Heritage Care at Home Ltd
Confidentiality and Information Policy
Policy reviewed and valid from: 01/01/20

Policy Statement:
Heritage Care at Home Ltd aims to maintain as confidential all sensitive personal information it stores, disclosing lawfully or within the Confidentiality Code of Practice and sharing lawfully or within the Public Sector Data Sharing guidance. Customers, staff and the public put their trust in this organisation to ensure and maintain the confidentiality of information within our systems and that it is shared appropriately.

Scope
This policy applies to

- all staff employed by Heritage Care at Home Ltd
- all third party to include Social Services, PCT staff

This policy and any sub policies complete a comprehensive map of all the elements which working together will ensure the confidentiality and appropriate sharing of personal information

Whilst this policy is comprehensive Heritage care at Home Ltd will continually seek to improve its practice. Any updated or new documents will be distributed to the workforce as appropriate.

Heritage Care at Home Ltd is committed to the delivery of a first class confidential service. This means ensuring that all customer information is processed fairly, lawfully and as transparently as possible so that Customers and staff:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information;
- gain trust in the way the company handles information and;
- understand their rights to access information held about them.

Legal and ethical obligations of confidentiality

1. Justify the purpose(s). Every proposed use or transfer of person-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
2. Don't use person-identifiable information unless it is absolutely necessary. Person-identifiable information items should not be used unless there is no alternative.
3. Use the minimum necessary person-identifiable information where use of person-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification.
4. Access to person-identifiable information. Only those individuals who need access to person-identifiable information should have access to it, and they should only have access to the information items that they need to see.
5. Everyone should be aware of their responsibilities. Action should be taken to ensure that those handling Customer identifiable information are aware of their responsibilities and obligations to respect confidentiality.
6. Understand and comply with the law. Every use of person-identifiable information must be lawful. The Manager is responsible for ensuring that the organisation complies with legal requirements.
7. Information provided in confidence should not be used or disclosed in a form that might identify a Customer or member of staff without his or her consent.

Staff
This section describes individual responsibility of people working for the organisation, this includes all staff. Confidentiality protocol will be included in Contracts of Employment, Staff Handbook & Whistle Blowing.

Personal Details
You are not to disclose any of your personal details including full name, phone number, address or email to any of our customers due to confidentiality and data protection purposes. This is for your own protection and to keep your information confidential at all times.

Duty of Confidence
As staff employed by Heritage care at Home Ltd, you have a legal duty of confidence to Customers and breaching that confidence can be a serious disciplinary Offence. You must not whilst you are employed or after your employment ends, disclose to any unauthorised person information concerning the Company's business or the Customers in its care, nor must you make a copy, abstract, summary or précis of the whole or part of a document relating to Heritage Care at Home Ltd.

Whistle blowing
Heritage Care at Home Ltd's policy on concerns at work about Customer care or matters of business probity/conduct. As a member of staff you may be worried about raising such issues or may want to keep the concerns to yourself, perhaps feeling it's none of your business or that it's only a suspicion. Issues raised under this policy will, wherever possible, be dealt with as per policy guidance and in a way that produces speedy and effective outcomes, which minimise the risk of any breach of confidentiality.

Induction
All new staff will receive a presentation at formal Induction with all necessary information. Staff are issued with their identity badges and must wear them at all times within their working hours.

Mandatory / Specialist Training
To maintain awareness of confidentiality and data sharing all staff will receive or be able to access updates to any confidentiality or sharing procedure, guidance or leaflet.

Access to Information Systems
No one should seek unauthorised access to any staff or Customer information system. When staff leave, for whatever reason access to sensitive personal information should cease, in some cases, immediately.

Staff access to their own records
Staff are entitled to access their own records. In some circumstances, responding to a request from a member or ex-member of staff may involve providing information relating to another individual who can be identified from that information ("third party information"). This can give rise to conflict between the data subject's right of access and the third party's right to respect for his or her private life. Third party information should be removed or made anonymous

Non Permanent Staff
This may be a contractor who also must protect personal data in accordance with the provisions and principles of the Data Protection Act 1998 and in particular the contractor must ensure compliance with the Company's security arrangements and ensure the reliability of its staff who have access to any personal data held by Heritage Care at Home Ltd. In addition, if the contractor is required to access or process personal data held by the company, the contractor shall keep all such personal data secure at all times and shall only process such data in accordance with instructions received from Heritage Care at Home Ltd

User Responsibility
The information users' responsibility is to:

- Understand this policy
- Know where to go for further information
- When in doubt seek help
- Record all unusual disclosures
- Ensure staff know if they follow the policy they will be supported

Information Security Policy
This sub policy must be understood as it details the legislative framework for securing confidential information and that only by appropriate reporting of incidents involving loss or breach of confidentiality can Heritage Care at Home Ltd maintain its high standards for ensuring safety and security of our information.

Customers
Information on entry - It is extremely important that Customers are made aware of information disclosures that must take place in order to provide them with high quality care. Similarly, whilst Customers may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not be the case and the efforts made to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-Heritage Care at Home Ltd bodies. Many current uses of confidential customer information do not contribute to or support the healthcare that a Customer receives. Very often, these other uses are extremely important and provide benefits to society – e.g. medical research, protecting the health of the public, health service and Social Care financial audit. However, we cannot assume that those Customers are content for their information to be used in these ways.

Accuracy checking at key events e.g. review and status change, ensuring confidentiality and preserve the trust placed with us as well as minimising complaints in our processing is the accuracy of our data. The Effective Care Coordination teams and the Information Services work through operational use and validation to maintain accuracy. All known errors are rectified.

Copying Correspondence
Confidentiality is paramount in operating this policy by incorporating the necessary safeguards from abuse either by falling into the wrong hands or delivered to the wrong place. Mental health professionals have been providing copies of effective care coordination documentation to Customers and carers for many years. This documentation normally includes assessment of need, the care pathway, contingency plans and risk assessments.

Customer access to their information
We need to respect the privacy of other people stored in Customer records. For health and social care records we must meet a second requirement i.e. a responsible care professional must ensure the record does not include anything that 'would be likely to cause serious harm to his or any other person's physical or mental health or condition'.

Sharing information for Health and Social Care purposes
This most commonly used and familiar model describes most of our day to day actions, describing generally consenting business of sharing within our caring community and describes disclosures to other staff involved in the provision of healthcare, to social workers or other staff of non-NHS agencies involved in the provision of healthcare, to parents and guardians and to carers.
This model also covers clinical audit. The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services is an essential component of modern health/ social care provision.

Exceptions
If the public good served by a disclosure is significant, there may be grounds for disclosure. The key principle to apply here is that of proportionality. The Data Protection Act 1998 allows for disclosure without the consent of the subject in certain conditions, including for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, and where failure to disclose would be likely to prejudice those objectives in a particular case. Disclosure should be justifiable in each case, according to the particular facts of the case, and legal advice should be sought in cases of doubt. Disclosure should be appropriate for the purpose and only to the extent necessary to achieve that purpose.

Risk of Harm
Disclosures to prevent serious harm or abuse also warrant breach of confidence. The risk of child abuse or neglect, assault, a traffic accident or the spread of an infectious disease are perhaps the most common that staff may face. However, consideration of harm should also inform decisions about disclosure in relation to crime.

Vulnerable adults
Recognition of suspected or actual abuse to vulnerable adults is the responsibility of all staff within Heritage Care at Home Ltd. When considering whether to disclose information to a third party, it will be necessary to identify the circumstances in which the practice of respecting confidentiality should be overridden in order to protect a vulnerable adult.

Examples of this may either be where a vulnerable adult is being intimidated or where there is concern about the risk to another vulnerable adult. The Protection of Vulnerable Adults Scheme (POVA) came into force in July 2004. At the heart of the scheme is the POVA list. Care Assistants are referred to the list if they have harmed, or put at risk of harm, a vulnerable adult in their care. In short, POVA is a workforce ban that will be one means of ensuring that known abusers who have abused or mistreated vulnerable adults in their care do not remain in the workforce or find their way back into such positions again.

Information sharing & using
This policy will enable Heritage Care at Home Ltd, its staff members and Customers to understand that data sharing can take place in a way that helps deliver a better service, while still respecting

people's legitimate expectations about the privacy and confidentiality of their personal information. Where personal accountability to a code of conduct does not apply then staff should be aware that complete confidentiality couldn't be offered to an individual.

Information given to an individual member of staff belongs to the company and not to the staff member alone and should be shared on a 'need to know' basis with other company colleagues, for example, with a line manager. It will always be difficult to make decisions about whether to share (or not to share) information about risk, particularly where the issue is about disclosing to individuals. It will always be crucial to gather the best information possible about the risk posed, assess the risk and consult thoroughly before reaching a decision.

Lawful sharing of information
Information sharing takes place in most of our work. If the following conditions apply sharing is lawful:

1. If the data collection and sharing is to take place with the consent of the Customer involved, a person's private life, family life, home and correspondence. This is the essence outlined in this policy. The Mental Health Act and is in pursuit of a legitimate aim. So for our purpose we can share information.
2. Again if the data collection and sharing is to take place with the consent of the Customers involved, the information will not be confidential and we can proceed.

Meetings Protocol
From Effective Care Coordination to Research Governance and Adverse Incidents, many meeting documents contain personal and perhaps sensitive information. All committees and teams must consider their paperwork and be aware of confidential references. They can work to reduce the amount of confidential material and collect papers, which have served their purpose, at the end of the meeting to reuse or recycle confidentially.

Complaints, Claims & Incidents
This section focuses on activities, which routinely access, record and report sensitive information. Inappropriate use of privileges is often found to be a major contributory factor to the failure of systems that have been breached. In noting this, the information security management code of practice raises two objectives:

1. To ensure that access rights are appropriately authorized, allocated and maintained, and
2. To prevent unauthorized access to information. Customers and staff rightly expect high levels of control in these areas. Privileged access brings responsibility and consideration of the risks in the long term. The over use of personal and sensitive information in our reports brings less control and a greater risk of breach, especially if the report is shared across a wide distribution. Therefore, information usage must be scrutinized for justification, on a need to-use, need-to-know and event by-event basis, i.e. the minimum requirement only.

The only other rule is to be clear about identifying an individual. This will vary across the range of reports but if an individual's identity is necessary for the report then it is justified. If the information is used for a different purpose or different audience then the justification ceases and anonymity must be established. To satisfy the code's requirements, the managers of these services have a responsibility to ensure those staff with privileges or reporting responsibilities follow this policy and associated guidance.