Helping Hands

POLICY (POL)

Title of Policy	Information Security (Inc Cyber Security)		
What type of document is this?	Policy (POL)	Policy Reference Number	HHH-POL-082
Purpose of POL	This policy sets out the organisational commitment and approach to Information Security (including Cyber Security) at Helping Hands. In more detail, our purpose is four-fold. • Establishing a clear framework for managing and protecting information assets, ensuring that everyone understands their roles and responsibilities in maintaining security for our business and customers. • Preventing security breaches through detecting and preventing the misuse of data, networks, computer systems, and applications, thereby reducing the risk of security incidents. • By protecting business reputation and ensuring compliance. Helping our first line of defence, our team members, understand the acceptable use of IT resources, helping team members understand what is appropriate when accessing and handling company data, together with providing them with Cyber Security Awareness Training on an annual basis.		

ROLES AND RESPONSIBILITIES Include in this section details of the key roles and associated responsibilities relevant to the document	
Roles	Responsibility
Chief Financial Officer, Supported by the IT Director	The custodian of this document. Responsible for the following: • Creation and development of the Information Security policy. • Maintenance and updates of the policy where appropriate. • Communicate the policy and any such updates, to all relevant stakeholders. • Ensure compliance and enforcement. • Ensure training and support for all team members where relevant. • Keep detailed records of policy reviews, changes and updates.
Head of Service Delivery	To provide updates and changes where relevant relating to the live IT service, including Infrastructure and Systems
Head of Data & Analytics	To provide updates and changes where relevant relating to data and analytics
Head of Digital	To provide updates and changes where relevant relating to digital services
Scope of POL	This policy is operationally relevant to anyone with a role that involves assuring the security of information at Helping Hands, and includes external partners providing technology services.

Table of Contents

1.0 Framework for Information Security

1.1 Information Security (including Cyber Security)

Information Security (Infosec) is the practice of protecting information by identifying and mitigating information risks. Information risks are not limited to straight forward security breaches ('hacking') but can affect any of the three elements of the Infosec 'Triad' of:

- Confidentiality
- Integrity
- Availability

1

1.2 The Information environment at Helping Hands

The nature of Helping Hands operations requires us to process special category (sensitive) data of vulnerable individuals as part of our core operations. With this comes a high duty of care and a moral responsibility to protect the privacy and dignity of those we support.

In addition to the moral responsibility, the nature of our work brings specific legal and regulatory responsibilities that we must be aware of and meet the requirements.

Appropriate information security is essential to protect the company operations and, where information is personal, is a legal requirement under data protection legislation.

Information risks cannot be eliminated, and so devising Information security controls requires ongoing review and judgement as to what is 'appropriate'. This judgement includes balancing the availability of technical controls to the financial and operational costs to the company.

[1] Diagram credit: The CIA Triad – Interests and Insights (jamestyson.co.uk)

1.3 Information Security as part of the Information Governance Framework

Information Security is one of the three governance streams that together constitute the Information Governance Framework at Helping Hands.

- Data Protection
- Information Security
- Customer data and Records Management

1.4 Resourcing

The Executive Committee will ensure that Information Security, as maintained and delivered by the IT resources within the business and under the leadership of the IT Director, has appropriate time, skills and resources to adequately meet the objectives of the Company, and in line with key risks as set out in the Corporate Risk Register.

1.5 Ownership

Information Security is owned by the Chief Financial Officer, supported by the IT Director and reports to the Executive Committee.

1.6 Objectives

Ensure compliance with Cyber Essentials with a scope of "whole organisation". The six key controls of which are:

  - Boundary firewalls and internet gateways
  - Malware protection
  - Security update management
  - Secure configuration
  - Access control
  - Device currency (laptops, desktops, mobile, tablets)
- Own Information Security and Cyber Security risks.
- Escalate risks to the Executive Committee, and ultimately to the Board where they cannot be accepted by the owner

Cyber Essentials is a government-backed, industry-supported scheme to help organisations protect themselves against common online threats and has two levels of certification.

Cyber Essentials - Level 1 – self-certification against the above six control areas

Cyber Essentials Plus - Level 2 – an independent external audit, covering all six control areas with an evidence based assessment determining compliance. In the instance of non-compliance, Cyber Essentials Plus certification will not be awarded, and defined remediation advised.

1.7 Scope

- All company data.
- The "whole organisation"
- Hardware devices including:
  - Servers, Laptops, Desktops, Printers, Network, Tablets and Mobile Phones.

2.0 Managing IT Assets

2.1 IT Asset Register

We will maintain an asset register of all IT hardware devices that are in use including laptops, smart phones, firewalls and routers. This will be maintained and reviewed annually.

2.2 Software Assets

- We will maintain a record of software that is in use across the company. This will indicate where software is likely to fall out of support in the next 12 months.
- Software will be configured to auto-update for all security updates. Users should not disable these auto updates.
- Software that is no longer in support will be retired
    - Where software is essential, but unsupported, it will be configured to be outside of the controlled network with appropriate firewalls between the secure environment and the unsupported software.

2.3 Data flow diagram

We will maintain an up-to-date data flow diagram to illustrate the scope of the company IT and data estate and to identify the main systems and data stores in use and how they integrate with each other.

2.4 Virtualised environments

Virtualised environments (either self-hosted or using commercial IaaS Cloud providers) are in scope of Cyber Essentials and are configured for security and privacy to the same standards as if they were physical networks.

3.0 Boundary Protection

3.1 Network, Firewalls and Gateways

- We utilise firewalls, with intrusion detection/ prevention systems provided by our external partners, together with antivirus (currently Defender Plan 1 and 2) appropriate software to protect the network and endpoints.
- We segregate the network to limit the impact of security breaches.
- We maintain secure firewalls and gateways at all points where data flows in, or out of the secure controlled network.
- All firewalls and gateways will have the default password changed and will use a strong password in line with the company's password requirements.
- Devices that allow for configuration from outside the secure network will have management from 'the internet' disabled so that changes can only be made from within the secure network.
    - Where not possible, or remote access is a requirement (e.g. to allow a third-party company to configure the device) the access is limited to a particular IP address or similar restrictions to minimise the risk.

3.2 Incoming internet traffic

- All incoming traffic to the secure network will be blocked by default. This is operated by zero trust – incoming and outgoing traffic is restricted to only relevant business traffic.
- Incoming Traffic will only be allowed for Permitted services
    - A register of Permitted services is maintained by our external partners.
    - The IT Director must approve any new Permitted Services – example, firewall rule changes for the recent penetration test with CSA.
    - Permitted Services will be locked down using IP Address filters or other similar technologies to minimise the risk of the exposed services.
    - The list of Permitted Services is reviewed annually.

4.0 Cloud Services

Cloud services refer to software or platforms that are hosted on the internet (outside of the secure controlled network) that hold or process company data. HH leverages external partners for our primary Cloud Platforms, and similarly SAAS for our primary applications

Only pre-approved cloud services will be used

- The IT Director will maintain and make available a list of permitted cloud services.
    - This list will identify the nature of the service e.g. IaaS, PaaS or SaaS
- All cloud services are configured to use MFA or similar protections such as a link to single sign-on (SSO) with the company's centralised authentication system.
- Cloud services will allow appropriate access controls to be configured, for example separating administrative user features from patient data access

5.0 Secure Configurations

All systems in use will have their configurations reviewed to consider the security implications and to implement a secure configuration. This includes:

- Only having active user and system account active that are needed and in use.
    - This includes on local systems and also permitted cloud services.
    - User accounts must be maintained on an ongoing basis and reviewed by system owners at least on an annual basis.
    - Unused accounts must be removed or blocked. Where devices have an auto-play or auto-run feature for removable media, this will be disabled.
- Mobile devices have a compulsory PIN code or equivalent locking mechanisms in-line with the requirements of the Mobile Device policy
- There must be no shared user accounts. Every user must login to systems with unique credentials that accurately identify the true user of the system.
- Systems will be configured to protect against 'brute force' (password guessing) attacks

- Depending on the system this may be through any combination of throttling authentication, applying MFA or account locking after multiple failed log-in attempts.
- Mobile devices and laptops will have device-level encryption

6.0 Malware Protection

Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems. It presents a very high risk to company data and the integrity of company systems.

- All systems have the installation and running of Anti-virus (Defender Plan 1 and 2) software enforced.
  - Where it cannot be enforced, it should be monitored to ensure that it is in use and updated.
  - Update to malware definitions are automatic and enforced on a regular basis.
- The installation of applications on to devices will be restricted to administrative users
  - Applications will only be installed from trusted, authoritative sources
- Mobile devices do not require anti-malware software as long as installation of applications is only possible from the authoritative mainstream application stores such as Google Play Store or the Apple App Store as examples.
  - 'Rooted' devices (ones which have been modified to gain more control) are never permitted to access systems that contain company data.
- Any suspicious software activity or behaviour must be reported to the TechTeam immediately who will investigate and resolve any issues in conjunction with our external cyber partners

7.0 User Accounts

7.1 Joiner / Mover / Leaver processes

Joiners

When a new employee, contractor or volunteer joins Helping Hands, the hiring manager will work with the People team to raise the ticket to ensure that the user is configured to have access to only the systems required for their role.

This includes configuring their access controls and any personal and mobile device settings are appropriate and in-line with this Information Security Policy.

Post Change

When a person changes job role, the line manager will work with the People Team to review and make appropriate changes to the user's access controls, through triggering a ticket for access. This must also include the removal of access that is no longer required

Leavers

When a person leaves, access must be removed immediately. Account login should be disabled first and foremost through raising a leaver request within the appropriate system, currently SelectHR. Where this is not possible, or access is required for other users, the password should be reset immediately via raising a ticket with TechTeam.

Where the leaver had access to one or more systems with shared credentials (e.g a network configuration device or a payment system), all of these login credentials must also be disabled / reset.

7.2 Access control register

We will keep and maintain a record of which service and systems each user account has access to.

- We aspire to have an industry recommended role-based access control (RBAC) to ensure employees have the minimum access necessary to perform their job

functions. We currently have a hybrid mode, and we will have Entra (Microsoft) enabled in 2025.

- We regularly review and update access permissions where appropriate.
- We use multi-factor authentication (MFA) for accessing sensitive information and systems.
- We will carry out an independent annual audit of all access permissions utilised to access sensitive customer / employee data at Helping Hands.

7.3 Administrator accounts

Administrator accounts of differing systems have different levels of control. Generally, an account that has any of the following should be considered to be an administrative account:

1. The ability to add new users or remove existing users
2. The ability to increase the amount of data or privileges that existing user is able access
3. Is able to access or delete the data on a bulk or systematic basis of other system users

- The creation and allocation of administrative accounts should be approved by Head of IT Service Delivery.
- A central record of which administrative accounts exist on what system will be maintained.
- A quarterly review and check of the administrative accounts active, will result in a physical sign-off to confirm the elevated permissions are still required for the work being undertaken.
- All users will have separate accounts should they require access to administrative features.
    - Business-as-usual accounts (e.g. accounts used for routine day-to-day activity such as email) do not have administrative access.

8.0 Backup and Disaster Recovery of IT Services

8.1 Business continuity and Disaster Recovery plan

- The company has created and evolved the (IT) disaster recovery and business continuity plan for the IT estate. This dovetails with the wider business BCP processes.
- The IT disaster recovery plan is reviewed and verified for suitability annually, as a minimum, including testing (and testing results) where appropriate, with our external partners.
- The Business Continuity Plan has undergone a significant change over the last year, and is now into a quarterly test cycle of incident recovery plans.
- These are reviewed to ensure that they are both entirely compatible with the organisational business continuity and disaster recovery plans where managed separately with external partners from the overall plans, and the evolution of the technology stack – as an example, on-premise to Cloud.

8.2 Backups

- Data stored in cloud services have an external backup solution for disaster recovery purposes. This will not rely entirely on the cloud providers own processes.
- Backups are tested every 12 months to ensure the veracity and recoverability of the data and a report generated for Helping Hands by our external partners where they document the process and findings of both the on premise and cloud based restores.
    - There are 3 separate back-up approaches:
        - Keepit Saas – backs up Exchange Online, SharePoint and Teams through the RMM directly into the tenant on a daily basis
        - Azure – backed up locally in the UK South zone (with an alternative UK DR zone).
        - StorageCraft/Acronis – StorageCraft is backing up to the local storage repository for quick restores, where Acronis is backing up to the cloud storage for air gapped backups

8.3 Cyber & Data Security Incident Response Plan

- A Cyber and Data Security Incident Response plan has been created and is maintained
    - This has at a minimum identified:
        - the key roles and responsibilities of the incident management team
        - the contact details of all the required team members / partners
        - details of the where and how the team will meet in the case of an incident.
    - All team members must be aware of their roles and responsibilities
    - The team meets together at least once per year to review the plan and update as necessary.
- A copy of emergency contacts and the incident management plan will be kept by Executive Committee members for contingency.
    - This will be available in a 'grab-and-go' format to enable the plan to operate in the case that IT systems are unavailable.
- A hard copy of the emergency contacts will be kept up to date and made available in the current Helping Hands on-premise data room and on the ground floor of the Support Office, Reception, in the BCP Battle Box. These will also be held off-site by the Head of IT Service Delivery and IT Director.

9.0 Passwords

9.1 Guidance for IT system users

The company maintains a simple guide that is communicated to all team members as part of their induction and on an annual basis as part of information security awareness raising communicating at least the importance of:

- Setting length of passwords of 14 characters as a minimum, including capital, lower-case letters, numbers and symbols and avoiding words that can be guessed.
- Avoiding common passwords
- Safely storing passwords including using password managers if appropriate.
- Not reusing any password between system
- Not exchanging or sharing credentials, no matter how important.

9.2 Password compromise procedures

If your password becomes compromised (you discover that it is known by someone else, including colleagues) it is imperative that you notify Head of IT Service Delivery and your line manager immediately once you are aware.

- Very quick action significantly limits the impact of password compromises, often completely mitigating the risk.
- TechTeam and our external cyber partners will follow a procedure in this situation that involves:
    - Locking relevant user accounts while the issue is contained and investigated
    - Resetting any affected passwords in line with 10.1
    - Reviewing access and audit logs to identify if the event meets the criteria of a Security Incident.

10.0 Corporate Risk Register

- The company maintains a Corporate Risk Register. This identifies risks and their associated severity and likelihood. The register also records where appropriate mitigations have been identified and the resulting risk rating that remains for either remediation or acceptance.
- The risk register is reviewed at least quarterly by the Executive Steering Committee
- Risks that cannot be accepted by the IT Director will be escalated to the Executive Committee, and where appropriate, the Board

11.0 Data Quality

For data to be high quality it needs to be accurate, up-to-date, complete, free from irrelevant data and consistent across system.

The quality of data that is stored and used by the company is important. Poor data quality leads to poor decision making. This can lead to financial costs to the company, and in the worst situations harm to data subjects.

- It is the responsibility of information owners to ensure that data is collected and maintained to ensure data quality.
- Appropriate data retention periods must be maintained to ensure that out-of-date information is not retained. Please refer to the Data Retention Policy.
- Where data is moved or duplicated between systems, efforts must be made to ensure that errors are not introduced and data remains consistent. This is likely to involve automating or systematising data integration activities.
- For clinical data a policy will be maintained to ensure this meets the legal requirements for clinical records and also the needs of our care provision services. All team members receive regular training covering the importance of data quality, security and control and the appropriate policies and procedures in use at Helping Hands

12.0 Record Keeping

The ISO definition of a Record is:

> *"Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business."*

Section 205 of the Data Protection Act also specifically identifies the concept of a health record as:

> *"consists of data concerning health that has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates."*

- Records will be maintained in a deliberate manner, selecting appropriate locations and systems for the record keeping appropriate for the length of storage that is required.
- Records will remain available to the company for the duration of the required record keeping period and should be destroyed or erased at the appropriate time.

- Health records will be managed in line with the specific policy on clinical record keeping.
- Information owners are responsible for appropriate keeping of records.
- Email systems are intended for timely communications and is not an appropriate system for storing records. Emails that are to become business records should be stored in separate appropriate systems that are fit for the purpose.
- Where further guidance is required, not provided in Helping Hands policies and procedures, the NHS Health Records Management Code of Practice (2021) should be used a point of reference.

13.0 Bring-Your-Own-Device & Mobile Devices

Bring-your-own-device (BYOD) is where you use a device (computer, laptop, tablet or mobile phone) that is not owned by the company to access company data.

Please refer to the Policy currently maintained and dedicated to BYOD in the following document: HHH-POL-050

14.0 Physical Security

Physical security is important to prevent loss and theft of equipment and to avoid people bypassing electronic security controls by, for example, connecting directly to a secure network segment, or accessing the physical hard drive of a server.

- Buildings which contain company data should have adequate security including locked doors and windows and managed access control to ensure that only approved individuals can gain entry to areas appropriate to their role.
- Anyone present on site should wear some form of official identification (lanyard). This should clearly identify them as either a team member or as a 'visitor'.
- When venturing outside/off-site in the day-time for breaks, the lanyard should be stored under the jumper or in a pocket (securely out of visual sight), to prevent an opportunity for social engineering.

- Rooms containing confidential data (electronic or hard copy) should be locked when not in use, even during the day.
- Confidential data (especially personal data) should be locked away in desk drawer or locked filing cabinets with key access appropriately managed.
- Alarms may be appropriate for certain areas.
- An annual Physical Penetration Test is held to determine currency and effectiveness of the current state controls in place.

15.0 IT Disposal

It is very hard to dispose of IT equipment in such a way that stored data is not recoverable by a third-party later. All IT equipment should be disposed of professionally by an accredited IT waste management provider. Electronic equipment should never be disposed of in general waste, nor removed from the site for reuse or personal disposal.

16.0 Awareness and Training

16.1 Annual review of training needs

The Learning and Development Team should review and undertake a training needs analysis on an appropriate periodic basis, reporting back to the Executive Committee to ensure sufficient resources are deployed. Training requirements should be updated where training needs have changed. This should be recorded in the appropriate team members training systems and details should be updated in this policy.

16.2 Training needs

Role	Training needs	Refresh frequency
All team members	Cyber Security Awareness Training eLearning for health – Data Security and Protection – NHS level 1	12 months repeat of full course.
Data Protection Officer	Appropriate practical Data Protection Officer training. Or industry recognised certificate such as CIPP/E, CIPM or C-DPO.	Annual refresh or extension training or sufficient CPD to maintain appropriate certification.
SIRO	Appropriate SIRO training as required by the DSPT	12 months
IT Director	Appropriate specialist IT security training or industry recognised certificate such as Certified Information Systems Security Professional	Annual refresh or extension training or sufficient CPD to maintain appropriate certification.

- Employee Training: we provide regular (annual or exceptional) cyber security training for all employees, making it real and in context, with both work and home experiences.
- Awareness Programmes: we conduct monthly phishing simulations and other awareness activities, that helps employees understand the risk and impact of being the front line of defence for the business.

- We promote a culture of security awareness, through positive communications and regular updates about the world of cyber security and what to watch out for at work, as well as at home, via our Weekly Bulletin

16.3 Additional measures

- To reduce the likelihood of security breaches, we also advise our team members to:
  - Lock their screens and lock their devices when leaving their desks,
  - Report stolen or damaged equipment as soon as possible to the TechTeam,
  - Report a perceived threat or possible security weakness in Helping Hands systems,
  - Refrain from downloading and using suspicious, unauthorised or illegal software on their company equipment.

17.0 Suppliers

Suppliers that process company data (referred to as Processors under data protection legislation) must deliver services that meet or exceed the standard of our own Helping Hand policies.

- At the point of commissioning a new provider the security and privacy implications of the procurement are be considered.
  - This must involve the IT Director and the Data Protection Officer to ensure that we are meeting our security and legal data processing obligations.

- Generally, this means that processors who do not meet either the Cyber Essentials or ISO27001 are unlikely to offer suitable protections.
  - Any processor handling clinical data must meet one of these two as a requirement of Helping Hands achieving the Data Security and Protection Toolkit 'standards met'.

- We conduct regular due diligence on suppliers who deliver information systems, networks, infrastructure, as well as those who have integrations with the Helping

Hands technology environment, to ensure they meet the above standards, and hold appropriate accreditation and certification.

- We will start an annual assessment of relevant suppliers' security practices.

18.0 IT Acceptable Use

Individual users have a significant role to play in ensuring that IT systems function as intended and that organisational and technical controls are effective.

The Company's policy on acceptable IT Use that applies to all IT systems is stated below.

These rules are in place to protect the employees, the people we process data about and the company. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and personal data, and legal issues.

Misuse or excessive personal use of our telephony, M365, SAAS solutions (Access) or inappropriate online use will be dealt with under our Disciplinary Procedure.

Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by

1. participating in online gambling, online dating
2. forwarding chain letters,
3. creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):
    a. pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
    b. offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our customers;
    c. a false and defamatory statement about any person or organisation;
    d. materials which are discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

e. confidential information about us or any of our employees or customers (except as authorised in the proper performance of your duties);
f. Unauthorised software;
g. any other statement or activity which is likely to create any criminal or civil liability (for you or us);
h. music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

19.0 Monitoring – IT Usage and Security

IT systems include audit and monitoring capabilities designed to support incident investigation and management, compliance and to support security, troubleshooting and smooth running of the IT estate. This data includes, but is not limited to, web browsing history, files downloaded, data input, network traffic, logons to corporate systems, interactions with data, peripheral device usage, and information about the user's computer.

Any monitoring must be in line with the terms of any employment contract and use of monitoring records must be proportionate and fair. Any investigation into an employee's usage of IT equipment or services should be done with advice from HR.

Although occasional personal use is permitted, users should be made aware in the acceptable use policy that corporately provided hardware and software is unlikely to provide suitable privacy for highly personal communications.

20.0 Enforcement Individuals found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties. Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.	
TRAINING Is training required?	Yes
Details of training	Cyber Security Awareness Training (annual) for all Monthly Phishing Campaigns (by BoxPhish) and follow up education with those who were "caught" New IT Partner induction for alignment
COMPLIANCE How is compliance within this document going to be monitored?	Compliance will be monitored via Academy for training completion, results of monthly Phishing campaigns. The GDPR steering group will monitor compliance on a quarterly basis. The policy will be updated aligned with any regulatory changes and best practice. As an aside with regard to external IT partners, all new partners are subject to an initial cyber security audit to validate they have the requisite controls and measures in place, before contracts are formally signed.

EQUALITY IMPACT ASSESSMENT AND PROCEDURAL INFORMATION		
	Positive/Negative/N/A	Comments
Does the document have a positive or negative impact on one group of people over another based on their:		
• Age?	N/A	
• Disability	N/A	
• Gender assignment?	N/A	
• Pregnancy and maternity (which includes breastfeeding)	N/A	
• Race (including nationality, ethnic or national origins or colour)?	N/A	
• Marriage or civil partnership?	N/A	
• Religion or belief?	N/A	
• Sex?	N/A	
• Sexual orientation?	N/A	
If you have identified any potential impact (including any positive impact which may result in more favourable treatment for one particular group of people over another), are any	N/A	

exceptions valid, legal and/or justifiable?	
If the impact on one of the above groups is likely to be negative:	
Can the impact be avoided?	N/A
What alternatives are there to achieving the document's aim without the impact?	N/A
Can the impact be reduced by taking different action?	N/A
Is there an impact on employee, customer or someone else's privacy?	N/A
Changes since previous version	At point of review updated the following: • Updated named third parties to 'partners' • 4.0 – cloud services • 6.0 - Malware Protection – anti-virus software and update of who will supported in resolving issues identified (last bullet point) • 7.3 – Added details of review and sign-off related to administrative accounts and use of separate accounts • 8.1 – Updated Backup and Disaster recover to include review of testing results and relevant external partners • 8.3 – Added where Incident response plan is located. • 14.0 - Added detail related to physical security – how lanyard should be worn / stored out of site • Added details related to Compliance with Policy whereby new partners are subject to initial cyber security audits before contracts are signed
Who was involved in developing	IT Director Executive Team

/reviewing/amending the document? (list titles)		
How confidential is this document	Restricted	Can be shared freely within Helping Hands but NOT outside
References		
Associated Documents	Business Continuity Plan Bring Your Own Device (BYOD) Policy Data Deletion and Retention Schedule Cyber & Data Security Incident Response Plan	