Title of Document	**Information Handling and Sharing Policy**
Name of Department	**Quality**

What type of document is this?	**Policy (POL)**		
Which Helping Hands POL/SOP does this document relate to?	Information Governance POL Data Protection POL Information Security (Inc Cyber Security) POL Records Management, Retention and Deletion POL Privacy Information POL Information and Data Sharing SOP Information Risk Management SOP Data Protection Impact Assessment SOP	**Index number of POL/SOP**	POL-084 POL-085 POL-082 POL-087 POL-007 SOP-039 SOP-040 SOP-038

Which Operational Priority/Priorities does this document link to?	Governance Framework	Internal & External Communications	Information Management & Technology

Custodian of document	Group Managing Director	**Committee responsible for this document**	Policy Committee
Approval date and committee chairperson signature	29.04.25	**When is its next scheduled review?**	29.04.28

Who does it apply to?	All employees at Helping Hands				
	Does it apply to bank workers?	Yes	**Does it apply to agency staff?**	Yes	**Does it apply to third party contractors?**	Yes

Purpose of the Policy	The purpose of this policy is to provide the standards that staff must follow when sharing personal data to ensure that legislation is not breached, personal and sensitive information is safeguarded and that standards of confidentiality are maintained at an exceptional level.

Roles and Responsibilities

Role	Responsibility
Data Protection Officer (DPO)	Provide advice and information on GDPR regulation, national law and Information handling and sharing best practice.
Directors **Senior Leader Team**	Ensuring staff comply with this policy and associated procedures in line with this GDPR and the DPA 2018, ensuring procedures are followed to prevent data loss and confidentiality breaches.
GDPR Team	To monitor compliance of this policy through training, awareness and internal audits.
TechTeam	Application of suitable security programs and the monitoring of all systems. Asset management and support to all staff on IT related issues
Employees	Comply and adhere to the GDPR principles and procedures in line with this policy and associated SOPs and Working Instructions where relevant. To recognise and report data breaches and SAR to line managers promptly.

1. Scope

1.1. This policy provides confidentiality guidelines and requirements for processing, handling, storing, accessing and disclosing information across Helping Hands.

2. Standards of Confidentiality

2.1. Helping Hands has set out the following confidentiality standards to reduce the risk of common and unintentional breaches of confidentiality:

2.1.1. All employees are required to sign a confidentiality clause within their contract of employment and should abide by it.

2.1.2. It is a condition of employment that disclosing confidential information such as customer or employee contact details (unless in an emergency) to any unauthorised third party (including members of your family) is not permitted.

2.1.3. Employees must not disclose information of a confidential nature relating to Helping Hands or services provided, during or after your employment ends, except in the proper course of your employment duties or as may be required by law.

2.1.4. Employees have a duty to maintain confidentiality of information given verbally or in writing by customers and their representatives.

2.1.5. Employees must not seek out confidential information from a customer unless expressly in the interests of that customer, i.e. to provide better care.

2.1.6. A customer's care record should only be shared on a need to know basis e.g. Health professional, Ambulance Crew, Manager.

2.1.7. Only employees who are authorised can share information externally. This can be either by written authority in their job description, or by approval from their Line Manager (refer to Information and Data Sharing Procedures Standard Operating Procedure).

2.1.8. This policy should not prevent the sharing of information when this is manifestly in the best interests of someone receiving care. Health and social care professionals should have the confidence to share information in the best interests of their customer when sharing is necessary for customer safety, quality and integrated care.

2.1.9. Authorised transportation of confidential documents must be carried out in a secure and timely manner. Documents are not to be left unattended in plain sight or overnight in homes or vehicles.

2.1.10. Documents or equipment belonging to the Business of which contain any confidential information must not be removed from work premises at any time without proper authorisation and must be returned to the Business upon request and termination of employment.

2.1.11. Employees must not use customer address details to open personal accounts or to receive personal parcels or mail; e.g. ordering from retail sites and receiving deliveries to customer addresses. The use of a customer's personal number / address will be considered as financial abuse and subject to disciplinary action which may lead to termination of employment.

2.1.12. Customer and employee details must not be stored on personal devices such as mobile phones and laptops etc. This does not include personal devices used in conjunction with the Bring Your Own Device application.

2.1.13. Employees must not disclose customer personal data such as name, address, telephone number or health information to other people without the written consent of the customer or authorisation by Helping Hands.

2.1.14. Employees must not share or post personal information and / or photographs, videos or recordings of a customer, their property or surroundings without prior

written consent from the customer and Helping Hands. This includes both digital and paper format. Refer to the HHH-POL-006 - Social Media Policy for details.

2.1.15. Only work devices can be used when taking consented photographs for work related purposes, or through controlled procedures via Access Products (such as Access Care Planner).

2.1.16. Employees must avoid using the personal data of real customers for training purposes or as part of documentation required for accreditation or a qualification.

3. Communication

3.1. Almost all job roles require personal information to be communicated verbally, used, transferred or stored. All these actions are sometimes referred to as 'processing data'. The way data is processed securely depends on the format of the data (paper or digital) and the method of communication (verbal, email, post).

3.2. Employees need to be able to share or exchange confidential information about both customers and employees securely

3.3. Employees with work assigned emails -@helpinghands.co.uk can share information via the Helping Hands secure email server. Ensuring that the right information is sent to who it is intended is another aspect of maintaining confidentiality.

3.4. Where employees with work assigned emails -@helpinghands.co.uk require to send sensitive and confidential information internally, documents should be password protected and the password forwarded in a separate email.

3.5. Sending confidential information to external emails is not secure and must be password protected or avoided where possible.

4. General Communication

4.1. Verbal and Telephone:

4.1.1. Do not make calls relating to sensitive or person identifiable information (PII) where you can be overheard.

4.1.2. Confirm the identity of the person asking for information by asking for their name, date of birth and / or address to ensure you are speaking to the right person. Do not ask leading questions.

4.1.3. Be aware of 'bogus callers' who attempt to obtain information to which they are not entitled. If in doubt, a call check must be done to verify their full name, date of birth, GP or call them back so that you can verify independently. If a bogus call is suspected, information must not be disclosed, and the incident must be reported to the Line Manager.

4.1.4. Ensure to put callers on hold if you need to speak with someone else or when transferring the call to avoid being overheard.

4.1.5. Do not leave confidential information on answerphones without prior consent from the recipient. It is better to leave your name and contact details or a brief message indicating that you will call back.

4.1.6. Do not text confidential or personal identifiable information to colleagues whether authorised or not. If it falls into the wrong hands, this would be a data breach.

4.1.7. Do not take pictures of customers directly on personal devices. Where customers consent to having their photo taken, it should be taken on a Helping Hands device or directly through the Access Care Planning application in line with Helping Hands procedures.

4.1.8. We do not permit staff disclosing customer details such as addresses, phone numbers etc to family and friends. The disclosure of personal data that may identify a customer is a data breach.

4.2. E-mail:

4.2.1. Personal, sensitive or confidential information must be password protected before attaching and sending via email.

4.2.2. Passwords for protected documents must be sent via a separate email.

4.2.3. When sending sensitive information, clearly indicate the subject header as **'Confidential'.** Do not put identifiable information in the subject heading and keep the information in the email to an absolute minimum.

4.2.4. Always check the email address you are sending information to. Sending personal or sensitive data to the wrong person is a data breach and must be reported.

4.2.5. Sending personal or sensitive data inappropriately by failing to use the blind copy (bcc) function or disclosing personal information without consent is a data breach and must be reported.

4.2.6. Use a customer's preferred method of communication if known or respond to an email address if the initial contact was made via this method.

4.2.7. Any bulk transfers of unencrypted data must be essential and kept to a minimum.

4.2.8. Any personal or sensitive data that needs to be sent via email to a non-work email address must also be password protected.

4.2.9. Requests for data by other people need to be considered very carefully and usually must include evidence of authority or consent by the owner of that data. Seek guidance from datarequest@helpinghands.co.uk as required.

4.2.10. Do not forward emails that contain personal or sensitive data when it no longer needs to be included (e.g. send a new email instead of continuing an email thread).

4.2.11. Emails containing person identifiable information must be stored appropriately when received and it is good practice to delete it from the email system when no longer needed.

4.3. Post

4.3.1. Ensure that if correspondence contains person-identifiable information, it is marked as 'Private & Confidential' and put in a sealed and robust envelope.

4.3.2. Ensure that post is sent to a named person/department.

4.3.3. Ensure that the details of the recipient are clear and accurate.

4.3.4. Ensure that the sender's details are included or known to the recipient.

4.3.5. Helping Hands uses services of 3rd party providers for the secure delivery of sensitive and confidential information via a recorded delivery service.

4.3.6. Helping Hands uses tracked/special delivery for customer identifiable information that is extensive in volume, extremely sensitive, batches of information or when delivery confirmation is required.

4.4. Print/Scan/Copy

4.4.1. Ensure that the secure document function, linking employee email address to the assigned machine, is used when printing or scanning documents.

4.4.2. Always check that copies and original documents, either printed or scanned are not left behind in the printer / photocopier.

4.4.3. Ensure that only the correct documents are retrieved promptly and alert the Line Manager if any other documents are found unattended.

4.5. Instant Messaging Services

4.5.1. Microsoft Teams is an authorised platform when communicating about work related activities or for business purposes.

4.5.2. Unauthorised applications such as WhatsApp / Facebook Messenger are not permitted for business activities or to support the provision of care.

4.5.3. It is the responsibility of the users on these platforms to ensure appropriate use in a personal capacity with the consent of all group participants prior to setting up a group chat.

4.5.4. Owners of groups must regularly review and remove members from such groups when necessary.

4.5.5. Helping Hands is not liable for the exchange or storage of any personal and/or sensitive information including images and videos on personal devices that use unauthorised applications or personal social media platforms and employees do so at their own risk.

5. Handling and Storing Data

5.1. It is essential that personal or sensitive data is handled, stored and transported in line with Helping Hands Data Protection and Information Security policy which outlines the General Data Protection Regulation (GDPR) as well as any legal and contractual obligations.

5.2. Helping Hands adopts a clear desk and locked screen approach which means that employees should clear their desks at the end of each workday and when away from their desks and ensuring screens are locked. Documents, notes, post-it-notes and business cards must be stowed away in the lockable drawers and cabinets provided.

5.3. All locations holding personnel / employee / customer files should not be accessed by un-authorised individuals.

5.4. Confidential records should be kept secure either physically in locked office drawers, filing cabinets or password protected on computers and other devices or applications.

5.5. Employees should not keep hold of documents and data for longer than necessary or carry them around when not required. This increases the risk of getting lost, damaged or unauthorised access and / or disclosure.

5.6. Confidential documents and portable devices containing personal and sensitive data must not be left unattended, in vehicles, unsecured overnight or taken home unless authorised.

6. Data Destruction

6.1. Ensure that unused prints, copies and other confidential waste are put in the certified waste disposal bins authorised for shredding by a 3rd party service provider.

6.2. If certified waste disposal bins are not available, employees must use approved GDPR-compliant machine shredders with cross-shredding capabilities available.

6.3. This only applies to the destructon of data or information that is unwanted, surplus or copies which are not subject to Helping Hands records management and retention schedule.

6.4. Types of Information (confidential waste) that should be shredded include**:**

- Employee/customer data
- ID cards and badges
- Company letterhead paper
- Business cards
- Brochures/ flyers/ leaflets
- Diaries
- Printed letters
- Printed emails
- Branded goods
- Used notebooks
- Printed Customer databases/spreadsheets
- Duplicated, surplus or inaccurate copies of records or collated information

7. Data Transfers and Storage

7.1. Helping Hands transfers and stores data under contractual agreements with data processors in the UK. Data transfers and storage may also occur in the European Economic Area (EEA) and other countries. These are known as Restricted Data Transfers.

7.2. Restricted Data Transfers:

7.2.1.

Under the UK GDPR, restricted data transfers from the UK to the EEA and other countries covered by a European Commission 'adequacy decision' are currently permitted subject to review by the UK Government.

7.2.2. At times is it may be necessary to transfer data to countries that do not have an adequacy decision. In these cases, we would only do so having adopted appropriate safeguards as required by the UK GDPR, including completion of a transfer risk assessment (TRA).

TRAINING

Is training required?	Yes
Details of training	Academy (LMS) - GDPR and Information Governance

COMPLIANCE

How is compliance with the Policy going to be monitored	• GDPR Steering Group • Quarterly Governance meetings for service review and improvement • Data Incident Notification (DIN) reporting • Complaints and Incident reporting • Document management and review process

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?		
• age?	N/A	
• disability?	N/A	
• gender reassignment?	N/A	
• pregnancy and maternity (which includes breastfeeding)?	N/A	
• marriage or civil partnership	N/A	
• race (including nationality, ethnic or national origins or colour)?	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 group of people over another), are any exceptions valid, legal and/or justifiable?	Positive	This policy provides a positive impact on the management of Information Governance
If the impact on one of the above groups is likely to be negative:		

• Can the impact be avoided?	NA	
• What alternatives are there to achieving the document's aim without the impact?	NA	
• Can the impact be reduced by taking different action?	NA	
• Is there an impact on staff, client or someone else's privacy?	NA	*If yes, privacy impact assessment required*

What was the previous version number of this document?	This is a new Policy	
Changes since previous version	N/A	
Who was involved in developing/reviewing /amending the policy?	GDPR Coordinator Quality Development Lead	
How confidential is this document?	Restricted	Can be shared freely within Helping Hands but NOT outside

References	https://ico.org.uk https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care https://app.croneri.co.uk/topics/caldicott-principles-and-patient-confidentiality/indepth https://www.ukcgc.uk/ https://www.nationalarchives.gov.uk https://www.restore.co.uk/Digital/Insights/Blogs/gdpr-what-are-the-statutory-retention-periods-for-hr https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/managing-email/ https://www.dsptoolkit.nhs.uk/Help/29
Associated Documents	Privacy Information Policy CCTV Policy Call Monitoring Policy Electronic Call Monitoring (ECM) Policy Bring your own Device (BYOD) Policy Records Management, Retention & Deletion Policy Access Right Verification & Consent WI Data Breach Risk Management WI Data Incident Notification (DIN) Form

Appendix One - Definitions

CONFIDENTIAL INFORMATION- This can be health information, any data, combination of data and other information, which can indirectly identify the person. This includes information relating to contacts and employees that is private and not public knowledge or information that an individual

would not expect to
be shared. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, tablet, mobile phones, digital cameras or even heard by word of mouth.

CONSENT- Means that a person is clearly given an option to agree or disagree to the collection, use or disclosure of personal information such as signing a consent form that clearly states why an organisation wants your personal information.

DATA BREACH- 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.

DATA PROTECTION- The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

DIN- Data Incident Notification

DPO- Data Protection Officer

EMPLOYEE- An individual who works part-time or full-time for Helping Hands under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent controllers.

PERSONABLE INFORMATION/ IDENTIFIABLE NATURAL PERSON- Anyone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

PERSONAL DATA- Any information (including opinions and intentions) which relates to an identified or identifiable Natural Person.

PROCESS, PROCESSED, PROCESSING- Means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

REQUESTOR – An individual, organisation or other 3rd party requesting on behalf of self or others

SAR – Subject Access Request

SENSITIVE OR SPECIAL CATEGORY DATA- Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data