Title of Document	**Data Protection Policy**
Name of Department	**Quality**

What type of document is this?	**Policy**		
Which Helping Hands POL/SOP does this document relate to?	Information Governance POL Information Security (Inc Cyber Security) POL Records Management, Retention and Deletion POL Privacy Information POL Information Handling & Sharing POL Information and Data Sharing SOP Information Risk Management SOP Data Protection Impact Assessment SOP	**Index number of POL/SOP**	POL-084 POL-082 POL-087 POL-007 POL-086 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 at all Facilities				
	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	Helping Hands is committed to conducting its business in accordance with all applicable General Data Protection Regulations (GDPR), and to fulfil our legal and moral responsibilities. The document is intended for all Helping Hands employees and aims to ensure that there is a consistent approach to the management, communication and implementation of all GDPR and data protection procedures that is available to everyone. This provides the legal framework to minimise the incidence and impact of data breaches within the entire organisation. It is the responsibility of all employees to adhere to this policy and its related documents and to be aware of their relevant roles and accountability with regards to the measures in place to maintain compliance and the security of personal and

	sensitive data. Non-compliance or a lack of adherence leaves Helping Hands vulnerable to complaints, regulatory sanctions, fines, loss to the business and reputational damage. This document ensures that guidance on other statutory and legal frameworks relating to personal data including Freedom of Information Act 2000, Human Rights Act 1998 and the common law duty of confidentiality are followed. Where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

Summary of Key Information Governance Requirements

The scope of this Policy outlines Helping Hands commitment to in the following areas:

- Roles & Responsibilities
- Definitions (Appendix 1)
- The General Data Protection Regulation (GDPR) principles
- Lawful, Legal Basis of Processing
- Records of Processing Activities (RoPA)
- Handling Data
- Data Protection by Design or Default
- Subject Access Requests & Data Disclosures
- Data Breach Management

Roles and Responsibilities

Role	Responsibility
Data Protection Officer (DPO)	Provide advice and information on GDPR regulation and national law, Reviewing legal record keeping Advise and monitor DPIAs Reporting to the board and contact point for employees and ICO notifications as required.
Directors **Senior Leader Team**	Ensuring staff comply with this policy and associated procedures in line with this GDPR and the DPA 2018. This includes responsibility for authorising access control and privileges to ensure procedures are followed to prevent data loss and confidentiality breaches.
GDPR Team	To monitor compliance of this policy through training, awareness and internal audits.
Tech Team	Application of suitable security programs and the monitoring of all systems and IT assets to prevent the incidence of malware (viral attacks) or unauthorised access by hackers. 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.

Table of Contents

1. Scope

1.1. Helping Hands meets its requirements regarding the access and confidentiality of personal data that is collected, used and transferred, retained, archived, disclosed or destroyed. This includes the processing of personal data both manually (in a structured and readily accessible filing system) and electronically on applications.

2. GDPR Principles

2.1. Helping Hands is committed to the GDPR principles which are essential for providing excellent service in social care. Data is only collected for a specific purpose and available when and where it is needed. Data should be kept securely and only for its intended use. The data kept must be relevant, up to date and protected from loss, damage and any unauthorised access, disclosures or alterations by maintaining appropriate levels of security and standards of confidentiality.

2.2. Principle 1 – Lawfulness, fairness and transparency

2.2.1. We uphold this principle by maintaining a register of our processing activities which is reviewed annually. Helping Hands processes data as outlined in its privacy promises for

transparency. Individuals have the right to access their personal data and any such requests shall be dealt with in a timely manner.

2.3. Principle 2 – Purpose limitation

2.3.1. Personal and Special category data is collected according to the lawful basis of processing defined in this policy and outlined in the respective privacy promises.

2.4. Principle 3 – Data minimisation

2.4.1. Data that is collected should be adequate for its purpose but limited to only what is necessary. Data cannot be collected for 'just in case scenarios' that fall outside of the lawful basis stated. Helping Hands is committed to reviewing processes and procedures that relate to collecting data and assessing the needs of the business. Data is assessed and deleted where possible upon request and after review.

2.5. Principle 4 – Accuracy

2.5.1. Efforts should be made to ensure data is accurate at the time of collection and regularly reviewed to keep it updated. Data that is inaccurate should be erased or rectified without delay.

2.6. Principle 5 – Storage limitation

2.6.1. Data that identifies an individual should not be kept for longer than is necessary. This period is defined by what the data is being used for and how long afterwards it needs to be retained for. **Helping Hands Record Management, Retention and Deletion Policy** details the archiving and deletion process for each record and sub-type held to determine what should/must be retained, for how long, and why.

2.7. Principle 6 – Integrity and Confidentiality

2.7.1. The data collected and processed by Helping Hands is stored securely using a variety of organisational and technical security measures that include appropriate access controls, physical security, system and network malware protection and back up and disaster recovery solutions that are in place.

2.8. Principle 7 – Accountability

2.8.1. Helping Hands as the data controller is responsible for all the data collected and processed and must be able to demonstrate that we comply to all the above principles.

2.9. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data, there are procedures in place to assess the risk to people's rights and freedoms and if appropriate includes reporting to the relevant authorities.

3. Lawful / Legal Basis of Processing

3.1. Helping Hands Homecare is a private homecare service provider regulated by the Care Quality Commission (CQC) and Care Inspectorate Wales (CIW) and processes data:

3.1.1. Article 6.1a - with clear consent from the data subject to process personal data for a specific purpose.

3.1.2. Article 6.1b - as necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.

3.1.3. Article 6.1c - as necessary to comply with the law and regulatory frameworks (not including contractual obligations)

3.1.4. Article 6.1f - in pursuit of legitimate interests, which include:

- Marketing purposes
- Sales enquiries and communications
- Corporate diligence, financial modelling, service development and innovation
- Asset and facilities management
- Telephone recording and CCTV

3.2. Helping Hands recognises that additional care is required when handling special category (sensitive) data. We process this in line with GDPR under Article 9(2)(h) and 9(3):

3.2.1. Article 9(2)(b) - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

3.2.2. Article 9(2)(f) - processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

3.2.3. Article 9(2)(h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3'

3.2.4. Article 9(3) – personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.'

3.3. Simply this means that we provide care by employing people (performance of a contract) to carry out their roles (processing) to manage care and support that care provision. That role could be in marketing to promote our services (legitimate interests), recruitment, training, customer support, finance, operations or HR. All these activities are required and involve processing both personal and special category which is why it is so important that we look after it.

4. Records of Processing Activities (RoPA)

4.1. We will create and maintain a Record of Processing Activity (RoPA) that is as a minimum in line with the requirements of Article 30 of UK GDPR.

4.2. The RoPA also includes, or links to documentation covering:

4.2.1. Information required for privacy notices, such as the lawful basis for the processing and the source of the personal data

4.2.2. Records of consent

4.2.3. Controller-processors register

4.2.4. The location of personal data

4.2.5. DPIA reports

4.2.6. Information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018 (DPA 2018)

4.3. We will keep this record of processing activities in electronic form so we can add, remove or amend information easily.

4.4. Review on an annual basis of the record against processing activities, policies and procedures is undertaken to make sure that it:

4.4.1. Remains complete, accurate and up to date

4.4.2. That the personal data is limited to only that necessary for the purpose in line with the minimisation principle.

4.5. We will maintain an internal record of all processing activities carried out by any processors on behalf of the Company.

Documenting the lawful basis

4.6. We will identify the most appropriate lawful basis (or bases) for each activity following a review of the processing purposes.

4.6.1. This will be identified and recorded before starting any new process.

4.7. We will document the lawful basis (or bases) in the RoPA. Where there is ambiguity or it is required for clarity, we will document the justification for the decision.

4.8. Where we process special category data or criminal offence data, we will identify and document a lawful basis for general processing and an additional condition for processing this type of data (or in the case of criminal offence data only, we identify the official authority to process).

4.8.1. In the case of special category or criminal offence data, we will document consideration of the requirements of Article 9 or 10 of the UK GDPR and Schedule 1 of the DPA 2018 where relevant.

4.8.2. Where Schedule 1 requires it, we will create and maintain an appropriate policy document including:

- Which Schedule 1 conditions we are relying on
- What procedures we have in place to ensure compliance with the data protection principle
- How special category or criminal offence data will be treated for retention and erasure purposes
- A review date; and details of an individual assigned responsibility for the processing

5. Handling Data

5.1. Privacy Information

5.1.1. We are legally obliged to provide individuals and users information about Helping Hands as an organisation, the lawful basis and purpose of the processing. This ensures that data is processed with the knowledge and consent of the individual.

5.1.2. We provide information about how data is collected, purpose of processing and why it is shared or disclosed in Helping Hands Privacy Information Policy and via the website https://www.helpinghandshomecare.co.uk/privacy/

5.1.3. Helping Hands regularly updates its privacy information when necessary and this should be read by all employees as part of the new starter induction/onboarding process and by the care team via the carer weblink.

5.2. Confidentiality

5.2.1. Confidentiality is an obligation for all employees in clinical or non-clinical roles. Employees must not reveal to anyone outside the Helping Hands organisation personal information that they learn in the course of their work, especially without a contact's consent. This includes discussing aspects of care or employment with non-relevant parties, that could lead to identification of a contact.

5.2.2. Employees are expected to participate in induction, training, awareness or publications to inform and update on confidentiality matters.

5.2.3. The Helping Hands Information Handling & Sharing Policy outlines our policy & procedures that are in place to safeguard personal, sensitive and confidential information between Helping Hands employees and external sources.

5.3. Non-Disclosure Agreements (NDAs)

5.3.1. A non-disclosure agreement (NDA), sometimes known as a confidentiality agreement is a legally binding contract by which one or more parties agree not to disclose confidential information that they have shared with each other. By signing an NDA, you agree to keep confidential information from being disclosed to unauthorised parties.

5.3.2. Where customers approach employees to agree to and sign an NDA, the employee must inform the Care Manager before doing anything else. For Helping Hands to facilitate an NDA, the following steps must be implemented:

- Seek advice from the People Team
- The support plan needs to highlight the requirement for the NDA
- Ensure any carer considering undertaking the package understands what an NDA is and suggest they seek their own legal advice if necessary

5.3.3. It should be made clear to employees that they are not obliged to sign an NDA and where they choose not to, their employment with Helping Hands will not be impacted in any way.

5.4. Caldicott Principles

5.4.1. Helping Hands provides social care and shares or receives personal identifiable information with other health care professionals in the best interests of its clients in relation to the framework set out by the seven Caldicott principles which are:

- Justify the purpose(s) of using confidential information
- Only use it when necessary
- Use the minimum that is required
- Access should be on a strict need-to-know basis
- Everyone must understand his or her responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

6. Data by Design or Default

6.1. Data protection by design is legal requirement that ensures that, at the senior and board level, Helping Hands has considered the privacy and data protection issues at the design phase or early stages of any operational system in use or to be implemented and then throughout the lifecycle.

6.2. Data protection by design has broad applications which include:

- Developing new IT systems, services, products and processes that involve processing personal data
- Developing organisational policies, processes, business practices and/or strategies that have privacy implications
- Physical design
- Embarking on data sharing initiatives
- Using personal data for new purposes or changing the way data is processed

6.3. Objectives

6.3.1. To provide a step-by-step approach to integrate data protection by design within change management and / or project processes using the relevant data protection impact assessment tool (DPIA)

6.3.2. When assembling the project team, we will ensure:

- That the project team has the required expertise in data protection

- Engagement with the Data Protection Officer and relevant stakeholders
- To record the name of the team member responsible for privacy

6.3.3. As part of the planning and design stage of a project, the team will proactively identify any potential risks to a data subject's privacy or to their rights. This is done by:

- Performing a Data Protection Impact Assessment template
- Obtaining the input of the DPO on the DPIA
- Submitting the completed DPIA to GDPR Compliance to update the DPIA register and set a review date

6.3.4. We can only use personal information for the purposes for which it was originally obtained or that the data subject has been informed about in advance. We will:

- Record and document the purpose of processing
- Confirm that the purpose is in line with the purpose it was originally obtained, and
- Ensure that the purpose is clearly communicated to the data subject in the privacy notice that we provide.

6.3.5. We will document the legal basis for processing the personal information lawfully. The project team is responsible for identifying and documenting a legal basis before processing can begin. We will:

- Identify the appropriate Article 6 legal basis(s) that apply to processing
- Where special category data is being processed (sensitive), identify the appropriate Article 9 legal basis for processing.
- If not stated on the DPIA, this must be documented and submitted to GDPR Compliance to update our Record of Processing Activity (ROPA).

6.3.6. We must ensure that we provide appropriate levels of physical and technical security to personal and special category data during all stages of processing activity. The following measures must be considered:

- Physical protection - Ensure that data is protected against loss, damage and theft regardless of where it is stored. (paper, computers, mobile devices etc)

- Data encryption - Data should be encrypted when in storage - e.g. on a laptop, hard drive or when in cloud storage.

- Encrypted in transit - When data is transferred electronically, it should be encrypted. Online forms or mobile applications must collect and transfer

data using a secure server connection. Typically, non-configured email systems are not suitable for secure data transfer.

- Access controls - Processing on systems use must have appropriate access controls that ensure only authorised personnel can access the data. These access controls should be in line with the business wide IT and information security policy.

- Back up - Data must be recoverable in the event of loss, system failure or data corruption.

- Malware protection - IT equipment used for processing data must have appropriate anti-malware software installed.

- Where the expertise or experience is not present in the project team, appropriate advice should be obtained from within the company.

6.3.7. It is legal requirement that we clearly inform data subjects of any data processing activities. We must:

- ensure that the privacy notice covers processing activity in plain English language.

- Update the notice if needed to reflect changes to legislation and/or a change in processing.

- Ensure that the privacy notice is made available to all users at the point they provide their information.

- We must review any planned processing activity to ensure that data subjects are able to exercise their rights. This includes:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making including profiling

6.3.8. We must provide individuals with the tools needed to determine how their personal data is being used and how this will be monitored or enforced.

6.3.9. Where a data subject has rights to restrict or object to processing, we must offer:

- strong privacy defaults
- user-friendly options and controls

6.3.10. We must only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design. To ensure this, we must:

- Identify all the third-party data processors that are involved in this processing and ensure that a Data Processing Agreement in place.
- Monitor compliance and maintain a register of data processors including details of any new processors.
- Retain a copy of the Data Processing Agreement.

6.3.11. When using different systems, services or products to carry out our processing activities, we must ensure that we use developers and manufacturers that take data protection into account.

6.3.12. We must ensure that all IT platforms have appropriate security and privacy controls with a suitable DPA in place.

6.3.13. Consider the use of Privacy-Enhancing Technologies (PETS). Technologies move quickly and that means that there may be new ways of enhancing privacy for data subjects. During the planning and design phase of a project, we must review the commercial marketplace for new software or hardware technologies that provide enhanced privacy control and protection for our data subjects.

7. Data Protection Impact Assessment (DPIA)

7.1. A Data Protection Impact Assessment is a tool used to identify and minimize the data protection risks of new and existing projects. DPIAs are an integral part of the Data Protection by Design or Default approach and is part of Helping Hands GDPR obligations to demonstrate accountability.

7.2. Completed DPIAs must be reviewed and approved by the DPO before the implementation phase of any major project.

7.3. Refer to the Data Protection Impact Assessment (DPIA) Standard Operating Procedure (SOP) for procedural details.

8. Contracts

8.1. As a data controller, Helping Hands has determined the purposes and means (legal basis) for data processing and has a responsibility to demonstrate compliance with GDPR principles to ensure that contractual agreements with employees, contractors or 3rd party data processors are upheld.

8.2. Employees that access to and process data in some way are subject to a written confidentiality clause within their employment contracts.

8.3. There are also contracts or service agreements in place with other data controllers or processors that outline each party's legal responsibility and liability so that both parties provide 'enough guarantees' that the requirements of GDPR will be met and the rights of data subjects are protected.

8.4. Data Processing agreements must be incorporated where applicable as part of the service procurement process. Authorisation of service agreements and contracts is the responsibility of the Finance Department and approved by the Chief Financial Officer.

9. Subject Access Requests (SAR) and Data Disclosures

9.1. The General Data Protection Regulations (GDPR) provides data subjects with certain rights in relation to their data.

9.2. Right to be Informed

9.2.1. Individuals must be given information about the processing of their personal data including purpose of processing their personal data, retention periods and who we share their data with. This information is available in the Privacy Promise.

9.2.2. The Privacy Promise is provided to individuals at the time their personal data is collected or within a reasonable time period if data is attained from other sources.

9.2.3. Any changes to the use of an individual's personal data must be communicated to individuals before a change is initiated.

9.3. Right to Access (Subject Access Requests)

9.3.1. Individuals have the right to request; confirmation that their data is being processed, access to their personal data and other supplementary information held by Helping Hands about themselves

9.3.2. The data should be provided in a secure and accessible manner. Where requests for information are large or not specific, Helping Hands has the right to ask the individual to specify the information the request relates to.

9.3.3. All requests must be processed using the Access Verification and Consent Procedure outlined in this policy and any data to be disclosed must be reviewed to ensure that there is no information about another individual included where there is a risk to that individual.

9.4. Right to Rectification

9.4.1. It is Helping Hands responsibility to ensure that personal data is accurate. Where an individual believes that the data held by an organisation is incomplete or inaccurate, they have the right to request that their personal data is rectified or completed.

9.4.2. Where requests to rectify are received, it is Helping Hands responsibility to take reasonable steps to satisfy that the data is accurate and to rectify the data if necessary.

9.4.3. Reasonable evidence may be requested from the individual to satisfy the validity of the request, for example by providing evidence of proof of address. This process excludes personal data requests which may be processed when there are changes to their circumstances (i.e. name change due to marriage or address change due to a move).

9.4.4. When considering requests to rectify the following should also be considered:

- A mistake in data, which is subsequently resolved may be accurate data and consideration should be given as to whether the data should be deleted or enhanced with the further information e.g. a diagnosis which is subsequently found to be incorrect

- Disputes about 'opinions' may be difficult to conclude if they are inaccurate and should be reviewed on an individual basis. Records should however clearly identify where an opinion has been made and whose opinion it is.

9.4.5. Whilst the individuals request is being considered the individual has the right to restrict the processing of their personal data. It is good practice to consider restricting the processing of personal data where there is a risk of harm to the individual due to a possible inaccuracy.

9.5. Right to Erasure (Right to be forgotten)

9.5.1.

Individuals have the right to have their personal data erased and can make a request. This right also extends to data online so requests to be deleted from social media and networking platforms, online publications and websites should be obliged. Reasonable steps must also be taken to inform our 3rd party partners to also comply with a request for deletion where applicable.

9.5.2. This right to erasure is not absolute and will only apply in certain circumstances where:

- The personal data is no longer necessary for the purposes which Helping Hands originally collected or processed it for
- The lawful basis for processing the personal data is consent, and the individual withdraws this consent
- The lawful basis for processing is legitimate interests and the individual objects to the processing of their data when there is no overriding legitimate interest to continue
- The data is being processed for direct marketing purposes and the individual objects to that processing
- The data has been processed unlawfully
- It is necessary to comply with a legal obligation

9.5.3. The right to erasure does not apply where the data is necessary:

- To comply with a legal obligation such as employment law
- For the performance of a task carried out in the public interest or in the exercise of official authority
- For archiving purposes in the public interest or statistical purposes where erasure would likely impair the achievement of that processing
- To establish, exercise or defence of legal claims
- For health purposes in the public interest (ensuring high standards of quality and safety of health care services)
- For the provision of health and social care or management of health and social care systems or services

9.5.4. On confirmation that the right applies, a request for erasure of all personal data should be processed. Where data is stored within internal systems or is required for statistical purposes, it is acceptable to anonymise the data to retain this statistical information. Data can be retained once it undergoes an appropriate process of anonymization. This means that all identifiable data is therefore anonymised and when no longer required for statistical purposes should be erased.

9.5.5. We do not process data on children under 18 but recognise that this may occur in unforeseen circumstances.

9.5.6. Any personal data provided by a child or minor will be deleted with no exceptions from any system and media platforms.

9.6. Right to Restrict Processing

9.6.1. Individuals have the right to request the restriction or suppression of their personal data, however this right only applies in certain circumstances. Where processing is restricted, Helping Hands can store the individual's personal data but may be limited in how it is used. Individuals should confirm their reasons for the request and any time limits to the request. Their right to restriction applies where:

- the individual has contested the accuracy of their data and a request for rectification is being processed
- the data has been unlawfully processed and the individual wishes to exercise their right to restrict rather than erase
- the personal data is no longer required however the individual requires us to keep it in order to establish, exercise or defend a legal claim
- the individual has objected to the processing and we are considering whether legitimate reasons override the request

9.6.2. Helping Hands restricts the use of an individual's personal data when there is a legitimate reason to do so. These restrictions include:

- Collection
- Configuring
- Distribution
- Erasure

9.6.3. This may be achieved by temporarily moving data to another system, making data unavailable to users or temporarily removing published data. Measures shall be put in place to ensure that whilst a restriction is in place processing cannot take place. Helping Hands may not process restricted data in any way except to store it, unless:

- the individual has consented
- the purpose is for the establishment, exercise or defence of legal claims
- it is for the protection of the rights of another person
- it is for reasons of public interest

9.7. Right to Data Portability

9.7.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services, known as data portability. This right enables individuals to have the data held moved, copied or transferred easily to another data controller in a safe and secure way without affecting its usability. This right only applies to data which the individual has provided to Helping Hands. This right applies where:

- the lawful basis for processing is consent or for their performance of a contract and the processing is automated (excluding paper file).

9.7.2. Personal data provided to Helping Hands by an individual includes data resulting from observation of an individual's activities, history of website usage, traffic and location data or 'raw' data processed by connected devices. This right does not apply to anonymous data.

9.7.3. Where the data includes information about other data subjects Helping Hands will consider whether processing the request would have adverse effects on other individuals.

9.8. Right to Object

9.8.1. Individuals have the right to object to processing of their personal data:

- for legitimate interests or performance of a task in the public/exercise of official authority
- for direct marketing
- for purposes of statistics

9.8.2. Individuals can have an objection on grounds relating to their situation. Helping Hands must comply with the request unless there are compelling legitimate grounds for the processing, or the processing is for the establishment, exercise or defence of legal claims.

9.9. Rights in Relation to Automated Decision Making and Profiling

9.9.1. This right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The right not to be subject to a decision or profiling applies where the decision is automated (no human

involvement) and it produces legal or significant effects on the individual. The rights do not apply where the decision:

- is necessary for entering into or for the performance of a contract
- is authorised by law
- is based on explicit consent
- does not have a legal or significant effect on the individual

9.10. Receiving a Data Request

9.10.1. Subject Access Requests (SARs) can be received in any format; verbal or written and received by anyone within Helping Hands.

9.10.2. SARs must be directed as follows:

- Employment references should be forwarded to **hr-references@helpinghands.co.uk**
- Requests for employee data by the employee or 3rd parties such as solicitors, property or employment agents should be forwarded to **datarequest@helpinghands.co.uk**
- Requests for financial information from any source (landlords, claims, insurance, etc) must be sent to **payroll@helpinghands.co.uk**
- All other SARs, received across the organisation, including the right to be forgotten, should be forwarded to **datarequest@helpinghands.co.uk**

9.10.3. SARs must be reported to GDPR Compliance to record as soon as it is received. It is good practice to acknowledge a SAR before reporting to GDPR Compliance and where possible, indicate how the requester would like the information to be sent such as by post or email.

9.10.4. GDPR Compliance will assist with a SAR in the following way:

- Verification of identity of the requestor
- Confirmation of legal authority / legal entitlement of requestor
- Data location and collation of data
- Application of redactions / exemptions for non-disclosure
- Secure data disclosure with password protection / encryption for secure email transfer
- Retention of evidence of SAR and any additional information or steps taken

9.10.5. SARs will be assigned to an individual, branch or department to be processed and support given to ensure compliance with UK GDPR and the Data Protection Act 2018.

9.10.6. SARs must be completed within 28 days from the date the request is received. Any unexpected delay that is anticipated must be communicated as early as possible to **datarequest@helpinghands.co.uk**

9.10.7. The time taken to process and comply with a SAR can only be extended in exceptional circumstances and this will be determined by GDPR Compliance

9.10.8. SARs are free of charge to the individual or organisation making the request

9.10.9. Any data or individual rights queries should be directed to **datarequest@helpinghands.co.uk** for advice and support.

9.11. Receiving a Request for Information / Health Records relating to a Deceased Person

9.11.1. The Data Protection Act 2018 and GDPR only applies to records relating to living individuals, but a duty of confidence extends to the deceased and their families. This type of request is processed under the Access to Health Records Act 1990 (AHCA).

9.11.2. The AHCA allows individuals the right of access to health records for the deceased in certain circumstances. A representative, friend or family of the deceased may request access to data where there is belief that there is a claim arising from the death.

9.11.3. Establishing the right to access this information will be reviewed by GDPR Compliance on a case by case basis in collaboration with the DPO under Helping Hands access review and best interest assessment Process.

9.12. Receiving a request for Information from the Coroner, CQC or CIW.

9.12.1. When receiving a request from the Coroner, CQC or CIW, the respective Regional Care Director (RCD) and Safeguarding Lead mut be informed.

9.12.2. The RCD and Safeguarding Lead must have oversight of the request prior to the release of information.

9.12.3. The information must follow the secure data and data disclosure process as outlined in 8.14 – 8.16.

9.13. Responding to requests for employment references

9.13.1. Helping Hands does not disclose the contents of employment references that are sent to other employers or received from another employer. This information is

exempt under the Data Protection Act (sch.2) and requests should be forwarded to **datarequest@helpinghands.co.uk** for authorisation to disclose.

9.14. Data Disclosures

9.14.1. When a data request has been verified and authorised to go ahead, the relevant data or information must be retrieved from the systems or storage facilities and collated into an organised and readable format ready for disclosure. The information requested must be supplied as a copy or print out as the original copies must be retained by Helping Hands for the duration of the retention period set out in the Helping Hands Retention Schedule.

9.14.2. Emergency requests for information depend on the need and circumstances of each case. In this situation, an employee with access may disclose the information needed. Where possible, the following safeguards should be applied:

- Get approval from a senior manager before disclosing the information requested.
- If a request is taken over the telephone, try to verify the identity of the caller and confirm the authenticity of the request by asking for a 'landline' number to call them back with the information or call them back using a contact number obtained from a public source such as the organisation's website or an online directory.
- Request that a written request is sent as a follow up to record the request and reason for disclosure. This must be sent to **datarequest@helpinghands.co.uk**
- Write a statement documenting the date of the request, the actions taken to verify and authenticate the requester and the nature of the information disclosed. Send this to GDPR Compliance at **datarequest@helpinghands.co.uk** as soon as it is practical to do so.
- If there are doubts to the validity of the request, do not be pressured into disclosing information.
- It may be an option to ask the requester to submit the request in writing, and/or refer the enquiry to **datarequest@helpinghands.co.uk**

9.15. Securing Data

9.15.1. Confidential information containing personal or sensitive data must be password protected as a PDF document before it can be safely transferred electronically. Alternatively, it must be sent using a reliable and tracked delivery service.

9.15.2. Email **datarequest@helpinghands.co.uk** to ensure data is password protected and any redaction necessary to protect 3rd party data is actioned. Ensure that an original copy of the information is kept as once a password is applied, it will not be possible to open the protected document without the password. Keeping password records is a data security risk and must be avoided.

9.16. Data Disclosure/Transfer

9.16.1. It is acceptable and reasonable to send data by email if an email address has been provided or the initial request was received by email. The following guidance should be implemented to transfer data securely in response to a SAR.

9.16.2. Email:

- Mark the message 'Confidential' or 'Private'
- Do not include confidential information such as names in the email subject field. Use the reference number assigned or an appropriate title.
- Do not send confidential or sensitive information in the email itself and any attachments must be password protected.
- Remember to check the recipient email address is accurate to avoid email misdirection and a data breach.
- Check that the password protection has been applied and is working before it is forwarded to the requester.
- Never send the password and the protected file/document in the same email. Send the password in a separate email or disclose the password in a telephone call, after confirmation of receipt has been received.
- Notify GDPR Compliance once the disclosure has been successfully completed.

9.16.3. Post:

- Ensure that the Name and Address of the delivery destination is accurate and clearly written.
- Ensure that the package is marked as 'Private & Confidential' and sealed securely.
- Use a reliable tracked delivery service to ensure confirmation of delivery and receipt.

10. Data Breach

10.1. A breach is defined as: 'Personal data breach' meaning a breach in security leading to the accidental or unlawful destruction, loss, alteration, unauthorised access or disclosure to personal data that is transmitted, stored or processed.

10.2. There are three types of breaches:

- Confidentiality breach – unauthorised or accidental access to or disclosure of personal data
- Availability breach – unauthorised or accidental loss of access to, or destruction of personal data
- Integrity breach – unauthorised or accidental alteration of personal data

10.2.2. The source of the breach can be external or internal depending on where it originates from.

10.2.3. External affects technical and physical measures that are in place to prevent unlawful infiltration of building premises or software and business application systems.

10.2.4. Internal incidents are usually caused by negligence or failure to comply with HH policy and procedures. Breaches of this nature can be prevented if due care is taken.

10.2.5. Breach reporting is a legal requirement for all organisations and includes breaches that might not have been notified under the previous data protection regime. The traditional view that a data breach is only reportable when data falls into the wrong hands is no longer the case. Any risk to the rights and freedoms of an individual constitutes as a breach.

10.2.6. We need to recognise a potential or actual breach to ensure effective reporting takes place. The table below highlights some examples.

Types of Confidentiality Breaches	
External	**Internal**
- Virus infection (malware) causing a temporary loss of availability until data can be restored from back up. - Access to internal network systems or infrastructure where personal data is accessed by a cybercriminal.	- Data posted to incorrect recipient - Data faxed to incorrect recipient - Data sent by email to incorrect recipient - Failure to redact data

	- Verbal disclosure or discussion with unauthorised individuals - Failure to use bcc when sending emails - Unauthorised personal information uploaded to webpage

Type of Integrity Breach
Accidental or unauthorised alteration of personal data is where an instruction in a health or social care record has been 'misfiled' in the wrong place with the potential for significant consequences. e.g. A 'do not resuscitate' notice on the wrong patient record may have the significant consequence of death.

Types of Availability Breach	
External	**Internal**
- Virus infection (malware) causing a temporary loss of availability until data can be restored from back up. - Loss of availability of data even if not accessed - Corruption or inability to recover electronic data	- Loss or theft of paperwork - Loss or theft of unencrypted device containing personal data - Loss or theft of only copy of encrypted data - Loss of data in transit (stolen paperwork or hardware) - Data left in insecure location for any length of time before being recovered - Cryptographic flaws (weak encryption) - Non secure transfer of Data (not password protected / special delivery) - Insecure disposal of paperwork or hardware

11. Data Breach Risk Management

11.1. Employees at Helping Hands must report a data breach if they commit a breach, are notified of a breach or become aware that a breach has occurred. This also includes a 'near miss' data incident.

11.2. In the event of a data breach, the following actions need to take place:

- Identify and report the potential or actual breach
- Containment and Recovery of the data

11.3. Identify and report the potential or actual breach:

11.3.1. Once a breach has been identified, the individual responsible or assigned to report it to the data breach team and their line manager must do so without delay.

11.3.2. A Data Incident Notification (DIN) Form can be completed individually or collectively and signed off by line manager/ interim manager or the most senior member of staff. In the absence of a manager, it should still be submitted.

11.3.3. DIN forms must be submitted to databreach@helpinghands.co.uk within 24 hours and any unexpected delays to this process communicated to databreach@helpinghands.co.uk

11.4. Containment and Recovery of the data:

11.4.1. Managers are responsible for ensuring that the incident is investigated thoroughly, and steps taken to contain further loss or ongoing disclosure of the data.

11.4.2. Where appropriate, immediate actions or measures should be taken to recover the data or failing that, authorise for the destruction of the data.

11.4.3. Managers are required to identify who needs to be contacted and what actions are required to contain/recover/delete data (e.g. request that the recipient delete an email received in error and send confirmation of completed action).

11.4.4. Measures taken to contain or recover the affected data must be documented and evidenced where possible. In most cases, data may need to be deleted if it cannot be recovered. (e.g. email confirmation of data deletion from a recipient who received an email in error).

11.5. Investigation and Root Cause:

11.5.1. The outcome of reporting an incident should involve an investigation aimed at identifying not only what has happened to cause the breach but also why it has happened (root cause).

11.5.2. The appointed investigating can be supported by the GDPR coordinator where required.

11.5.3. Outcomes of the investigation should include learning actions which may include staff retraining, staff supervision, upgrading of systems, procedures or processes to prevent a similar breach in the future.

11.5.4. Evidence of planned corrective and preventative actions may be requested by GDPR Compliance.

11.6. The secondary role of GDPR Compliance is to review all DIN forms submitted as part of Helping Hands Data Breach Risk Management. This consists of:

- Risk assessment to quantify the impact and severity of the breach
- Evaluation and response at branch and organisational level

11.7. Risk Assessment on the impact and severity of the breach:

11.7.1. All incidents are reviewed by the GDPR Compliance team to establish the likelihood and significance of a data breach incident (see W.I-004 – Data Breach Risk Management work instruction).

11.7.2. GDPR Compliance liaises with the DPO to assess and grade the incident according to the impact on the individual or group of individuals affected.

11.7.3. When assessing the risk of an incident, it is a requirement to consider the potential impact and severity of those consequence to the affected individuals.

11.7.4. A risk assessment is also conducted for the impact on Helping Hands in relation to Strategy and Operations, Compliance, Financial Impact, Reputation and Continuity of Service.

11.8. Evaluation and Response at branch and organisational level:

11.8.1. The resultant risk score determines if there is a need to notify the affected individuals, regulatory authorities, external 3rd parties and organisations etc, and will determine in conjunction with the DPO whether the organisation's Business Continuity Policy should be invoked.

11.8.2. Managers will receive recommendations on appropriate safeguards or steps to prevent a future reoccurrence.

11.8.3. Evidence of corrective actions taken or implemented must be forwarded with the DIN form at time of submission or forwarded soon after.

11.8.4. Employees must not report any breaches to external parties or agencies until advised to do so by GDPR Compliance or the Data Protection Officer (DPO).

11.9. Notification of any data breach is subject to authorisation by the DPO who is responsible for notifying the Information Commissioner Office (ICO) within 72 hours of a breach occurring if deemed to be of significant risk and severity.

TRAINING

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

COMPLIANCE

How is compliance with the POL 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?	N/A	

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 staff, client or someone else's privacy?	N/A	*If yes, privacy impact assessment required*

What was the previous version number of this document?	N/A	
Changes since previous version	This is a new Policy	
Who was involved in developing/reviewing /amending the POL?	GDPR Coordinator Head of Quality Quality Development Lead GDPR Steering Group	
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	Information Governance Policy Information Security (Inc Cyber security) Policy Information Handling & Sharing Policy Privacy Information Policy Records Management, Retention & Deletion Policy Business Continuity Management Policy CCTV Policy Access Right Verification & Consent WI Data Breach Risk Management WI Subject Access Request WI Information Risk Management Standard Operating Procedure Information and Data Sharing Standard Operating Procedure Data Protection Impact Assessment (DPIA) Standard Operating Procedure Data Protection Impact Assessment (DPIA) Template Data Protection Impact Assessment (DPIA) Screening Checklist Data Incident Notification (DIN) Form

Appendix 1 - Definitions

ANONYMISATION- Data amended is such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person

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.

EXPLICIT 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.

CONTACT- Any past, current or prospective Helping Hands customer or employee

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 CONTROLLER- A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

DATE PROCESSORS- A natural or legal person, Public Authority, Agency or other body which Process Personal data on behalf of a Data Controller.

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

DATA SUBJECT- A living individual to whom the requested personal data relates to an individual who is the subject of personal data.

DIN- Data Incident Notification

DPIA- Data Protection Impact Assessment; a process to help identify and minimise the data protection risks of a project.

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.

ICO- Information Commissioning Office

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.

PROFILING- Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or generic characteristics relating to an identifiable Natural Person. To analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement

PSEUDONYMISATION- Data amended is such a way that individuals cannot be identified from the data (whether directly or indirectly) without a 'key' that allows the data to be re-identified

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

THIRD PARTY- An external organisation with which Helping Hands conducts business with and has been authorised by the data subject to process personal data obtained from Helping Hands.