Policy and Procedure on Confidentiality

Purpose

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all staff or volunteers who work for CareTech (and the companies owned by it – now referred to as 'The Company') and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

The Company is committed to all aspects of data protection and takes seriously its duties, and the duties of its Employees, under GDPR and Data Protection Act 2018.

In addition, the common law duty of confidence, and the data subjects' rights within the Human Rights Act 1998, Article 8 ECHR, places obligations on us as an employer when responding to requests for information and our responsibilities towards our staff.

This policy sets out how the Company deals with personal data, including personnel files and data subject access requests, and Employees' obligations in relation to personal data.

Scope

All Employees, irrespective of their role within the organisation, are held by the contents of this policy and are required to follow and uphold the values, principals and expected behaviours of The Company when carrying out their duties and responsibilities.

Policy Statement

Any breach of confidentiality, inappropriate use of health or staff records, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported.

Data Protection Principles

All employees are bound by a legal duty of confidence to protect personal 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 and the Data Protection Act 2018. Please refer to The Company Data Protection Policy.

Sensitive Personal Data

'Sensitive personal data' is information about an individual 's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);

• physical or mental health or condition;

• sex life;

• commission or alleged commission of any criminal offence; and 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.

Procedure

The Company will not retain sensitive personal data without the express consent of the Employee in question. The Company will process sensitive personal data, examples of which include:

- Sickness and injury records
- Management investigations
- Safeguarding investigations which may contain details of alleged or actual criminal activity
- References
- Disciplinary records,
- Supervision documents
- Recruitment documentation
- Changes in employment details
- Pay records, in accordance with the seven data protection principles.
- Biometric data

If The Company enters into discussions about a merger or acquisition with a third party, The Company will seek to protect Employees' data in accordance with the data protection principles.

All requests for information should be forwarded to The Company Data Protection Officer. The Compliance and Regulation team will assist. A Request for Information application is available on Rezume (Your Social Care Records and How to Access Them)

Consequences of Non-Compliance

All Employees are under an obligation to ensure that they have regard to the data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an Employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an Employee accesses another Employee's employment records without the requisite authority, The Company will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

The Data Protection Act 2018 requires that six data protection principles be followed in the handling of personal data. These principles require that personal data must:

1. be fairly and lawfully processed and in a transparent manner; The Company will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. be processed for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes; The Company will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3.be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; The Company will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4.be accurate and kept up to date; The Company will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify The Company if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of The Company to ensure that any notification regarding the change is noted and acted on.

5. kept for no longer than is necessary, The Company undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means The Company will undertake a regular review of the information held and implement a data cleansing process. The Company will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g., secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage The Company recognises that Individuals have various rights under the legislation including a right to:

- be told the nature of the information The Company holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision-making process that will significantly affect them.

• not have significant decisions that will affect them taken solely by automated process. • sue for compensation if they suffer damage by any contravention of the legislation.

• take action to rectify, block, erase or destroy inaccurate data.

• request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

All staff must ensure that the following guidance is adhered to:

• 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.

• 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 must be discussed with either your Line Manager or your HR Business Partner

• 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. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

• All 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 put into a confidential waste bin. Discs, tapes and printouts must not be left lying around but be filed and locked away when not in use.

• No personal information should be kept on USB or similar devices without specific permission from a Director. Any USB used for the storage or transport of information must be encrypted.

• Telephone calls and discussion should be held in private where the information discussed pertains to the personal details or circumstances of service users or staff.

• Staff should not discuss the personal details or circumstances of staff or service users in the presence of people who have no “need to know”. This includes other staff, visitors and service users.

• Your Contract of Employment includes a commitment to confidentiality.

Disclosing Confidential Information

• To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

• 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.

• When the information is required by law or under a court order. In this situation staff must discuss with their Line manager or Human Resources staff before disclosing, who will inform and obtain approval of the Data Protection Officer.

• When there is a requirement to access staff files. In this situation staff must obtain the approval of the Data Protection Officer. Access will only be granted to authorised staff for a specific period regarding business-critical data.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. Staff must be careful of being overheard on the telephone or communicating sensitive information at all times whether in the office or care setting.

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. Please see Data Protection policy.

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.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not store any sensitive information on their own computers or devices.

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. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

The Company will provide training to all Employees on data protection and confidentiality matters on induction and on a regular basis thereafter. If an Employee considers that he/she would benefit from refresher training, he/she should contact their Line Manager in the first instance.

8 Document Change Control

Date of review: October 2025

Date of review: July 2023

Date of review: July 2021

Date of review: May 2019

Date of review: April 2017

Date of release: November 2015

Monitoring and Review

The Company will undertake a formal review of this policy if there are any changes to procedure, legislation or regulations

Signed *Russell Edge* Russell Edge

Senior Information Risk Owner (SIRO) & Data Protection Officer
October 2025

This policy must be read in conjunction with the following policies:

- The Data Governance Strategy
- Appendix 1 The Data Governance Roadmap
- Information Security
- Risk Management
- Records Management
- Information Systems Acceptable Use
- Access to Records
- Confidentiality Code of Practice
- Processing of Special Category Data and Criminal Offence Data
- Remote Working Policy
- Data Protection Impact Assessments