Data Protection Policy

At a glance

This policy sets a framework for the principles of Data Protection Policy.

Who this policy applies to

This policy applies to all members of staff who work under a contract of employment with Harry's Rainbow, 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. Colleagues are reminded that it is their responsibility to keep up to date with policy changes.

The charity is fully committed to compliance with the requirements of the Data Protection Act 2018 and all other data protection legislation currently in force. The Regulation applies to anyone processing personal data and sets out principles which should be followed and gives rights to those whose data is being processed.
To this end, the charity endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

• processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency'); • processed no further than the legitimate purposes for which that data was collected ('purpose limitation').
• limited to what is necessary in relation to the purpose ('data minimisation'); • accurate and kept up to date ('accuracy').
• kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation').

Owner: Odette Mould	Approved/Reviewed date: 12/01/2022
Approved by: The board	Review Date: 12/01/2023

Data Protection Policy

• processed in a manner that ensures security of that personal data ('integrity and confidentiality').
• processed by a controller who can demonstrate compliance with the principles ('accountability').

These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the charity will:

• observe fully the conditions regarding having a lawful basis to process personal information; • meet its legal obligations to specify the purposes for which information is used; • collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements.
• ensure the information held is accurate and up to date.
• ensure that the information is held for no longer than is necessary.
• ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018 (i.e., the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect information).
• take appropriate technical and organisational security measures to safeguard personal information.
• ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection.

Employees' Personal Information

Throughout employment and for as long as is necessary after the termination of employment, the charity will need to process data about you. The kind of data that the charity will process includes:

• any references obtained during recruitment.
• details of terms of employment.
• payroll details.
• tax and national insurance information.

Owner: Odette Mould	Approved/Reviewed date: 12/01/2022
Approved by: The board	Review Date: 12/01/2023

Data Protection Policy

• details of job duties.
• details of health and sickness absence records.
• details of holiday records.
• information about performance.
• details of any disciplinary and grievance investigations and proceedings; • training records.
• contact names and addresses.
• correspondence with the charity and other information that you have given the charity.

The charity believes that those records used are consistent with the employment relationship between the charity and yourself and with the data protection principles. The data the charity holds will be for management and administrative use only but the charity may, from time to time, need to disclose some data it holds about you to relevant third parties, for example where legally obliged to do so by HM Revenue & Customs, where requested to do so by yourself for the purpose of giving a reference or in relation to maintenance support, and/or the hosting of data in relation to the provision of insurance. In some cases, the charity may hold sensitive data, which is defined by the legislation as special categories of personal data, about you. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet the charity's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of which may cause concern or distress, you will be asked to give express consent for this information to be processed, unless the charity has a specific legal requirement to process such data.

Access to Data

You may, within a period of one month of a written request, inspect and/or have a copy, subject to the requirements of the legislation, of information in your own personnel file and/or other specified personal data and, if necessary, require corrections should such records be faulty. If you wish to do so you must make a written request to your Line Manager. The charity is entitled to change the above provisions at any time at its discretion.

Owner: Odette Mould	Approved/Reviewed date: 12/01/2022
Approved by: The board	Review Date: 12/01/2023

Data Protection Policy

Data Security

You are responsible for ensuring that any personal data that you hold and process as part of your job role is stored securely.
You must ensure that personal information is not disclosed orally, in writing, via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.
You should note that unauthorised disclosure may result in action under the Disciplinary Procedure (for employees) which may include dismissal for gross misconduct OR the Serious Misconduct procedure (for Volunteers) which may result in removal from the role.
Personal information should be kept in a locked filing cabinet, drawer, or safe. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight, for example in the boot of a car. Whilst working away from the office, either at home or at an alternative venue, i.e.: Rainbow group, you must ensure that personal data is kept with you at all times, enclosed in a folder and not accessible to any other person.

Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe. When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and, where possible, it should be locked away out of sight, for example in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When using an electronic device away from the office i.e.: at home, you must ensure your screen is facing away from any person who does not have authority to see the data you are viewing.

Notifying Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.
The following are examples of data breaches

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a data controller or data processor; • sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission.

Owner: Odette Mould	Approved/Reviewed date: 12/01/2022
Approved by: The board	Review Date: 12/01/2023

• loss of availability of personal data.

Data Protection Policy

Investigation and Notification

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by the CEO (Chief Executive Officer).
We will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required. We will undertake to notify the individual whose data is the subject of a breach if there is an elevated risk to people's rights and freedoms without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

Record of Breaches

The charity records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under the Data Protection Act 2018. It records the facts relating to the breach, its effects and the remedial action taken.

Please refer to our Data retention Schedule for further details, a copy of which can be requested by contacting Odette Mould odette@harrysrainbow.co.uk.

Owner: Odette Mould	Approved/Reviewed date: 12/01/2022
Approved by: The board	Review Date: 12/01/2023