Data Protection Policy

Data Protection Policy

At a Glance

This policy sets out the principles of Data Protection and how they apply to our organisation.

This policy applies to all members of staff who work under a contract of employment with Harry's Rainbow, any contractors engaged by the organisation, volunteers and to members of the Board.

Policy Status

This policy is owned by the Board of Trustees. It is non-contractual and may be updated or changed by the Board at any time. Changes will be notified to all parties the policy applies to. You should ensure you review the policy and any changes and if you are unsure how the policy and any changes apply to your role, check with your line manager or supervisor.

Introduction

This Policy explains the Charity's obligations regarding all uses of information about people, also known as personal data. The charity processes personal data about its staff, volunteers, contractors, board members and beneficiaries. The processing of or use of their data is governed by this policy. Processing includes all stages of use of personal data including its collection, use, transfer, storage, and disposal.

The procedures and principles set out in this policy must be followed at all times by the Charity, its employees, volunteers, contractors, or other parties working on behalf of the Charity.

Scope

Harry's Rainbow places high importance on the correct, lawful, and fair handling of all information we hold about people (their personal data), respecting their rights, privacy, and trust of all individuals we deal with.

The Charity's Data Protection Lead is the CEO.

Owner: Odette Mould	Approval Date: 02/10/24
Approved by: CEO & Board	Next Review Date: 02/10/25

Data Protection Policy

The Data Protection Lead is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

All managers and supervisors are responsible for ensuring that employees, volunteers, contractors, or other parties working on behalf of the Charity comply with this Policy.

All managers and supervisors are also responsible for making sure we have appropriate practices, processes and controls in place to make sure personal data is used in line with data protection legislation.

Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Lead. In particular, the Data Protection Lead should always be consulted in the following cases:

- if there is any uncertainty about ways we will use information about people and what allows us to do this.
- if consent is being relied upon to use information about people (known as personal data);
- if there is any uncertainty relating to the length of time we should hold personal data;
- if any new or amended privacy notices are required;
- if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);
- if any incident or issue has occurred using or relating to personal data;
- if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;
- if personal data is to be shared or transferred outside of the organisation if personal data is to be transferred outside of the UK
- when any new or significant project is likely to use personal data, or significant changes are to be made to existing ways of working or when personal data is to be used for purposes different to those for which it was originally collected;
- if any automated processing, including profiling or automated decision-making, is to be carried out; or
- if any assistance is required in complying with the law applicable to direct marketing.

Owner: Odette Mould	Approval Date: 02/10/24
Approved by: CEO & Board	Next Review Date: 02/10/25

Data Protection Policy

The Data Protection Principles

This Policy aims to ensure the charity are meeting their responsibilities under Data Protection Law.

The UK GDPR a set of seven principles we need to be able to show we meet the requirements of when we handle personal data. They are called the Data Protection Principles.

This section of the policy explains how we as a charity will meet the requirements of these principles and also highlights where your responsibilities are in the work that you do.

How we meet The Data Protection Principles

Principle 1 – Lawful, fair and transparent use of personal data

The charity ensures all use of personal data is lawful, fair and transparent in the following ways:

- All new ways of working or changes in practice are done with support from the data protection lead who will ensure that the charity knows what allows them to use personal data and consider whether their use of personal data is fair.
- The charity maintains a record of processing activities (ROPA) which is regularly reviewed to sure it remains relevant.
- The charity maintains appropriate privacy notices and reviews them annually to make sure they reflect the work they do.
- The charity make sure that privacy information is provided to staff/volunteers and service users before we start using their data (i.e. included in online forms, email footers and on the charity website as a minimum) and is pointed to in all communications with service users/staff/volunteers and located on the charity website for anyone interested in our work to view.

Responsibilities:

Managers/Supervisors must take advice from the charity Data Protection lead regarding updates to the privacy notices to reflect changes in practice.

Managers/Supervisors must ensure that clear instructions are given to all staff involved in projects that involve use of personal data.

Staff/volunteers and managers/supervisors must ensure that any new use of personal data or significant

Data Protection Policy

change proposed to the use of personal data or the way in which it is managed must be discussed with the charity's data protection lead who will provide advice on lawfulness, fairness and transparency for the proposed use of personal data.

Staff/volunteers must ensure any written communications with service users include links to the relevant privacy information.

Principle 2 – compatibility of processing

The Charity uses personal data collected directly from data subjects and personal data obtained from third parties.

The Charity only collects, processes, and holds personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by Data Protection Law).

Responsibilities:

Managers/Supervisors must ensure that any proposed re-use of data is discussed with the charity data protection lead in advance of a change of use.

Principle 3 – data minimisation

The Charity will only collect, and process personal data needed for the purposes set out in this policy and will ensure processes are in place to collect only the necessary personal data from staff/volunteers/service users.

Responsibilities:

Managers/Supervisors/Staff/contractors/volunteers may only collect personal data needed to provide the services they are employed to provide. Excessive personal data must not be collected.

Managers/Supervisors are required to consider how to use less personal data and to minimise the personal data collected, used, shared, stored and otherwise processed on the basis of what the charity needs

Data Protection Policy

Managers and supervisors must also ensure appropriate procedures are in place to support staff and volunteers in their roles.

Managers/Supervisors/Staff/contractors/volunteers may only use or access personal data when it is necessary for their role.

Principle 4 – data accuracy

The charity takes steps to make sure the data we process is accurate. We will ensure our staff and volunteers responsible for working with information about people know how to update out of date or inaccurate data.

Responsibilities:

Managers/Supervisors will ensure all staff/volunteers are aware of the need to keep accurate records and that if an individual disputes the information e hold this should be referred to the charity's Data Protection Lead.

Managers/Supervisors/Staff/contractors/volunteers must regularly check the accuracy of personal data with service users/staff and ensure any changes required are made promptly.

Staff and managers must also ensure their own records are kept accurate and updated in the HR system when necessary.

Principle 5 – retention of personal data

The Charity shall not keep personal data for any longer than is necessary for the purposes agreed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the Charity's approach to data retention, including retention periods for specific personal data types held by the Charity, please refer to our Data Retention Policy.

Responsibilities:

Managers/Supervisors must ensure data is not held for longer than the agreed retention periods and

Data Protection Policy

should ensure they are familiar with the Charity's data retention policy.

Managers/Supervisors are responsible for ensuring the safe and secure destruction of personal data in line with the retention policy.

Principle 6 – security of personal data

The Charity takes the following steps to make sure that personal data is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

All technical and organisational measures taken to protect personal data are regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

- All emails containing personal data are encrypted, marked confidential and are only sent over secure networks.
- Any personal data provided by email or other messaging format approved for use by the charity should be copied and stored in the appropriate location if it is needed for the purposes of the charity. Email/other approved messaging formats should not be relied on as a storage facility for personal data relating to staff/volunteers/service users. Emails/other instant message formats should be appropriately managed and deleted when the necessary information has been transferred and saved securely.
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient.
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".
- All electronic copies of personal data should be stored securely and only able to be accessed by those with a genuine need.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar; and accessed only by those with a genuine need.
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether the device belongs to the Charity or otherwise without the formal written approval of the CEO for specified agreed purposes.
- No personal data should be transferred to any personal device belonging to an employee, agent, contractor, or other party working on behalf of the Charity.

Data Protection Policy

- Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Charity where a contract is in place and appropriate measures have been demonstrated to ensure the security of the personal data.
- When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Charity's Data Retention Policy.
- No personal data may be shared informally. If an employee, volunteer, contractor, or other party working on behalf of the Charity requires access to any personal data that they do not already have access to, this must be formally requested from the CEO;
- No personal data may be transferred to any employee, agent, contractor, or other party, without the authorisation of CEO;
- Personal data must be handled with care at all times and should not be left unattended or on view to any unauthorised persons at any time.
- All staff/volunteers/managers/supervisors must ensure computer screens are locked if they are to be left unattended.;
- Where personal data held by the Charity is used for marketing purposes, it shall be the responsibility of CEO to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

Data Security - IT Security

The Charity ensures the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
- All passwords used to protect personal data should follow national cyber security centre

Data Protection Policy

standards and should not be used internally and externally to the charity (i.e. staff must not use the same passwords in work and in their personal life);

- All software used by the Charity is designed to require such passwords;
- Under no circumstances should any passwords be written down or shared between any employees, volunteers, contractors, or other parties working on behalf of the Charity, irrespective of seniority or department.
- If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Charity's IT provision shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible;
- No software may be installed on any Charity-owned computer or device without the prior approval of the CEO.
- Where personal data held by the Charity is used for marketing purposes, it shall be the responsibility of Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.
- No external media or devices may be plugged into the charity's devices/network without the prior approval of the charity's IT staff and Managing Director. Case by case assessment of the need will be carried out all staff should request removable media from senior management with a clear business case for the need. No personal non encrypted sticks should be used – this is not permitted for business.

Data Security – Organisational measures

The Charity shall ensure that the following measures are taken:

- All employees, volunteers, contractors, or other parties working on behalf of the Charity shall be made fully aware of both their individual responsibilities and the Charity's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, volunteers, contractors, or other parties working on behalf of the Charity that

Data Protection Policy

need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Charity;

- All employees, volunteers, contractors, or other parties working on behalf of the Charity handling personal data will be appropriately trained to do so and will be appropriately supervised/supported in their roles;
- All employees, volunteers, contractors, or other parties working on behalf of the Charity handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- The performance of those employees, volunteers, contractors, or other parties working on behalf of the Charity handling personal data shall be regularly evaluated and reviewed;
- All employees, volunteers, contractors, or other parties working on behalf of the Charity handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;
- The charity has an information security policy in place and ensures this is regularly reviewed and updated.
- The charity follows guidance from NCSC, ICO and other relevant authorities around the necessary steps they should take to secure personal data they are data controller for.
- The charity have an established breach management process in place and all staff and managers are made aware of the correct process for reporting data security incidents and potential personal data breaches to the charity management for investigation (supported by the data protection officer).
- The charity have deployed a number of specific security measures as detailed below, to ensure the security of the personal data the charity holds.

Data Security – Technical measures

The Charity shall ensure that the following measures are taken:

- All electronic copies of personal data including emails should be stored securely using passwords

Data Protection Policy

and data encryption and emails containing personal data should be marked confidential;

- Personal data may only be transmitted over secure networks;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
- All personal data transferred physically should be transferred in a suitable container marked “confidential”;
- All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely; no personal data should be stored on removable media without approval from the CEO and data protection lead.

Data Sharing and working with third parties measures

- No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Data Protection Officer.
- No personal data may be transferred to any staff, agents, contractors, or other parties, whether such parties are working on behalf of the Charity or not, without authorisation;
- Where the charity engage with third parties to process personal data on our behalf, we ensure we have robust contracts in place, and undertake necessary checks to ensure appropriate levels of security are in place with those contractors to maintain the safety and security of our customer and staff personal data.
- If we intend to share personal data with other parties the charity will ensure that the privacy information provided to those individuals reflects this and that we understand what allows us to do so;
- All agents, contractors, or other parties working on behalf of the Charity handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Charity arising out of this Policy and Data Protection Law;
- Where any volunteer, contractor or other party working on behalf of the Charity handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Charity against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Data Protection Policy

Responsibilities:

Staff, managers, contractors and volunteers must do everything in their power to maintain the security, confidentiality, integrity and availability of personal data.

Staff, managers, contractors and volunteers must adhere to the requirements of this policy and the information security policy and all and any relevant guidance as issued by the management or the data protection lead.

Staff, managers, contractors and volunteers must ensure they report any suspicious activity, suspected data incident or personal data breach to management for investigation (with the support of the Data Protection lead).

Staff, managers, contractors and volunteers must ensure the complete their mandatory training on data protection and ask any questions arising from this.

Staff, managers, contractors and volunteers must ensure they only access necessary personal data to carry out their roles.

Principle 7 – accountability and record keeping.

The Data Protection lead is responsible for management of this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

The Charity follows a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments are carried out when appropriate.

All staff, agents, contractors, or other parties working on behalf of the Charity shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Charity policies.

The Charity's data protection compliance shall be regularly reviewed and evaluated by means of annual Data Protection Audits.

The Charity shall maintain a record of processing activities for those activities which meet the requirements of the law.

Responsibilities:

Owner: Odette Mould	Approval Date: 02/10/24
Approved by: CEO & Board	Next Review Date: 02/10/25

Data Protection Policy

Managers/Supervisors must ensure all staff/volunteers/contractors are provided with the necessary policies, procedures and guidance to undertake their roles in relation to working with personal data.

Managers/Supervisors must ensure all staff/volunteers/contractors undertake appropriate mandatory training in data protection.

Managers/Supervisors must ensure that the data protection lead is kept up to date with new ways of working/new projects which involve use of personal data to allow for a data protection by design approach to be taken and for the maintenance of the record of processing activities.

All staff/volunteers/contractors must follow the charity's policies, procedures and guidance relative to their role and not use personal data they are provided with access to in any other way.

All staff/volunteers/contractors must attend mandatory training in data protection.

Data Protection Impact Assessments (DPIA)

The Charity carries out Data Protection Impact Assessments (DPIA) for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

Data Protection Impact Assessments shall be overseen by the Data Protection lead

Responsibilities

Managers and supervisors must ensure that all staff check with the data protection lead before starting a new piece of work to decide if a DPIA is required.

Owner: Odette Mould	Approval Date: 02/10/24
Approved by: CEO & Board	Next Review Date: 02/10/25

Data Protection Policy

All staff, volunteers and contractors must discuss changes in working practices/new projects with their manager/the CEO/Board as appropriate before beginning and may need to consult with the Data Protection lead.

The Rights of Data Subjects

The UK GDPR sets out the following key rights for all individuals who's information (personal data) is used by organisations:

- The right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (also known as the 'right to be forgotten');
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights with respect to automated decision-making and profiling.

For further information on how the charity handles rights requests please see our SAR and other rights policy.

Transferring personal data outside of the UK

The Charity may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The UK GDPR requires us to make sure the data is offered the same level of protection and rights are able to be exercised regardless of where the data is held

The Charity will ensure that any international transfers are assessed using a DPIA and that appropriate safeguards and measures are put in place to ensure the security of the data and the ability to exercise rights.

Data Breach Notification

Owner: Odette Mould	Approval Date: 02/10/24
Approved by: CEO & Board	Next Review Date: 02/10/25

Data Protection Policy

Any misuse, loss, unlawful destruction, alteration of or unauthorised disclosure of or access to information about people may be a personal data breach. This means all staff must be aware of the correct process to follow if they suspect something has gone wrong.

Some breaches need to be reported to the Information Commissioners Office (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage). This must happen within 72 hours of anyone working with or within the charity becoming aware of the issue. We may also have to tell the people whose data has been affected.

All personal data breaches must be reported immediately to the Charity's Data Protection Lead.

If an employee, volunteer, contractor, or other party working on behalf of the Charity becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves.

All data breach assessments need to consider what has happened to ensure we resolve the issue and minimise the possibility of it happening again. The charity will keep records of breaches and learn from them, sharing this learning with other staff and volunteers.

Responsibilities:

Managers/Supervisors must ensure that staff/volunteers and contractors understand who to contact if something goes wrong involving personal data.

All Staff/volunteers/contractors must ensure they speak to their manager/the data protection lead if they suspect a data breach has occurred for an assessment to be carried out. Provide as much information as you can including:

What happened

When it occurred and how you found out.

Whose data has been affected (and how many people are affected) and the types of information involved/affected

Any known or suspected consequences of the breach for the people whose data was affected;

Review of this policy

Owner: Odette Mould	Approval Date: 02/10/24
Approved by: CEO & Board	Next Review Date: 02/10/25

Data Protection Policy

This policy is reviewed biannually by the Board and the CEO taking into account external advise where appropriate.

The policy was last updated in Augus 2024.

Owner: Odette Mould	Approval Date: 02/10/24
Approved by: CEO & Board	Next Review Date: 02/10/25