Helping Hands
Caring since 1989

Title of Document	Information Governance Policy
Name of Department	Quality

What type of document is this?	Policy	
Which Helping Hands POL/SOP does this document relate to?	Data Protection 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-085 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	Superior Client Care	People, Performance & Culture	Business Growth
	Maximising Efficiency & Cost Management	Facilities & Sustainability	Internal & External Communications	Information Management & Technology

Custodian of document	Group Managing Director	Committee/Group 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 Helping Hands employees					
	Does it apply to bank workers?	Yes	Does it apply to agency staff?	Yes	Does it apply to third party contractors?	No

Purpose of the Policy	The purpose of this policy is to define our Information Governance framework providing a unified approach for handling information, which complies with the law and outlines best practice.

ROLES AND RESPONSIBILITIES

Role	Responsibility
Data Protection Officer	Provide advice and information on GDPR regulation and national law Own the Information Risks for Helping Hands Reporting to the board and contact point for employees and ICO notifications as required
Group Managing Director	To ensure compliance with Data Protection Legislation including UK GDPR, Data Protection Act 2018 and Privacy in Electronic Communications 2013, to highlight and escalate risks as per this policy.
Chief Financial Officer (supported by IT Director)	To ensure compliance with Information Security including Cyber Essentials, to highlight and escalate risks as per this policy.
Head of Quality (supported by Clinical Lead)	To ensure compliance with Care Records Management and Handling, retention and sharing of data, to highlight and escalate risks as per this policy.

1.0   Scope

    1.1   As an organisation we are committed to high-level coordination and oversight of Information Governance. This commitment ensures accountability and integrity and helps us to use information in a legal and ethical way, ensuring that data is safe, secure, available, up-to-date and accurate.

2.0   Framework for Information Governance

    2.1   Information Governance

    2.1.1   Information governance (IG) is the overall strategy for managing information at an organisation. Information governance balances the risk that information presents with the value that information provides. Information governance helps with legal compliance, transparency and the quality and efficiency of operations.

    2.1.2   Good information governance requires a mix of skills and knowledge and a logical framework to ensure that good practice can be demonstrated in all working procedures of the organisation.

    2.2   The Information Environment at Helping Hands

    2.2.1   The nature of Helping Hands operations requires us to process special category data of customers and employees 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 and employ.

2.2.2 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.

2.3 The Information Governance Framework at Helping Hands

2.3.1 The Information Governance Policy and the overall Information Risks are owned by the Group Managing Director, as a member of the Executive Team, represents Information Risk to the highest level of the organisation.

2.3.2 Information Governance is to be assured through three complimentary governance streams:

2.3.2.1 Data Protection
2.3.2.2 Information Security
2.3.2.3 Care Records Management and Handling

2.3.3 Each area has a defined owner and scope of responsibility and reports to the Quality & Governance Committee via the Information Governance Steering group.

2.3.4 The agreed framework is summarised in the following table:

Information Governance		
Owner: **Group Managing Director – Karyn MacKenzie**		
Committee: **Quality & Governance Committee**		
Data Protection	**Information Security**	**Care Records Management and Handling**
Accountable: Group Managing Director	**Accountable**: Chief Financial Officer	**Accountable**: Head of Quality
Responsible: Data Protection Officer	**Responsible**: IT Director	**Responsible**: Clinical Lead
Objective: Compliance with GDPR, Data Protection Act. ICO Accountability Framework	**Objective**: Compliance with Cyber Essentials and Access Control, Acceptable Use	**Objective**: Compliance with Care Records Management, Information Handling and Sharing, Code of Practice and Caldicott principles.

2.4 Resourcing and Co-Operation

2.4.1 There is significant overlap between these areas and good governance can only be achieved through close co-operation. It is the GMD's responsibility to ensure that this co-operation is effective and to organise appropriate methods and forums for this joint-working to happen.

2.4.2 The GMD will ensure that appropriate time, resources and skills are available to the owners of each area in order to adequately fulfil their responsibilities.

2.5 Level of Commitment

2.5.1 Helping Hands commits to meet all legal and mandatory regulatory requirements with regards to Information Governance.

3.0 Data Protection

3.1 Accountability and Responsibility

3.1.1 The Group Managing Director is accountable Data Protection.

3.1.2 The Data Protection Officer is responsible for ensuring compliance with Data Protection.

3.2 Objectives

3.2.1 To be aware of and comply with relevant Data Protection Legislation. Primarily UK GPDR, Data Protection Act 2018 and Privacy in Electronic Communications 2013. Primary regulatory body is the ICO.

3.2.2 To be aware of the requirements of and to ensure practice that is aligned with the ICO Accountability Framework

3.2.3 Escalate risks to the Quality & Governance committee

4.0 Information Security

4.1 Accountability and Responsibility

4.1.1 The Chief Financial Officer is accountable for Information and Cyber Security.

4.1.2 The IT Director is responsible for ensuring compliance with Cyber Essentials and putting in place appropriate cyber security controls.

4.2 Objectives

4.2.1 Ensure compliance with Information Security including Cyber Essentials.

4.2.2   To be aware of the Information Security requirements of NHS Data Security and Protection Toolkit and to implement appropriate controls and records to meet those requirements.

4.2.3   Escalate risks to the Quality & Governance committee.

5.0   Care Records Management and Handling

5.1   Accountability and Responsibility

5.1.1   The Head of Quality is accountable for the appropriate use of confidential health and care records and information about customers.

5.1.2   The Head of Quality retains responsibility on how customer data and care records are shared to non-operational teams and systems. Like all personal data, the Data Protection and Information Security (Inc Cyber Security) policies govern how that data is processed.

5.1.3   The Clinical Lead is responsible for ensuring that there are appropriate procedures and operating practices in place.

5.2   Objectives

5.2.1   To be aware of and ensure compliance with legislation and regulations that concern the management, retention and sharing of data.

5.2.2   Escalate risks to the Quality & Governance committee

TRAINING

Is training required?	No
Details of training	This policy establishes the information governance framework for Helping Hands. GDPR training is available through the Learning Management System – Academy.

COMPLIANCE

How is compliance with the POL going to be monitored	Monitored through quarterly Steering Group.

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 on the basis of their:		
• age?	N/A	
• disability?	N/A	
• gender reassignment?	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 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?	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	Data Protection Policy Information Security (inc Cyber Security) Policy Information Handling & Sharing Policy Privacy Information Policy Records Management, Retention & Deletion Policy