Information Security Policy – Hope4 (Rugby) Ltd 2019

The security of the information we hold & the systems we use to handle it are extremely important to us. With the development of new technologies & new ways of working comes the challenge of keeping the information we hold & use secure. This policy aims to set out how we will go about maintaining our cyber security and dealing with the challenges presented by the technologies we use.

1) Definitions:

i) We or us refers to Hope4 Rugby Ltd

ii) Personal Data;

(i) Personal data only includes information relating to natural persons who:
(ii) can be identified or who are identifiable, directly from the information in question; or
(iii) who can be indirectly identified from that information in combination with other information.
(iv) Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and we may only process them in more limited circumstances.

iii) Hardware;

(i) These are the physical elements which make up a computer, laptop, tablet or computer system like server, switch, router, network attached storage.

iv) Software;

(i) Software is a generic term used to describe computer programs. Scripts, applications, programs and sets of instructions which tell hardware what to do & how to do it are all software. In this context Firmware is taken to be software. Firmware is software which is permanently or semi-permanently installed in hardware.

v) User Resource;

(i) This is taken to be a device like PC, Laptop, tablet or mobile phone

vi) Encryption;

(i) A method of scrambling data to make it unrecognisable and not decipherable by anyone without a special decryption key. It ensures that any intercepted data on public networks like the internet cannot be read.

vii) Data Loss;

(i) This is taken to mean the destruction or misplacement of data from where it would normally be stored.

viii) Backup;

(i) This is taken to be the copying of physical or virtual files or databases to a secondary location for preservation in case of equipment failure or disaster. The process of backing up data is pivotal to a successful disaster recovery plan.

ix) Cloud Storage;

(i) This is taken as a data storage model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on a storage server.

x) Data transmission;

(i) Data transmission is the process of sending digital or analogue data over a communication medium to one or more computing, network, communication or electronic devices. It enables the transfer and communication of devices in a point-to-point, point-to-multipoint and multipoint-to-multipoint environment. Data transmission is also known as digital transmission or digital communications.

(ii)

xi) Electronic Messaging;

(i) This is taken to include but is not limited texting, emailing, tweeting messaging as a generic method of contacting.

xii) Malware

(i) Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software. The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware, among other terms. Malware has a malicious intent, acting against the interest of the computer user—and so does not include software that causes unintentional harm due to some deficiency, which is typically described as a software bug.

2) Personal data – see Data Protection Policy

i) How we deal with Personal Information is covered on the Hope4 (Rugby) Ltd Data Protection Policy

3) Financial data – see Data Protection Policy

i) How we deal with Financial Information is covered on the Hope4 (Rugby) Ltd Data Protection Policy

4) Hardware security –

a) Network Infrastructure is taken to mean server, switches, routers, wireless access points & cabling

i) These will only be accessed on a 'Need to' basis, generally this will be by the Director or anyone designated by him/her. From time to time under the IT Directors control trusted 3rd parties will be allowed to access the server, switch, router wireless access points for the purpose of modifying settings or software.

b) All IT User Resources – to include Desktops, laptops, tablets and mobile phones

i) All users will have a unique account identity within Hope4 (Rugby) Ltd. Users must only use their User Account login details to access a Hope4 (Rugby) Ltd IT resource.

ii) All users must logout or lock a resource when they move away from it. This is to prevent other people accessing your resources.

iii) Passwords for User Accounts must comply with Sect. 6 part b ii below. They should not be shared with other people.

iv) USB memory devices must be either password protected or encrypted or preferably both. They should not routinely be used to move data from one place to another & should not be used to remove data from Hope4 (Rugby) Ltd.

v) Data, images, video & audio are currently stored on local machines but once a network is installed data will not be stored locally, any left on the local machine will be wiped at regular intervals. It is the user's responsibility to ensure that data is saved in the correct place.

vi) In using Hope4 computers & infrastructure any documents downloaded for printing or printed directly from another source should be deleted. Any documents that have been downloaded for printing or printed directly from another source and are left open on a Hope4 (Rugby) Ltd hardware can be added to the Clients file or deleted. If any such documents are saved onto a Hope4 (Rugby) Ltd computer then they can be added to the Clients file or deleted, whichever assists Hope4 (Rugby) Ltd to best help the Client. If they are added to the Clients file then they will be treated in accordance Hope4 (Rugby) Ltd's Data Protection Policy.

c) Laptops & tablets

i) Hope4 (Rugby) Ltd laptops taken off site must be adequately protected for loss of data and loss of device. Offsite laptops should not be used by anyone other than the Hope4 (Rugby) Ltd person. They may not be lent to or used by anyone other than the Hope4 (Rugby) Ltd user.

ii) The items 4b i – v for Desktops above equally apply to laptops.

d) Mobile phones

i) Hope4 (Rugby) Ltd mobile phones will be password protected with a complex password which complies with Sect 6 part b ii

ii) Personal mobile phones **should not** be used for any Hope4 (Rugby) Ltd business activities. If personal mobile phones are brought onto Hope4 (Rugby) Ltd premises or taken to Hope4 (Rugby) Ltd activities, then the owner is entirely responsible for them. Hope4 (Rugby) Ltd cannot be held responsible or liable for the mobile phone's loss, damage or misuse.

iii) Personal mobiles phones should never be used to store Hope4 (Rugby) Ltd data of any description this includes images, video & audio.

iv) Where Hope4 (Rugby) Ltd mobile phones are used to store data, images, video or audio then the data should be stored on the phone for the shortest possible time commensurate with the task it is being used for.

e) Media

i) Video

CCTV is used at the Hope Centre for security & Safety of Clients, Staff & volunteers. The cameras record 24 hours a day. The video is stored on a digital recorder and the recordings are kept for 30 days before being over written. The video footage is password protected and can only be played back, stored for longer, copied or deleted manually by the ICT Director, Buildings Manager or Centre Manager. The images are not available over the internet.

ii) Images

Static images of Clients are taken & used for their records to enable accurate & correct identification of the individual. They are taken and stored on Hope4 (Rugby) Ltd equipment only, except for INFORM, which is covered by a service level agreement with Homeless Link. Images once taken are stored as part of the Client's record and are treated in line with our Data Protection Policy. See also Hope4 (Rugby) Ltd Data Brotection Policy

iii) Audio

Any Audio files recorded either to enable accurate identification of a Client or with consent as a record of a meeting will be delt with like any other data for the purpose of Data Protection.

iv) Storage

CCTV Video will be stored electronically on site for 1 month before deletion unless it is required for an investigation. If required for an investigation the CCTV recording will be kept until such time as all processes relating to the investigation have been exhausted.

v) Usage

CCTV will NOT be used to invasively spy on any Client, volunteer, Staff, Director or visitor. It will be used solely for the purposes of safety & security.

5) Software security –

a) Installation

i) Software can only be installed on Hope4 (Rugby) Ltd resources by the IT Director or someone appointed by him/her. Any attempt to install software without the IT Directors permission will be treated a a Major Breach of Trust.

ii) Downloading programmes, software or apps is not allowed.

iii) No attempt should be made to interfere, change, rewrite or modify software already installed on Hope4 (Rugby) Ltd resources. Any attempt to do this will be treated a a Major Breach of Trust.

iv) The construction of software from scratch on any Hope4 (Rugby) Ltd resource is not allowed.

v) Any attempt to use software licence keys or software from Hope4 (Rugby) Ltd resources elsewhere is forbidden and will be treated a a Major Breach of Trust.

b) Updating

i) Updating or upgrading of software will be carried out by the IT Director or by a person appointed by him/her

c) Usage

i) Hope4 (Rugby) Ltd software may only be used for the purposes for which it was intended. Attempts to subvert Hope4 (Rugby) Ltd software are not allowed and taken as a breach of trust.

6) Internet security –

a) Usage

i) This applies to all Employees, Volunteers Clients, Visitors, Directors or visitors who use the Hope4 (Rugby) Ltd hardware & if appropriate their own hardware to access the internet for information related to the purpose of the charity. They may not;

(1) Visit sites which encourage or display Pornography, racist, sexist or extremist material or material encouraging hate crimes or material which is offensive to other users.

(2) Look for or try to download information in (1) above from sites. If they do so it will be treated as a Breach of Trust of this Policy. Such behaviour could result in disciplinary action by the Hope4 (Rugby)Ltd If the activity is illegal Hope4 (Rugby) Ltd will inform the Police or other statutory authorities.

ii) Client usage of Hope4 (Rugby) Ltd hardware will have regard to a fair use policy. When there are more clients wanting to use resources than there are machines then rationing will take place on a 15-minute rota basis.

iii) Employees, Volunteers Clients, Visitors & Directors may not;

(1) Download or upload obscene, offensive or illegal material.

(2) Send confidential information to unauthorized recipients.

(3) Invade another person's privacy and sensitive information.

(4) Download or upload movies, music and other copyrighted material and software.

(5) Visit potentially dangerous websites that can compromise the safety of Hope4 (Rugby) Ltd.'s network and/or computers.

(6) Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

b) Passwords

i) Passwords must be used when logging onto any Hope4 (Rugby) Ltd IT resource. Any accounts which are created as part of an employees', volunteers', clients', visitors' or Directors' normal activities at Hope4 (Rugby) Ltd will be subject to the following;

ii) Complexity

(1) More than 8 characters

(2) Uses at least one from each of the following; uppercase, lowercase letters, numbers special characters [!%&()?#-_+*]

iii) Passwords must never be disclosed to other people, must be stored securely & never sent over any insecure connection (email or text without encryption).

c) Electronic Messaging

i) Content

Electronic messages sent from or on behalf of Hope4 (Rugby) Ltd should contain accurate, truthful information, which is not personally defaming, insightful, hateful or illegal. They should not contain personal information unless the electronic message is 'End to End' encrypted ie Whatsapp or encrypted emails.

ii) Usage

Hope4 (Rugby) Ltd resources are meant to be used for Hope4 (Rugby) Ltd business only. The sending & receiving of Electronic Messages generates a log, which will include the messages, this should not be deleted or tampered with in any way.

iii) Security

(1) Hope4 (Rugby) Ltd uses commercial Security Software as well as a hardware Firewall device to protect networked devices, however care should be taken when open messages, however they are transmitted

(2) Emails which are unsolicited & from an unrecognised source should not be opened. Caution should be exercise when opening any email attachment. Be suspicious. If it doesn't look right, then it properly isn't.

(3) If personal information has to be transmitted electronically then it has to be encrypted 'End to End' and it is the sender's responsibility to ensure this.

d) sites visited

i) Type

(1) Clients, Volunteers, Staff, Directors & visitors may use Hope4 (Rugby) Ltd IT infrastructure primarily to gather, store and use information pertinent to the business of Hope4 (Rugby) Ltd or themselves in the role they have whilst working with Hope4 (Rugby) Ltd.

(2) They may NOT visit sites which are channels of hate, fear or radicalisation. They may not visit pornographic sites whether legal or illegal on any of Hope4 (Rugby) Ltd resources.

(3) They may NOT visit sites which are linked to the distribution of any type of Malware.

7) Disaster management –

a) Backups

i) Hope4 (Rugby) Ltd data will be backed up on a regular schedule to ensure that in the event of a data disaster the loss will be minimal.

ii) Backups will be made and stored locally & remotely. The remote location will be made using a commercial cloud location within the UK or EU.

iii) Backups of Hope4 (Rugby) Ltd data will take place daily. Data left on local machines will be wiped at regular intervals.

iv) Backups & the backup schedule will be the responsibility of the IT Director

v) Recovering lost data will be the responsibility of the IT Director.

b) Storage

i) Currently data is stored on individual PCs, laptops, tablets or phones electronically. It is also stored in 'The Cloud' using commercial providers. All of this data, whether personal or otherwise is password protected. Hope4 (Rugby) Ltd is moving to encrypting all data but are not there yet. Any personal paper information is stored in locked filing cabinets with access limited to the Centre Manager, Key Workers, Directors or others as authorised by the Centre Manager or the Directors.

c) Data breach

i) A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

ii) Personal data breaches can include:

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

(ICO Website; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/)

iii) If a data breach is suspected an investigation will be conducted by either the ICT Director, a Director or the Centre Manager

iv) If a personal data breach has occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there is a risk then we will notify the ICO; if it's unlikely then we will not report it. However, if we decide not to report the breach, we will justify this decision and document our decision and the evidence which lead to it in a timely manner. See also Hope4 (Rugby) Ltd data Protection Policy.

(1) In assessing the risk to rights and freedoms, we will focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

> *"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."*

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job.

Other breaches can significantly affect individuals whose personal data has been compromised. We will assess this case by case, looking at all relevant factors.

d) Data loss recovery
   i) Electronic data loss is currently mitigated by using off site 'Cloud' based back up systems. However, some PCs for staff at the Hope Centre have attached USB drives which back up local files.
   ii) Recovery will have to be initiated manually once an electronic data loss is identified. A more comprehensive solution will be implemented when we install our own Networked resources.

e) Malware
   i) If malware is suspected on any Hope4 (Rugby) User Resource the IT Director should be informed immediately. No attempt to open or remove it should be undertaken without express permission of the IT Director.

8) Actions & Consequences –

a) Breaches of this policy will be viewed as breaches of trust and are likely to fall into 3 categories, which will be handled in the ways outlined below. All breaches of this policy will be treated seriously as the reputational & informational damage to Hope4 (Rugby) Ltd could be catastrophic.

b) Any breach of trust when reported to the ICT Director will be investigated to establish the facts. If it is deemed necessary then the person/people involved in the breach can be suspended and instructed not to communicate with anyone in Hope4 (Rugby) Ltd except the ICT Director the Chair, the Secretary or the Treasurer. Suspension, if used, will not imply any guilt. It is simply to ensure that as much clean evidence as possibly can be obtained before a decision is made.

c) A minor breach of trust

(1) This is likely to be but not exclusively;
(2) Leaving computers unlocked, whilst unattended
(3) Leaving files where unauthorised people can see them.

ii) Consequences of minor breach of trust

(1) The person will be spoken to by the Centre Manager or one of the Directors and taken through some training relevant to the breach. The Minor Breach will be documented and regarded as 'Spent' 1 year after the event.

d) A major breach of trust

(1) Likely to include but not exclusively
(2) Persistent minor breaches of trust
(3) Removing data without authorisation
(4) Loosing or misplacing a password protected but not encrypted memory stick, laptop or phone, belonging to Hope4 (Rugby) Ltd
(5) Failing to adequately password protect any device with Hope4 (Rugby) Ltd data on it.
(6) Failing to secure paper files
(7) Loading Hope4 (Rugby) Ltd data onto any unauthorised device or service.

ii) Consequences of major breach of trust.

(1) A formal warning would be given, and a note attached to the individual records which will be regarded as 'spent' 1 year after the event.

Patron: The Right Rev Dr Christopher Cocksworth, Bishop of Coventry

Hope4 (Rugby) Ltd, The Hope Centre, 8 Newbold Road, Rugby CV21 2LJ
Registered Charity in England and Wales (1126487)
Company Limited by Guarantee (6614898)

COMMUNITY FUND
foodbank

e) A gross breach of trust

(1) Deliberate sharing of Hope4 (Rugby) Ltd information, whether digital or paper without the express knowledge & permission of The Centre Manager, or IT Director or Directors. In the case of the Centre Manager then the IT Director or Directors would need to give permission.

(2) Any attempt to compromise the security or integrity of the data or the IT infrastructure held or owned by Hope4 (Rugby) Ltd

(3) 2 major breaches of trust

ii) Consequences of gross breach of trust

(1) Staff – This will be treated as Gross Misconduct & dealt with under the Disciplinary Policy, which could include dismissal.

(2) Volunteers – will be spoken to by the Centre Manager and a Director with a view to stopping them volunteering with Hope4 (Rugby) Ltd.

(3) If the breach involved any illegal activity Hope4 (Rugby) Ltd would report this to the relevant Statutory Authority with a view to supporting a criminal prosecution.

The Legal Framework for this policy is derived, primarily, from the following legislation

1) Computer Misuse Act 1998 amended 2015
2) Data Protection Act 1998
3) General Data Protection Regulations 2018

To be available online & from the Hope Centre

Review date: **Every 3 years unless the law changes**

Agreed by the Board of Trustees May 2019

Signed:

Date: 8th May 2019