Title of Policy:	**Confidentiality**
Section:	**Operations**

Purpose

This policy outlines and clarifies the obligations of Carers Choices towards the protection of Clients confidential information in line with the Data Protection Act 2018 and relevant features of the General Data Protection Regulation 2018. To also outline the principles relating to confidentiality and to support staff in understanding and applying this principle with the policy guidance.

Statement

It is the policy of Carers Choices that we will only share information that is in the best interest of the Client and with their consent, unless on occasions when it could be detrimental to the individual's wellbeing. Carers Choices understands and accepts its legal, moral and ethical duty to protect information which is confidential to its Clients, employees and all others with whom it comes into contact during the course of its operations. Everyone employed within Carers Choices is under a strict obligation to adhere to the practices and principles outlined within this policy statement. Any breaches will be dealt with under Carers Choices' disciplinary policy.

Procedure and Guidance

Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number, National Insurance

number etc. Even a visual image (e.g., photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive/confidential personal information refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Confidential information within a healthcare environment is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including employee records, occupational health records, etc. It also includes confidential business information.

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g., financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.

All employees working in Carers Choices are bound by a legal duty of confidence to protect personal and/or confidential information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence, the Data Protection Act 2018 and relevant features of the General Data Protection Regulation.

Responsibilities of the Registered Manager

- To Ensure safe systems and processes are in place for the security of information and records.
- To ensure all staff have received the appropriate training and understand confidentiality and the policy guidance.
- Act on any breaches of confidentiality and notifying the relevant people.
- To understand their Duty of Candour obligations

Governing Principles

Carers Choices will operate under the following governing principles, each of which must be strictly adhered to:

- All staff must sign a confidentiality agreement as part of their contract of employment. The confidentiality agreement also extends to agency and contractual workers.
- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted, or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information, such as clarification as to when, how and if information is to be shared, or concerns that the policy is not being adhered to must be reported to either the employee's line manager, or, if this is not appropriate under the circumstances, to a more senior manager within Carers Choices.
- Carers Choices is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

- Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.
- Access to rooms and offices where terminals are present, or person identifiable or confidential information is stored must be controlled.
- All administrative office staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.
- Unwanted printouts containing person-identifiable or confidential information must be disposed of in a safe manner.
- Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.
- Breaches of confidentiality could be liable and result in prosecution.

Disclosing Personal/Confidential Information

In general, no information may be disclosed either verbally or in writing to other persons without the Client's consent. This includes family, friends and private carers, and other professionals.
Every effort will be made to ensure that Clients understand how information about them will be used before they supply any confidential information, and their consent is given to the disclosure. That Clients also understand when information about them is likely to be disclosed to others, and that they have the opportunity to withhold their permission if they so wish.

If disclosing information outside Carers Choices, could have personal consequences for the Client, that consent is obtained and the individual understands what will be disclosed, the reasons for disclosure and the likely consequence of the information being shared with others. If the Client withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:

- They can be justified in the public interest (usually where disclosure is essential to protect the Client or someone else from the risk of significant harm)
- They are required by law or by order of a court.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed. Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioners Anonymisation Code of Practice.
- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager before disclosing.
- In Child Protection proceedings if it is considered that the information required is in the public or child's interest.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime.
- When disclosing confidential information, staff must be prepared to explain and justify the decision. Where there are doubts, they will discuss them with the Manager.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. Taking home/removing paper documents that contain person-identifiable or confidential information from Company premises is discouraged and always kept to a minimum.

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations. If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc.

- Confidential information is kept out of sight whilst being transported.

If staff do need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be

able to see the content or have any access to the information. Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person-identifiable or confidential information on a privately owned computer or device.

Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally.

Staff may be held personally liable for a breach of confidence and must:

- Not talk about person-identifiable or confidential information in public places or where they can be overheard.
- Not leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents,
- Not share passwords or leave them lying around for others to see.
- Not leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed unattended.
- Switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Not make comments to the press or other media. Media enquiries should be referred to the person responsible for handling any media enquiries within Carers Choices.

Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on computers. Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access computer data, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal.

Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information relating to their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 2018.

CQC Registration and Inspection Compliance

Key Questions and Quality Statements applicable to this Policy	Care Quality Commission (Registration) Regulations 2009 applicable to this Policy
Caring • Kindness, Compassion and Dignity	

Legislative Compliance

Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 applicable to this Policy	Other legislation relevant to this Policy
Regulation 9: Person-centred care Regulation 10: Dignity and Respect	Data Protection Act 2018

Policy Reviewed on Date of Implementation by the Following Company Officer:

Full name:

Paul Ramsden

Job Title:

CEO

Signature:

P. Ramsden

Annex 1 - The Legal Framework

The Organisation will comply with the following legislation and guidance as appropriate:

The Data Protection Act (2018) regulates the use of "personal data" and sets out six principles to ensure that personal data is:

1. Processed fairly and lawfully.
2. Processed for specified, explicit and legitimate purposes.
3. Adequate, relevant and not excessive.
4. Accurate and where necessary kept up to date.
5. Not kept longer than necessary, for the purpose(s) it is used.
6. Processed in a manner that ensures appropriate security.

The Caldicott Report (1997) recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis.
- Comply with the law.
- Everyone should be aware of their responsibilities.
- The duty to share information can be as important as the duty to protect patient confidentiality.
- Inform the Client how their information will be used.

The Organisation will identify a Caldicott champion who will ensure the Caldicott principles are adhered to as follows.

Article 8 of the Human Rights Act (1998) refers to an individual's "right to respect for their private and family life, for their home and for their correspondence".

The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation. a. Making, supplying, or obtaining articles for use in offences 1-3

Common Law Duty of Confidentiality Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.