Policy Name	Module
Confidentiality & Data Protection	**Human Resources**

Statement of purpose

Hand in Hands is fully committed to compliance with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2018.
The above legislation/regulation applies to any organisation processing personal data, sets out the principles which should be followed and gives rights to those whose data is being processed.

Hand in Hands understands that confidentiality and data protection is not only our duty but every individual's right. It is central to developing trusting relationships, where individuals, employees and other relevant stakeholders can live safe in the knowledge that their confidences will be kept and where information about them will be protected.

This policy aims to comply also with the current obligations and requirements set by the:

- ✓ *Health and Social Care Act 2008 (Regulated Activities) Regulations 2014;*
- ✓ *Care Quality Commission (CQC) Fundamental Standards;*
- ✓ *Data Protection Act 2018;*
- ✓ *General Data Regulation 2018;*
- ✓ *Information Commissioner's Office (ICO);*
- ✓ *The7 Caldicott Principles;*
- ✓ *The Common Law of Confidentiality;*
- ✓ *The Human Rights Act 1998;*
- ✓ *The Care Act 2014:*
- ✓ *The Health and Social Care (Safety & Quality) Act 2015;*
- ✓ *Freedom of Information Act 2000;*
- ✓ *The Health and Care Act 2022.*

We all have a responsibility to safeguard confidential information and preserve information security throughout all daily practices within Hand in Hands. We are fully committed to protecting the privacy and security of all personal information and seek to be transparent in the way in which we process data on behalf of those we support, employees and other relevant stakeholders.

This policy intends to outline the principles that must be implemented by Hand in Hands and its employees when accessing and processing personally-identifiable or sensitive information, in order to protect this information from being accessed, handled, stored or shared unlawfully.

As the Data Controller, Hand in Hands fully recognises, supports and adheres to the Data Protection/GDPR Principles listed below. When processing data we will ensure that it is:

- ✓ Obtained and processed fairly, lawfully and in a transparent way;
- ✓ Processed and used for specified, explicit purposes only;
- ✓ Processed in a way that is adequate, relevant and limited to only what is necessary;
- ✓ Always accurate and kept up to date;
- ✓ Kept for no longer than is necessary;
- ✓ Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage;
- ✓ Processed by a controller who can demonstrate compliance with the principles.

It is the overall responsibility of the Registered Manager to ensure that all staff have read and signed (as understood) this Policy and Procedure for Hand in Hands, and that it is implemented consistently in daily practice. It is the overall responsibility of every staff member to follow this policy

and procedure. Failure to do so may lead to disciplinary action.

All staff are expected to sign the Confidentiality Agreement during the induction process to the organisation.

A current copy of the policy will be available in the Main Office.

This policy will be reviewed at least annually, or more frequently if significant changes occur.

This person accountable for this Policy/Procedure is Michelle Dudderidge.
This Policy / Procedure was last updated on 17/02/2023.
This Policy / Procedure is due to be reviewed on 12/11/2023.

Definitions

Data Protection - Is the process of safeguarding important information from corruption, compromise or loss.

Confidentiality - Refers to maintaining the privacy of sensitive or restricted information. Confidentially does not mean to keep things a secret, but rather ensuring that only those who need to know or have a right to confidential information have access to it.

Personally-identifiable information - Is any information that identifies a person, either directly or indirectly, for example, a person's name and address.

The Health and Social Care Act 2008 (as amended) defines 'confidential personal information' as information that is:

"obtained by the commission on terms or in circumstances requiring it to be held in confidence"
and that:
"relates to and identifies an individual".

Data Controller(s) - A data controller is the person(s) that decides how and why to collect and use data. Within Hand in Hands the Data Controller is *Registered Manager, Michelle Dudderidge.*

Sensitive personal information - Any personal data that reveals:

- ✓ Race
- ✓ Ethnic background
- ✓ Political opinions
- ✓ Religious or similar beliefs
- ✓ Trade union membership
- ✓ Genetics
- ✓ Biometrics (where used for identification)
- ✓ Physical or mental health condition
- ✓ Sexual life or orientation

Hand in Hands will comply with stronger legal protection for such sensitive information.
There are separate safeguards for personal data relating to criminal convictions and offences.

Business sensitive information - Includes anything that poses a risk to the organisation or its' reputation if it is disclosed.

Subject data - The identified or identifiable living individual to whom personal data relates. For example, this will include individuals and staff.

Consent - The consent of the 'data subject' means any freely given, specific, informed and unambiguous indication of his or her wishes, either by a statement or a clear affirmative action, that signifies the 'data subject's' agreement to personal data relating to them being processed. This type of consent may also be called 'explicit' or 'expressed' consent.
Implied consent is when an individual or others, provide consent through signalling, using gestures or behaviour to show compliance.

Secure systems - Refers to systems in place to ensure that information is kept safe, maintained and made available when needed, to authorised persons only.

'Need to Know'- Refers to the sharing of information when it is necessary and only to the people who need to know it.
All staff have a duty to protect every individual's confidentiality (this includes the children they come into contact with). However, if an individual or child is at risk of harm or poses a risk to others, this duty of care may be overridden to protect their best interest, or the interest of the public.

👉 *Please view further information around key legislation and codes of practice in Appendix 1*

Data Subject Rights

Under the Data Protection Act 2018 and The General Data Protection Regulation (GDPR) everyone has the following rights in respect of the personal data that Hand in Hands obtains, uses, shares and stores:

- ✓ The right to be informed about how personal data is processed by Hand in Hands;
- ✓ The right to access personal data and verify its' accuracy;
- ✓ The right to have data updated if the information is inaccurate or incomplete;
- ✓ The right to be forgotten and have data erased;
- ✓ The right to stop or restrict the processing of personal data;
- ✓ The right of data portability (allowing information to be transferred to another organisation/service);
- ✓ The right to object to how personal data is processed in certain circumstances;
- ✓ The right not to be subject to decisions without human involvement. I.e. automated decision-making processes that predict behaviours or interests.

👉 *For further information on your rights can be found on the following website: www.ico.org.uk*

Privacy Notice

The General Data Protection Regulation (GDPR) requires all 'Data Controllers' to provide certain information to the individuals whose data they hold and process; this is known as a Privacy Notice. The Hand in Hands Privacy Notice is available upon request and is located in the Main Office.

Hand in Hands commitments towards maintaining confidentiality, data protection and following governing principles are as follows:

- ✓ To observe and monitor fully the conditions regarding having a lawful basis upon which to process personal information;
- ✓ Always meet its legal obligations to specify the purposes for which information is to be used;
- ✓ Ensure that all personal and confidential information is effectively protected against improper disclosure when it is received, stored, shared or disposed of.
- ✓ Ensure that all personal information will be treated with respect and integrity at all times.
- ✓ Ensure that consent is obtained from the individual and/or their representatives concerning the gaining and sharing of information about them.
- ✓ Ensure clarity when obtaining information from individuals and/or representatives and employees. Provide explanations of why information is to be collated and the intentions of its use.
- ✓ Ensure security systems and procedures are in place to protect personal information and data.
- ✓ Regularly review records held to ensure they are accurate and held for no longer than is necessary;

- Ensure that staff are fully aware of the legal and moral obligations they have when processing personal and sensitive information.
- Ensure that all staff are trained and supervised in order to enable effective compliance with this policy.
- Ensure that only sufficient and relevant information is gained and processed within care documents.
- Ensure that all individuals are informed of their right to not provide consent for information to be used and their right to complain if they are not satisfied with the security of their personal information.
- Fulfil our duty of candour and apologise where mistakes happen around the processing of their information and provide support as necessary to preserve rights.
- Promote transparency by allowing information about Hand in Hands services and any outcomes to be shared with individuals and other stakeholders.
- Ensure that all individuals and staff have the right to access information that is held about them and that they can access this information with the support of Hand in Hands.
- Take any breaches of confidentiality seriously and take disciplinary action where necessary.
- Ensure that personal or sensitive information is not transferred outside of the EU, to other countries or international organisations without an adequate level of protection.

Hand in Hands data will not be:

- Communicated informally;
- Stored for more than a specified amount of time;
- Transferred to organisations or countries that do not have the adequate data protection policies or legislation;
- Shared or distributed to any party other than the ones agreed upon by the data subject; (exempting legitimate requests from law enforcement authorities).

Responsibilities

Data Protection Compliance

Hand in Hands has appointed Registered Manager, Michelle Dudderidge as the organisation's compliance officer who is responsible for the management and effective implementation of data protection activities and policies. Ensuring the organisation and its employees are informed, supported and trained in mandatory data protection and confidentiality.

They can be contacted on the following details:
Devonshire Business Centre, Works Road, Letchworth, Hertfordshire, SG6 1GJ
01462 222400

The Registered Manager - is ultimately responsible for ensuring compliance with this policy. The Registered Manager is required to ensure that its' standards are maintained consistently in daily practices and any breaches of data security are reported to relevant regulators.

Responsibilities - All Employees

It is everyone's responsibility within Hand in Hands to be aware of the importance of maintaining confidentiality, including their responsibility and duty to safeguard individuals confidentiality and ensure that personal and sensitive data is consistently kept secure.

All employees must comply with current codes of practice, regulations and legislation and ensure they fully understand them. No employee shall knowingly misuse any information or allow others to do so. Breaches of confidentiality or data security breaches will be taken very seriously and non-compliance of this policy may result in disciplinary action being taken.

All employees must ensure that any personally-identifiable or confidential information is effectively protected against improper disclosure when it is received, stored, shared, disposed of, or otherwise processed in any way.

It is expected that all employees always remember that individuals and our employees have the right to privacy and dignity and any information must be handled or shared sensitively.

All employees must ensure that all personal information is treated with respect and in the best interest of the person to whom it relates.

This duty of confidentiality at all levels is detailed within employee contracts.

Data Security

Hand in Hands takes the security of data extremely seriously. We therefore use appropriate and safe technical and organisational measures to keep personal data secure, and to protect against unauthorised or unlawful processing, accidental loss, destruction or damage.

Our secure systems in place ensure that:

- ✓ Only authorised persons have access to and use personal information;
- ✓ Authorised persons can access information only if they require it for authorised purposes;
- ✓ Where possible, personal data is password protected or encrypted.

Third parties will only process your personal information on our instruction and where they have agreed to treat the information confidentially and securely.

Our security procedures include:

- ✓ All manual/paper based data is stored securely within locked cabinets and desks within Hand in Hands premises.
- ✓ All computers are password protected to reduce the risk of unauthorised access when left unattended.
- ✓ Any data that needs to be stored on CDs or memory sticks are encrypted or password protected and locked away securely.
- ✓ All servers containing sensitive data must be approved and protected by security software
- ✓ The Registered Manager or Director must approve any electronic systems or cloud used to store data before use.
- ✓ All data is backed up in accordance with data protection procedures.
- ✓ Confidential paper or electronic records cannot be removed from Hand in Hands premises or our individuals homes, except in line with the agreed protocol or procedure.

Hand in Hands and all employees are legally obliged to adhere to the Data Protection Act 2018, General Data Protection Regulation 2018, Common Law Duty of Confidentiality and Confidentiality Codes of Practice to ensure the protection of all personal data.

Consequences of Non-Compliance

If the organisation does not comply with legislation of any kind, then we will be breaking the law, which means that we will be heavily fined. The organisation's practices will be reviewed, and its' good reputation will be damaged as a result.

If staff member(s) do not comply with legislation in every working practice, then they may be in breach of their contract. They may also be in breach of their duty to promote the confidentiality and safeguarding of information, as per the basic human rights of the individuals we support.

If Hand in Hands discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of any individuals, we will report this within 72 hours of discovery to the Information Commissioner's Officer.

If the breach is likely to result in a high risk to the individual's rights and freedoms, the organisation will inform the individual(s) immediately and inform them of the mitigation measures we have taken.

All staff must be aware that any breach of data security or confidentiality will be handled in accordance with the Hand in Hands Disciplinary Procedure. The breach may also generate grounds for complaint or legal action against them by the organisation or the individual/s concerned.

National Data Opt-Out

The National Data Opt-Out is a service that allows individuals to opt out of their confidential health information being used for any reason beyond their care and treatment, such as for research and planning purposes. In July 2022 it became a requirement for all adult social care providers to be compliant with the national data opt-out policy.

Hand in Hands reviews all of our data processing on an annual basis to assess if the national data opt-out applies. This is documented in our record of processing activities. All new processing of data is assessed to see if the national data opt-out applies.

Consent

Giving consent for information to be obtained or shared is everyone's right and consent from individuals must be sought before requesting their information. This includes supporting individuals to understand the possible need to obtain information from previous care notes for additional information.

Whilst individuals usually understand and accept that information needs to be gained and shared within the care team and others such as GPs and Nurses etc to enable holistic care, it is still necessary that permission from the individual or the representative acting on their behalf, is gained and that they fully understand what information is disclosed and to whom as is their right.

Disclosing information without this consent may lead to a breakdown in trust, confidence and relationships between individuals/representatives and Hand in Hands. This can also cause individuals to be reluctant to give information that may be required to provide the appropriate level of care.

Individuals have the right to give, as well as withdraw their consent for processing information at any time.
When seeking consent from an individual during new and review assessments, staff must show the individual and/or representative (if applicable) the Hand in Hands 'Privacy Policy'. This is to ensure

they are aware of their rights and what to expect from Hand in Hands in terms of how their information will be obtained and handled and that they consent to this.

The individual or their representative should also be asked to agree to information being released or shared through the organisation's *'Consent to Share Information Form'*.

👉 *Please see Appendix 2 for a copy of the Information Consent to Share Information Form.*

Staff must support the individual to make informed choices and decisions around their care and the handling of their personal information. When doing so, staff must be very clear and honest with the individual around why their information is required and how it will be used. Time and opportunity should be given to the individual/s to ask questions and seek further advice from people they trust if they wish.

All staff will be asked to sign a 'Consent to Share Information Form', to provide their consent on the sharing of their information.

Mental Capacity

The Mental Capacity Act 2005 applies to all adults who do not have the capacity to provide consent. Under this act, individuals are presumed to have capacity, unless they have had the appropriate assessments to determine that they do not, due to an impairment affecting the mind e.g. dementia or a learning disability, which means they are unable to make specific decisions within a specific time.

It is also a requirement that all practical steps have been taken to help and provide opportunity to enable individuals who do not have capacity to make decisions wherever possible.

The overriding principle is that the disclosure of confidential information is made in the best interest of the person lacking capacity. This may involve releasing information about their condition, for example, to their carer, to ensure they receive the best treatment.

Exemptions to Confidentiality and Consent

All Hand in Hands employees have a responsibility to safeguard and promote the well-being of all individuals. In specific situations, a disclosure of personal information without the consent of the individual may be justified where failure to do so may put the individual or others at serious risk. Generally, confidentiality can be broken if it is to prevent a person from being harmed or to comply with the law.

It is acceptable to break normal confidentiality rules in the following situations:

- ✓ Where a person is in grave or imminent danger;
- ✓ Where there is risk of harm to themselves such as suicidal behaviour;
- ✓ To prevent abuse or harm. When the abuse of a child or adult is disclosed or suspected;
- ✓ When the health and safety of the person or others is at risk;
- ✓ When disclosure is in the public interest;
- ✓ When a criminal offence has occurred or is likely to occur;
- ✓ When a court orders specific information about an individual to be disclosed.

In such circumstances, Hand in Hands reserves the right for staff to break their duty of confidentiality and to take the information to the Registered Manager and/or local authorities such as, the Local Safeguarding Adults/Children Boards, the police or emergency services.

In these circumstances, the individual will be informed of Hand in Hands position and duty to them and others, with full details being discussed with the individual and/or the relevant person. Appropriate notes will be made in the individuals care and support plan, safeguarding logs and/or accident & incident forms. These notes will be open to inspection by the individual at any time if they wish.
The information will only be shared with those who need to know and wider issues of confidentiality relating to that information will still apply.
All Hand in Hands individuals will have accessible complaints procedures and will be free to make a complaint via this procedure if they wish. They will be fully supported throughout the process.

👉 *Please view further guidance on how to raise concerns and report incidents with the 'Accident, Incident, Investigation & Falls Prevention Policy' and the organisation's 'Safeguarding Adults at Risk Policy'. These policies can be found* in the Main Office.

Disclosure of Personal Data to Third Parties

It is very important to us to provide our individual with holistic care to meet their needs and wishes. To do this effectively, we may sometimes need to share information about our individuals with others such as other professionals or agencies involved in their care and treatment. This is done so with our individual consent and on a 'need to know' basis. Only staff who are directly involved in the individual care and support will have access to their personal and sensitive information through their personal Care & Support Plan.

Hand in Hands will not disclose personal information about our employees without permission, for example, when contacting previous employers for the purpose of references.

As part of our duty of care to ensure the safety and wellbeing of our individuals and staff, there may be exceptions to seeking consent for information to be disclosed. This would be when we are required by law to provide information, e.g. to help with a criminal investigation.

When seeking to notify the local authority of a safeguarding matter or the Care Quality Commission (CQC) of an incident that requires us to notify them, we would only do so with consent or by ensuring that the information provided is treated in confidence. We will share information for everyone's best interest in the event of an emergency. We expect all third parties to respect the security of data they receive.

International Data Transfers

Hand in Hands does not transfer personal or sensitive data to any recipients outside of the EEA.

Access to Records

Individuals have a right under Data Protection law and General Data Protection Regulation (GDPR) to access personal information that is held about them, this includes Hand in Hands employees. The information that can be shared with the individual is limited to 'personal data' that relates to them only, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone).

Requests can be made in any form i.e. verbally, email or letter. The organisation also supplies a form that can also be used electronically or posted to assist individuals in making a subject request. The organisation does advise all individuals to aim to complete our Subject Data Request Form

when requesting personal data, as this will be the quicker process for the organisation to deal with the request.

👉 *Please see Appendix 3 for a copy of the Subject Data Request Form.*

Where requests are made by individuals to access this data, Hand in Hands will take the following steps:

- ✓ Provide the individual with a 'Subject Data Request Form';
- ✓ Request proof of ID to support the request;
- ✓ Request proof of authority to request information on behalf of a 'Data Subject';
- ✓ Respond to the request within one month of receipt of the request.

Under complex circumstances or in the event of numerous requests from the individual, an additional two months may be added to the response time.

No charges will be made by Hand in Hands for the supply of subject data unless:

- ✓ It is manifestly unfounded or excessive; or
- ✓ An individual requests further copies of their data following a request.

Refused Requests of Records

On rare occasions the request to access personal records can be refused. The occasions may include:

- ✓ Where it is likely to cause serious harm to the physical or mental health of the individuals or to others;
- ✓ Where the information requested relates to another person.

Such decisions must only be made by the Director and Registered Manager.
Decisions must be considered in light of the legal duty under the Data Protection Act 2018 and the General Data Protection Regulation 2018.
The decisions must be clearly explained to the individual concerned and recorded appropriately.

The Right to Make a Complaint

Everyone has the right to complain if they feel, at any time, Hand in Hands has failed to safeguard their personal information.

In the first instance, Hand in Hands would ask everyone to contact us on the following contact details to allow us to investigate the matter thoroughly to identify any security issues.

Name and Position:	
Telephone:	
Email:	
Address:	

If anyone believes we are not processing their data or respecting their rights relating to the handling or security of personal information, or if they feel we have not been able to resolve their complaint to their satisfaction, they have the right to lodge a complaint with the Information Commissioners Office (ICO). The ICO are the UK's regulatory authority around data protection. All individuals are entitled of course to contact the Information Commissioner's Office without first referring their complaint to us.

Information Commissioner's Office
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF,
UK: +44 (0) 303 123 1113,
Email: casework@ico.org.uk
Website: https://ico.org.uk/make-a-complaint/

Hand in Hands requests that any individual who objects to the processing of personal data, wishes to access, review, verify, correct or request erasure of their personal information; or wishes for a copy of their personal information to be transferred to another party, please contact us on the following contact details:

Name and Position:	
Telephone:	
Email:	
Address:	

Storage & Retention

Hand in Hands will not keep any data for longer that is necessary in line with the Data Protection Act 2018 and General Data Protection Regulation 2018 principles.

We will always hold your personal information whilst you still receive our services/are still employed under Hand in Hands.

- ✓ We shall hold your personal information that is stored within our electronic and manual individual files for 7 Years.
- ✓ We shall hold employee personal information that is stored within our electronic and manual files for 7 Years.
- ✓ Data that is gathered from your feedback during compliments, complaints, grievances, incidents and safeguarding logs will be held for 7 Years, to support Hand in Hands to identify areas for improvement to our services and identify particular patterns and trends.

👉 *Please view further information and guidance within the 'Data Retention & Disposal' Policy & Procedure. This policy can be found* in the Main Office.

Procedures

Responsibilities - All Employees

When Handling Information, All Staff Must:

- ✓ Only access personal information if it is appropriate to the job that the employee is to undertake.
- ✓ Maintain confidentiality when dealing with personal/sensitive information about an individual, their family/representatives, colleagues and others whom the organisation works with.
- ✓ Never share personal information about an individual to another individual, their families or any unauthorised persons, or enter into gossiping conversations about others.
- ✓ Never gossip or share personal opinions about an individual, their family, colleagues or others or pass on information to any other individual other than for professional reasons.
- ✓ Never have conversations relating to confidential matters affecting an individual in public spaces where information can be overheard by unauthorised persons, for example, in the car with the window down or outside of work.
- ✓ Discussions on confidential matters should take place where they cannot be overheard at any time.
- ✓ Only pass information on that is relevant to the individual care needs and with their expressed consent, the consent of the Registered Manager and the individual representative (if applicable), to others within the care team, or other professionals involved with the individual care, on a 'need to know' basis.
- ✓ Ensure that every effort has been made to inform an individual why information is to be obtained, how the information about them is to be used and held, what and when information is going to be shared and to whom, including the reasons for disclosure and possible outcomes or consequences.
- ✓ Inform individuals of their right to not disclose information or provide consent to information about them being shared.
- ✓ Ensure individuals are aware of their rights, including those to withdraw consent.
- ✓ In the event of an emergency or when it is in the best interest of the individual, share information on a 'need to know' basis which must be passed on without delay.
- ✓ Share confidential information when appropriate, relevant and necessary with colleagues with whom they are sharing care activities for the benefit of that individual.

- Pass and receive confidential information to and from colleagues on occasions when there is a need for staff to replace other staff due to sickness, holidays or other appropriate reasons, responsibly and respectfully.
- Seek advice and guidance from the Registered Manager if there are any concerns, doubts or worries about how to handle or share information in the workplace.
- Direct any external requests for information from other professionals or agencies to the Registered Manager.
- Be aware of this policy and fully understand own role and responsibilities around the handling of information and key legislations.
- Not identify individual or others within the organisation during training or team meetings. Any discussions during this time must be treated with respect and caution to not breach individual rights to confidentiality.
- Never discuss the commercially sensitive information of Hand in Hands, such as new projects, plans, pay rates or details of accounts to anyone who is not authorised or directly involved within the organisation.
- Confidential information relating to anyone connected to Hand in Hands should not be given over the telephone unless consent has been gained from the Registered Manager and individual first. Unless however, it is in the event of an emergency, or information is being disclosed to the individuals' representative/advocate or a professional involved with the individuals' health and care, such as their GP or Social Worker.
- Wherever employees have any doubt as to what information and to whom information is to be disclosed, employees must not give any information before seeking guidance from the Registered Manager first.
- All envelopes containing confidential or personal information should be clearly and fully addressed and securely sealed.

When Storing Information, All Staff Must:

- Ensure written records and correspondence are kept securely at all times when not being used by staff members i.e. timesheets or rotas etc. They must not be left unattended in vehicles, public transport or elsewhere.
- Ensure that all files or written information of a confidential nature (within Hand in Hands office) are stored securely within a locked filing cabinet and are only accessed by staff who have a need or a right to access them. If staff wish to view information stored within locked cabinets and filing systems then they must request permission from the Registered Manager first.
- Within the homes of individual, a designated safe and secure area of where the care documents will be stored will be agreed with the individual. This may include a secure draw or cupboard and is only accessed by those who are authorised to view it.
- Ensure care documents are not left lying around and are stored away immediately after use.

Electronic Information Storage Systems, All Staff Must:

- Ensure computer screens are locked whenever they are unattended.
- Always log off fully when finished with the computer.
- Use secure passwords to enter into computers and computer-based/electronic files to prevent unauthorised persons viewing confidential information. Staff must not share their password and it is advised to change passwords regularly to maintain the security of information.
- Ensure computers and laptops have been logged out of before leaving them unattended.
- Use file protection on files stored on computers to protect records from being deleted or altered.
- Use firewall protection software on computers to ensure that others outside of the organisation cannot view personal data.
- Use anti-virus software on electronic devices to prevent information and data from being deleted, interrupted or interfered with.

- ✓ All information stored within electronic devices should be backed-up to prevent information and data from being lost and ensure that it can be easily retrieved. Ensure that consent has been gained from the Registered Manager before information is backed up on manual devices such as memory sticks as they can be easily lost or stolen and are an insecure method.
- ✓ Ensure that no files are deleted or destroyed without the permission from the Registered Manager first.
- ✓ Ensure that no individual files are removed from the main office, unless permission has first been granted by the Registered Manager for this to happen. Any documents being taken out of the main office should be signed in and out so the location of personal information is always known.

Mobile phones and Smartphones

All employees are expected to follow procedures outlined within Hand in Hands 'Code of Conduct for Staff' Policy and as outlined within Employee Handbooks. The policy can be found in the Main Office, and each staff member should have a copy of their Employee Handbook. Employees should contact the Registered Manager if they have misplaced their Employee Handbook.

Staff must always be aware of the conversations they have on their mobile phone when speaking to other colleagues, the Registered Manager or On-Call for example, as confidential information that is necessary to share with the care team may not be appropriate in public places or in another individual's home.

Where smartphones are used in the delivery of care such as via 'apps' or other 'electronic devices' these must always be password protected and logged out of properly after use to prevent unauthorised persons viewing confidential information.

Staff must ensure that all mobile phones or other devices included as part of their work are kept with them at all times, to reduce the risk of them being stolen or lost.

Social Media

All employees are expected to follow procedures outlined in the Hand in Hands Photography & Social Media Policy & Procedure. This policy can be found in the Main Office.

Staff are prohibited from sharing information about an individual or the organisation on social media networking sites, this includes taking and posting photos online.

Email

Careful consideration must be taken before sending confidential information via email and the following steps are necessary security measures that Hand in Hands employees should take when doing so:

- ✓ Consider if information is required to be sent via email at all or is there a more secure and appropriate method?
- ✓ Ensure the recipient of this information is aware that the information is going to be sent to them electronically.
- ✓ Never include personally-identifiable information within the subject line of the email.
- ✓ Any personal or confidential information should be attached to the email, rather than included within the main email itself.
- ✓ Highly sensitive information should be password encrypted and passwords to them should not be included in the original email.
- ✓ Caution should be taken to ensure the correct email addresses are entered before sending them.

Facsimile (Fax)

Before faxing any personal information, confirmation should be sought from the addressee that the information within it will be confidential and only viewed by the person meant to receive it. Faxed information is not a secure method of sending and receiving information and can breach legislation and regulations if used incorrectly. The following must be considered:

- ✓ Consider if information is required to be sent via fax at all or is there a more secure and appropriate method?
- ✓ Ensure the recipient of this information is aware and available first before faxing information to prevent the risk of unauthorised persons viewing information that is not meant for them.
- ✓ Always send a cover sheet stating that information is confidential to make others aware that the contents are only to be viewed by authorised people.
- ✓ Confirm with the recipient by telephone or email to ensure that they have received the information safely.

When Sharing Information All Staff Must Be Aware Of The Seven Golden Rules.

Seven Golden Rules for Information-Sharing

- ❖ **Remember that the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) are not barriers to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.
- ❖ **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be, shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
- ❖ **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.
- ❖ **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
- ❖ **Consider safety and wellbeing:** base your information-sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.
- ❖ **Necessary, proportionate, relevant, accurate, timely and secure:** ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.
- ❖ **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose

👉 *Source:- HM Government – Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers July 2018*
👉 *https://www.england.nhs.uk/wp-content/uploads/2017/02/adult-pocket-guide.pdf*

Concerns over the Recording, Storage and Sharing of Information

During day to day work activities, a lot of information is recorded, stored and shared constantly, there may be occasions when the correct procedures are not being followed for several reasons.

Examples may include:

- ✓ Staff not fully understanding what information can be shared and to whom, therefore confidential information is shared to others who are not authorised to hear or view it.
- ✓ Staff not recording information accurately within care plan notes or MAR charts or any other documents, therefore leading to the individual care needs not being met.
- ✓ Staff not understanding the importance of where to store care documentation within the individual's home, therefore leaving personal information around so that it can be easily viewed by unauthorised people.
- ✓ Staff are overheard talking about individual in public areas.

This is not an exhaustive list, therefore staff must report any concerns or worries they have directly to the Registered Manager to gain clarity of their role or to ensure breaches of data or confidentiality are addressed appropriately.

If staff do not feel that their concerns have been addressed at all or appropriately, then they must report the matter to the next most senior person.

If the matter has still not been resolved then staff are advised to follow the 'Whistleblowing' Policy and Procedure. This policy and procedure can be found in the Main Office.
This is a part of all employees' duty of care to report poor practice or suspicions of abuse which is supported by legislation.

Disposal of Information

Any confidential or personal information that is no longer needed should be destroyed and shredded promptly.
No records or information should be destroyed without consent from the Registered Manager first.

- 👉 *Please view further information and guidance within the 'Data Retention & Disposal' Policy & Procedure. This policy can be found* in the Main Office.

Training

All new staff are required to read and understand the policies and procedures relating to Confidentiality and Data Protection as part of their induction process. Staff are also required to achieve the mandatory Care Certificate Fundamental Standard 14 'Handling Information' to define knowledge, skills and behaviours that are expected as part of job roles in health and social care.

All staff who use computer systems will be thoroughly trained in its' use.

All staff will be trained in the organisations secure systems and reporting procedures.

All staff are responsible for attending mandatory training and keeping up to date with legislations and best practice.

Monitoring

It is Hand in Hands Registered Managers responsibility to regularly monitor and review the effectiveness and quality of records and documentation to ensure the standards of this policy are maintained.

Relevant Legislation

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Data Protection 2018

http://www.legislation.gov.uk/ukpga/2000/36/contents
- Freedom of information Act 2000

http://www.legislation.gov.uk/ukpga/2014/23/contents/enacted
- The Care Act 2014

http://www.legislation.gov.uk/ukpga/1998/42/contents
- Human Rights Act 1998

http://www.legislation.gov.uk/ukpga/2005/9/contents
- Mental Capacity Act 2005

http://www.legislation.gov.uk/ukpga/1990/18/contents
- The Computer Misuse Act 1990

http://www.legislation.gov.uk/ukpga/1998/23/contents
- Public Interest Disclosure Act 1998

http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted
- Health and Social Care (Safety & Quality) Act 2015

Relevant Regulations

https://ico.org.uk/
- Information Commissioner's Office

https://www.scie.org.uk/publications/adultsafeguardinglondon/informationsharing/legalframework.asp
- Common Law Duty of Confidentiality

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
- General Data Protection Regulation 2018 (GDPR)

https://www.legislation.gov.uk/uksi/2014/2936/contents/made
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014

http://static.ukcgc.uk/docs/code.pdf
- NHS Digital (formally HSCIC) Code of Practice on Confidential Information 2014

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/a-guide-to-confidentiality-in-health-and-social-care
- NHS Digital (formally HSCIC) Guide to confidentiality 2013

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/records-management-code-of-practice-for-health-and-social-care-2016
- Records Management Code of Practice for Health and Social Care 2016

https://www.cqc.org.uk/sites/default/files/20150324_guidance_providers_meeting_regulations_01.pdf
- Regulation 9: Person-centred care
- Regulation 10: Dignity and respect
- Regulation 11: Need for consent
- Regulation 17: Good governance

- Regulation 20: Duty of candour

https://www.skillsforcare.org.uk/Documents/Topics/Digital-working/Information-sharing-for-social-care-employers.pdf

- Information Sharing for Social Care Employers/ Skills For Care

https://www.legislation.gov.uk/uksi/2000/2699/contents/made

- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Key Lines of Enquiry KLOE

SAFE: How do systems, processes and practices keep people safe and safeguarded from abuse?

- Do staff have all the information they need to deliver safe care and treatment to people?

Effective: How are people's care and treatment outcomes monitored and how do they compare with other similar services?

- Is consent to care and treatment always sought in line with legislation and guidance?
- How well do staff, teams and services work together within and across organisations to deliver effective care and treatment?

Caring: How are people's privacy, dignity and independence respected and promoted?

Well-led: Are there clear responsibilities, roles and systems of accountability to support good governance and management?

- Are there clear and effective processes for managing risks, issues and performance?
- Is appropriate and accurate information being effectively processed, challenged and acted on?
- Are there robust systems and processes for learning, continuous improvement and innovation?

Appendix 1

Data Protection Act 2018

The Data Protection Act sets out the rights people have in relation to how information about them can be legally used, recorded, stored and shared. Any organisation, business and the government must follow strict rules called 'data protection principles' to ensure that information is protected from being misused or abused. The 'data protection principles' are as follows and state that information should be:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

General Data Protection Regulation (GDPR)

GDPR shares many of the principles and rights stated within the Data Protection Act. The GDPR enhances people's rights by placing more emphasis on how personal information is to be shared and managed within the organisation.

There are seven GDPR principles which must be followed when storing and managing personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and Confidentiality
- Accountability

Freedom of Information Act 2000

This Act sets out people's rights to access general information that is held about them by public authorities such as the NHS healthcare records and the police.

NHS Digital (formally HSCIC) Code of Practice on Confidential Information 2014
This code of practice sets out the rights people have when confidential health and care information is collected, analysed, published or shared by organisations.

NHS Digital (formally HSCIC) Guide to confidentiality 2013
This guide provides health and social care workers with information on how to share information safely and gives 5 rules around confidentiality.

Rule 1: All confidential information about individuals must be respected and treated confidentially.
Rule 2: Confidential information should be shared when it is needed for the safe and effective care of an individual.
Rule 3: Information that is shared for the benefit of the community should be anonymised.
Rule 4: Respect the right of the individual not to have their confidential information shared.
Rule 5: Organisations should have policies, procedures, and systems in place to maintain confidentiality.

Health and Care Act 2022

This Act supports the collaboration of Integrated Care Systems (ICSs) in different geographical areas to improve the health of the population within that area and the services that are provided/available to them. It introduces changes to public health and outlines the responsibilities of public bodies in handling information and sharing data in order to provide joined-up, co-ordinated care that meets individual needs in a person-centred way.

Human Rights Act 1998

This Act sets out people's rights and freedoms within the UK. Everyone has a right to be treated fairly, with respect and dignity. In relation to handling information, the law states under Article 8 that everyone has the right to respect for their private, family life, home and correspondence, which includes letters, telephone calls and emails.

The Care Act 2014

This Act sets out the rights of people in relation to being able to access information and advice about their care and support from local authorities. It also sets out people's rights concerning the sharing of information when there are safeguarding concerns.

The Caldicott Principles

The Caldicott principles are a set of 7 fundamental principles that should be followed to protect information that could identify a person. They also include principles on how information should be used and shared appropriately. The principles in addition to the Data Protection law are as follows:

- ✓ Justify the purpose
- ✓ Only use personal confidential data if it is absolutely necessary
- ✓ Only use the minimum necessary personal confidential data
- ✓ Access to personal confidential data should be on a need-to-know basis only
- ✓ Ensure that everyone with access to personal confidential data is aware of their responsibilities
- ✓ Comply with the law
- ✓ The duty to share information can be as important as the duty to protect patient confidentiality

The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014

The 2014 Regulations established the 'Fundamental Standards' that are the expected standards that care organisations must meet. It is also a fundamental standard that Duty of Candour is given by providers to be open and transparent with individuals and their representatives when mistakes happen regarding their care.

The Health and Social Care (Safety and Quality) Act 2015

This Act sets out a number of provisions relating to the health and social care services in England. It covers the integration of information relating to users of health and social services. It also explains the sharing of information for individuals who use health and social care services.

Common Law Duty of Confidentiality

The Common Law has not been determined by acts of parliament, but rather developed through the courts making decisions in cases on legal points and creating binding precedents. Essentially the

common law states that anyone who receives confidential information must not disclose it without consent or justification, irrelevant of age, mental health or capacity.

Public Interest Disclosure Act 1998

This Act protects workers who disclose information about malpractice including abuse at their current or previous workplace. It promotes the human right to be protected from abuse or harm by ensuring workers can report their suspicions or allegations of abuse free from fear or repercussion from their employers.

Appendix 2

INFORMATION SHARING CONSENT FORM

Information sharing is an essential aspect of partnership working, to provide safe care, treatment and support, in line with confidentiality and data protection legislations.

Your information is confidential and will not be disclosed or used by Hand in Hands or any member of staff for any other purpose than organising or providing care and/or support to the person named below.

Hand in Hands will only share this information where it is necessary to organise and deliver care or support services or when we are legally obliged to do so. When we do share, we ensure that whomever we share information with will treat it with the same level of confidentiality that our own staff do.

Hand in Hands will only share this information when the reason for doing so has been explained to the person to whom the information relates – or a person representing that person and you agree to allow this.

Permission

I understand that I will be giving my information to Hand in Hands for the purpose of my care and support.

I understand that my information will be processed safely and securely in accordance with the Data Protection Act 2018 and the General Data Protection Act 2018.

I understand that Hand in Hands will at times need to share relevant information about me with other professionals in other organisations/agencies, such as health services, to ensure I receive the level of care and support I need.

I understand that if there are any concerns about my health, safety and wellbeing, that these concerns may need to be shared with other appropriate professionals such as, local authorities in line with Hand in Hands duty of care responsibilities towards me.

I understand that my information will only be shared to relevant professionals and only when necessary to do so. I understand that my information will not be shared for marketing or other commercial purposes.

I understand that my information will not be shared with any relative or friend without my knowledge or prior agreement.

I understand that I can withdraw my consent for my information to be shared at any time and my rights outlined within data protection legislation have been explained to me.

I understand that if I do not provide my consent for information to be shared about me, that this may make it difficult to arrange the care and support that I need.

Please complete and sign the below boxes to indicate that you are willing to allow Hand in Hands to share the personal information it holds about you.

This consent form will be reviewed during your care plan review meetings, unless your consent is withdrawn before this date.

individual Full Name:	
individual Address:	
individual Contact Number:	
Signature:	
Date:	

Representative/NOK Full Name:	
Representative/NOK Relationship to individual:	
Representative/NOK Contact Number:	
Signature:	
Date:	

Name and position of person seeking the information (e.g. Registered Care Manager)	
Signature:	
Date:	

Additional information/requests
Please detail any specific information or requests that are relevant to the sharing of information. For example, details of any person/ organisation that consent to share information with has not been given.

Appendix 3

SUBJECT ACCESS REQUEST FORM

This form is to assist you in making a request for personal data that Hand in Hands hold about you. You are entitled to receive this information under data protection legislation.

You are not obliged to complete this form to make your request, however by doing so this will make it easier for Hand in Hands to process your request quickly.

The information that you provide within this form will only be used for the purpose of identifying the personal data you are requesting and to respond to your request.

PART A - Personal Information	
Full Name:	
Address:	
Telephone number:	
Email:	
What is the nature of your relationship with Hand in Hands?	*(i.e. 'service user' or employee etc.)*

PART B - Are you the Data Subject?	
YES	If you are the data subject please supply evidence of your identity e.g. birth certificate, driving licence or passport. *(Please fill in parts D to E)*
NO	Are you acting on behalf of the data subject with their written authority? If so that authority must be enclosed. *(Please fill in part C to E)*

PART C - Please outline your relationship with the data subject that leads you to make this request for information on their behalf?

PART D - Please describe the information you seek together with any other relevant information. This will help identify the information you require.

PART E - Declaration	
I _____ certify, that the information given on this application form to Hand in Hands is true. I understand that it is necessary for Hand in Hands to confirm my/the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct information.	
Signature:	
Date:	

Office use only	
Date received:	
Received by:	
Signature:	
Date completed:	