Data Breach

At a glance

This policy sets a framework for the principles of Data Breach 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 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 sets out the obligations of Harry's Rainbow, a registered Charity in the United Kingdom under number 1194917, whose registered office is at Milton Keynes Business Centre, Hayley Court, Linford Wood, MK14 6GD ("the Charity") regarding the handling and reporting of data breaches and personal data breaches in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

Personal data is any information we can use to identify a living person. Personal data is not limited to information where someone is named and can include information relating to their online or physical lives, their location, their behaviour and interests. There is a sub section of personal data which is much more sensitive, it's called special categories of personal data and refers to information about health, race, ethnicity, religion and other beliefs, sexual orientation, genetics and biometrics, political and trade union views and memberships. This needs more care as any issue affecting this type of data

Owner: Odette Mould	Approved Date: 24.10.24
Approved by: The Board	Review Date: 24.10.25

is much more likely to have a significant effect on the individuals.

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 otherwise processed.

The Charity is under a duty to report certain types of personal data breach directly to, the Information Commissioner’s Office (“ICO”). The Charity is also required to inform individual data subjects in the case of breaches that present a high risk to them.

All personal data collected, held, and processed by the Charity will be handled in accordance with the Charity’s Data Protection Policy.

The Charity has in place procedures for the detection, investigation, and reporting of data breaches. This Policy applies to all data breaches (including personal data breaches) within the Charity and is designed to assist in both the handling of such breaches and in determining whether or not they must be reported to the ICO and/or to data subjects.

Odette Mould, CEO, odette@harrysrainbow.co.uk is responsible for the implementation of this Policy, for overseeing the handling of all data breaches, and for ensuring that this Policy is adhered to by all staff.

Scope of Policy

This Policy relates to all formats of data (including personal data and sensitive personal data collected, held, and processed by the Charity.

This Policy applies to all staff of the Charity, including but not limited to employees, agents, contractors, consultants, temporary staff, casual or agency staff, or other suppliers or data processors working for or on behalf of the Charity.

This Policy applies to all data breaches, whether suspected or confirmed.

Data Breaches

For the purposes of this Policy, a data breach means any event or action (accidental or deliberate) which presents a threat to the security, integrity, confidentiality, or availability of data.

Incidents to which this Policy applies may include, but not be limited to:

- the loss or theft of a physical data record;
- the loss or theft of computer equipment (e.g. laptop), mobile devices (e.g. smartphone or tablet), portable data storage devices (e.g. USB drive), or other data storage devices;
- equipment failure;
- unauthorised access to, use of, or modification of data (or inadequate access controls allowing unauthorised access, use, or modification);
- unauthorised disclosure of data;
- human error (e.g. sending data to the wrong recipient);

Owner: Odette Mould	Approved Date: 24.10.24
Approved by: The Board	Review Date: 24.10.25

- unforeseen circumstances such as fire or flood;
- hacking, phishing, and other 'blagging" offences whereby information is obtained by deception.

Internal Reporting

If a data breach is discovered or suspected, you should complete a Data Breach Report Form (available from Data Breach Form.docx Official documents/Policies and procedures/data breach) and send the completed form to the CEO.

A completed Data Breach Report Form should include full and accurate details about the incident including, but not limited to (where applicable):

- the time and date of the breach;
- the time and date the breach was discovered;
- the type(s) of data involved;
- where the breach involves personal data, the categories(s) of data subject to which the personal data relates (e.g. customers, employees etc.);
- whether or not any sensitive personal data is involved;
- how many data subjects are likely to be affected (if known).

Where appropriate, you should liaise with the CEO when completing a Data Breach Report Form.

If a data breach occurs or is discovered outside of normal working hours, it should be reported as soon as is reasonably practicable.

Unless and until instructed to by CEO, you should not take any further action with respect to a data breach. In particular, you should not take it upon yourself to notify affected data subjects, the ICO, or any other individuals or organisations.

Initial Management and Recording

Upon receipt of a Data Breach Report Form (or upon being notified of a data breach in any other way), the CEO shall begin by determining whether the data breach is still occurring. If this is the case, appropriate steps shall be taken immediately to minimise the effects of the data breach and to stop it.
Having established the above, the following steps shall then be taken with respect to the data breach:

- undertake an initial assessment of the data breach, liaising with the relevant staff and departments where appropriate, to establish the severity of the data breach;
- contain the data breach and, to the extent reasonably practicable, recover, amend, or restrict the availability of (e.g. by changing or revoking access permissions or by temporarily making the data unavailable electronically) the affected data;
- determine whether anything further can be done to recover the data and/or other losses, and to limit the damage caused by the breach;

Owner: Odette Mould	Approved Date: 24.10.24
Approved by: The Board	Review Date: 24.10.25

- establish who needs to be notified initially (including, if physical records or equipment have been lost or stolen, the police) as part of the initial containment;
- determine, in liaison with the relevant staff and departments, the best course of action to resolve and remedy the data breach; and
- record the breach and the initial steps taken above in the Charity's Data Breach Register.

Having completed the initial steps described above, the CEO shall proceed with investigating and assessing the data breach as described below.

Investigation and Assessment

The CEO shall begin an investigation of a data breach as soon as is reasonably possible after receiving a Data Breach Report Form (or being notified in any other way) and, in any event, within 24 hours of the data breach being discovered and/or reported.

Investigations and assessments must take the following into account:

- the type(s) of data involved (and, in particular, whether the data is personal data or sensitive personal data);
- the sensitivity of the data (both commercially and personally);
- what the data breach involved;
- what organisational and technical measures were in place to protect the data;
- what might be done with the data as a result of a breach (including unlawful or otherwise inappropriate misuse);
- where personal data is involved, what that personal data could tell a third party about the data subjects to whom the data relates;
- the category or categories of data subject to whom any personal data relates;
- the number of data subjects (or approximate number if calculating an exact number is not reasonably practicable) likely to be affected by the data breach;
- the potential effects on the data subjects involved;
- the potential consequences for the Charity;
- the broader consequences of the data breach, both for data subjects and for the Charity.

The results of the investigation and assessment described above must be recorded in the Charity's Data Breach Register.

Having completed the investigation and assessment described above, the CEO shall determine the parties to be notified of the breach as described below.

Owner: Odette Mould	Approved Date: 24.10.24
Approved by: The Board	Review Date: 24.10.25

Notification

The CEO shall determine whether to notify one or more of the following parties of the breach:

affected data subjects;

- the ICO;
- the police;
- the Charity's insurers;
- affected partners;

When considering whether (and how) to notify individual data subjects in the event of a personal data breach, the following should be considered:

- the likelihood that data subjects' rights and freedoms will be adversely affected;
- whether there is a legal or contractual requirement to notify;
- whether measures in place to protect the affected personal data (e.g. pseudonymisation or encryption) have been applied, thereby rendering the data unusable to any unauthorised parties;
- whether measures have been taken following the data breach that will ensure that a high risk to the rights and freedoms of affected data subjects is no longer likely to occur;
- the benefits to data subjects' of being notified (e.g. giving them the opportunity to mitigate the risks posed by the data breach);
- whether notifying individuals will involve disproportionate effort (in which case a public communication or other widely available notice may suffice, provided that affected data subjects will still be informed effectively);
- the best way of notifying data subjects, taking into account the urgency of the situation and the security of the possible methods;
- any special considerations applicable to certain categories of data subject (e.g. children or vulnerable people);
- the information that should be provided to affected data subjects;
- how to make it easy for affected data subjects to contact the Charity to find out more about the data breach;
- further assistance that the Charity should provide to the affected data subjects, where appropriate;
- the risks of over-notifying – not all data breaches require notification and excessive notification may result in disproportionate work and numbers of enquiries from individuals.

When individual data subjects are to be informed of a data breach, those individuals must be informed of the breach without undue delay. Individuals shall be provided with the following information:

- a user-friendly description of the data breach, including how and when it occurred, the

personal data involved, and the likely consequences;

- clear and specific advice, where relevant, on the steps individuals can take to protect themselves;
- a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects;
- contact details for the CEO from whom affected individuals can obtain further information about the data breach.

When considering whether (and how) to notify the ICO of a data breach, the following should be considered:

- the risk and potential harm to data subjects, their rights, and freedoms – harm can include (but is not limited to) financial harm, physical harm, loss of control over personal data, discrimination, identity theft or fraud, damage to reputation, and emotional distress;
- the volume of personal data involved – the ICO should be notified if a large volume of data is involved and there is a real risk of data subjects suffering harm as a result, however it may also be appropriate to notify the ICO if a smaller amount of high-risk data is involved;
- the sensitivity of the data involved – the more sensitive the personal data is, the less the volume of it is relevant and if the data breach presents a significant risk of data subjects suffering substantial detriment or distress, the ICO should be notified.

If the ICO is to be notified of a data breach, this must be done within 72 hours of becoming aware of the breach, where feasible. This time limit applies even if complete details of the data breach are not yet available. The ICO must be provided with the following information:

- the category or categories and the approximate number of data subject whose personal data is affected by the data breach;
- the category or categories and the approximate number of personal data records involved;
- the name and contact details of the CEO from which the ICO can obtain further information about the data breach;
- a description of the likely consequences of the data breach; and
- a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects.

The police may have been contacted at an earlier point in the data breach procedure, however further investigation may reveal that the data breach resulted from a criminal act, in which case the police should be further informed.

Records must be kept of all data breaches, regardless of whether notification is required. The decision-making process surrounding notification should be documented and recorded in the Charity's Data Breach Register.

Owner: Odette Mould	Approved Date: 24.10.24
Approved by: The Board	Review Date: 24.10.25

Evaluation and Response

When the steps set out above have been completed, the data breach has been contained, and all necessary parties notified, the CEO shall conduct a complete review of the causes of the data breach, the effectiveness of the measures taken in response, and whether any systems, policies, or procedures can be changed to prevent data breaches from occurring in the future.

Such reviews shall, in particular, consider the following with respect to data (and in particular, personal data) collected, held, and processed by the Charity:

- where and how data is held and stored;
- the current organisational and technical security measures in place to protect data and the risks and possible weaknesses of those measures;
- the methods of data transmission for both physical and electronic data and whether or not such methods are secure;
- the level of data sharing that takes place and whether or not that level is necessary;
- whether any data protection impact assessments need to be conducted or updated;
- staff awareness and training concerning data protection.

Where possible improvements and/or other changes are identified, the CEO shall liaise with the Board with respect to the implementation of such improvements and/or changes.

Policy Review and Implementation

This Policy will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.

This Policy shall be deemed effective as of 20th December 2022. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Owner: Odette Mould	Approved Date: 24.10.24
Approved by: The Board	Review Date: 24.10.25