying info shared
Programme participation data (attendance, feedback, progress reports)	Young people	Collection, storage, analysis	To monitor engagement, evaluate impact, and report to funders	Programme staff, funders (aggregated/anonymised data)	Minimum 6 years after programme completion*	Access-limited databases, anonymisation for reporting
Safeguarding records	Young people, volunteers, staff	Collection, investigation, reporting	To protect welfare and meet safeguarding legal obligations	Local authorities, police, safeguarding boards	Minimum 6 years (or in line with safeguarding law)*	Highly restricted access, encrypted files, secure sharing protocols

Minimum of 6 years is added as the average cycle and retention Reaching Higher engages with young people.