IT Security Policy

At a glance

This policy sets a framework for the principles for our IT Security.

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. The Board will take steps to ensure staff, volunteers and board members are provided with an updated version of this policy at any point it is amended.

Staff, volunteers and board members are required to provide a signed copy to their manager/supervisor or CEO as appropriate at any amendment point to evidence they understand the document and any changes made.

Introduction

This document sets out the measures to be taken by all employees/volunteers/members of the Board of Harry's Rainbow (the "Charity") and by the Charity as a whole in order to protect the Charity's computer systems, devices, infrastructure, computing environment and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate, or accidental

Key Principles

All IT Systems are to be protected against unauthorised access.

All IT Systems are to be used only in compliance with relevant Charity Policies.

Owner: CEO & Board	Approved Date: 02.10.24
Approved by: CEO & Board	Review Date: 02.10.25

All employees/volunteers of the Charity and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors (collectively, “Users”), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

All line managers must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times.

All data stored on IT Systems are to be managed securely in compliance with all relevant parts of EU Regulation 2016/679 General Data Protection Regulation (“GDPR”) and all other laws governing data protection whether now or in the future in force.

All data stored on IT Systems are to be classified appropriately (including, but not limited to, personal data, special categories of personal data, and confidential information. All data so classified must be handled appropriately in accordance with its classification.

All data stored on IT Systems shall be available only to those Users with a legitimate need for access.

All data stored on IT Systems shall be protected against unauthorised access and/or processing.

All data stored on IT Systems shall be protected against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by our IT Support company (“IT Support”).

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the IT Support unless expressly stated otherwise.

All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the IT Department. Any breach which is either known or suspected to involve personal data shall be reported to the Data Protection Lead, the CEO.

All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the CEO.

CEO Responsibilities

The CEO shall be responsible for the following:

- ensuring that all IT Systems are assessed and deemed suitable for compliance with the Charity’s security requirements;
- ensuring that IT security standards within the Charity are effectively implemented and regularly reviewed, working in consultation with the Charity’s Managers and reporting the outcome of such reviews to the Charity’s Trustees;
- ensuring that all Users are kept aware of the requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the GDPR and the Computer Misuse Act 1990.

The Managers shall be responsible for the following:

- assisting all Users in understanding and complying with this Policy;
- providing all Users with appropriate support and training in IT security matters and use of IT Systems;
- ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;
- receiving and handling all reports relating to IT security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the CEO;
- taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;
- assisting the CEO in monitoring all IT security within the Charity and taking all necessary action to implement this Policy and any changes made to this Policy in the future.

Users Responsibility

- All Users must comply with all relevant parts of this Policy at all times when using the IT Systems.
- All Users must use the IT Systems only within the bounds of UK law and must not use the IT Systems for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.
- Users must immediately inform the CEO of any and all security concerns relating to the IT Systems.
- Users must immediately inform the CEO of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.
- Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Charity's disciplinary procedures.

Software Security Measures

- All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases will be applied at the sole discretion of the IT Support company. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release, falling within the remit of new software procurement and outside the scope of this provision.
- Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied. [If the security flaw affects, is likely to affect, or is suspected to affect any personal data, the CEO shall be informed immediately.

- No Users may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the CEO. Any software belonging to Users must be approved by the CEO and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.
- All software will be installed onto the IT Systems by the IT Support company unless an individual User is given written permission to do so by the CEO. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

Anti-Virus Security Measures

- Most IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up-to-date with the latest software updates and definitions.
- All physical media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred. Such virus scans shall be performed automatically upon connection. Any external media (USB etc) is only to be used with the strict permission of the CEO and should only be on charity issued media which will be secure, protected and encrypted.
- Where any virus is detected by a User this must be reported immediately to the CEO (this rule shall apply even where the anti-virus software automatically fixes the problem). The CEO shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be as soon as possible to limit disruption to the User.
- Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Charity’s disciplinary procedures.

Hardware Security Measures

- Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised access to such locations for any reason.
- All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.
- All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided

by the Charity should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location [other than their private homes or Charity premises]. If any such mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment.

- All devices issued by or authorised for use by charity staff/volunteers will be encrypted and where those devices are not owned by the charity will be required to have regular updates and security patching applied.
- All charity owned devices will be maintained and security patching applied on a regular basis and staff issued with the devices should expect to have to return the device to the charity premises on occasion for this work if necessary
- The CEO/IT Support company shall maintain a complete asset register of all IT Systems.

Access Security

- Access privileges for all IT Systems shall be determined on the basis of Users' levels of authority within the Charity and the requirements of their job roles. Users shall not be granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.
- All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode.
- All passwords must, where the software, computer, or device allows:
  - be at least 8 characters long;
  - ideally by three random words with an upper case and a symbol;
  - be changed at least every 6 months, unless you know a data breach has occurred in which case it must be changed immediately;
  - be different from the previous password;
  - not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.); and
  - be created by individual Users.
- Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone, including the CEO or other members of staff. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password, they should change their password immediately [and report the suspected breach of security to the CEO.
- If a User forgets their password, this should be reported to the IT Support company. The they will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of

the IT Support company responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.

- Where deemed appropriate the charity will use multifactor authentication for access to systems and data. Staff/volunteers/board members will be required to follow the instructions provided where this type of authentication has been deemed necessary.
- All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after 5 minutes of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).
- All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Charity shall be set to lock, sleep, or similar, after 5 minutes of inactivity, requiring a password, passcode, or other

Data Storage Security

- All data, and in particular personal data, should be stored securely using passwords and/or data encryption.
- All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Charity or otherwise without the formal written approval of the CEO and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.
- No data, and in particular personal data, should be transferred to any computer or device personally belonging to a User unless the User in question is a contractor or sub-contractor working on behalf of the Charity and that User has agreed to comply fully with the Charity's Data Protection, BYOD Policy and the GDPR.

Data Protection

- All personal data (as defined in the GDPR) collected, held, and processed by the Charity will be collected, held, and processed strictly in accordance with the principles of the GDPR, the provisions of the GDPR and the Charity's Data Protection Policy.
- All Users handling data for and on behalf of the Charity shall be subject to, and must comply with, the provisions of the Charity's Data Protection Policy at all times. In particular, the following shall apply:
    - All emails containing personal data must be encrypted/or password protected;
    - All emails containing personal data must be marked "confidential";

    - Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;

- All personal data to be transferred physically, including that on removable electronic media, shall be transferred only using approved encrypted removable media and only where necessary. Steps must be taken by staff/volunteers/board members to ensure the security of those devices.
- Where any confidential or personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it.
- Any questions relating to data protection should be referred the CEO.

Policy Review

The Charity shall review this Policy not less than yearly and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this Policy should be communicated to CEO.

Owner: CEO & Board	Approved Date: 02.10.24
Approved by: CEO & Board	Review Date: 02.10.25