Comfort Care Recruitment and Training Ltd.

Data Protection
Policy and Procedure

APRIL 2026

ISSUED DATE:	AUTHORISED BY:	DATE OF NEXT REVIEW:
14/04/2026	BENSON OZOUR	14/04/2027

Data Protection Policy and Procedure

Purpose of Policy

This Data Protection Policy outlines Comfort Care Recruitment and Training Limited's policy on how we will process and maintain the security of information relating to clients, employees and stakeholders.

To meet the legal requirements of the following legislation:

- Freedom of Information Act 2000
- The Care Act 2014
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- The Health and Social Care (Safety and Quality) Act 2015
- General Data Protection Regulation 2016
- Data Protection Act 2018

To meet the following guidance:

- The Caldicott Principles https://www.gov.uk/government/publications/the-caldicott-principles

Scope

The policy applies to:

- All employees, including those designated as temporary, bank staff, agency staff, volunteers or work experience
- Contractors
- Stakeholders

Objectives

The objectives of this policy are:

- To meet legislative requirements
- To meet regulatory requirements
- To comply with the Caldicott Principles

ISSUED DATE:	AUTHORISED BY:	DATE OF NEXT REVIEW:
14/04/2026	BENSON OZOUR	14/04/2027

- To ensure personal information is kept confidential and secure
- To ensure that clients and stakeholders are aware of our responsibilities relating to Data Protection
- To ensure that employees understand their responsibilities relating to Data Protection
- To ensure accountability
- To provide a process for managers in the event of a Data Protection breach

Policy Statement

Comfort Care Recruitment and Training Limited recognises our legal responsibilities in relation to the collection, processing and storing of personal data in order to carry out our business functions. Comfort Care Recruitment and Training Limited is committed to the compliant processing of personal data.

Comfort Care Recruitment and Training Limited understands personal data to be any information relating to an identified person who can be identified directly or indirectly from the data held by reference to an identifier such as name, an identification number, location data or online identifier. Data includes digital information and paper information.

Comfort Care Recruitment and Training Limited recognises the rights of people to have their personal information secured and kept confidential.

Comfort Care Recruitment and Training Limited is committed to complying with our legal responsibilities to ensure:

- Personal data is processed lawfully, fairly and transparently
- Personal data is only collected for specified and legitimate purposes
- Personal data is adequate, relevant and limited to what is essential to the purpose of processing the information
- Personal data is accurate and kept up to date
- Personal data is only kept as long as necessary
- Personal data is processed securely

Comfort Care Recruitment and Training Limited is committed to complying with the data rights of the General Data Protection Regulation:

- Right to be informed
- Right of access

- Right to rectification
- Right to erasure/to be forgotten
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Comfort Care Recruitment and Training Limited will comply with the Caldicott Principles for Health and Social Care:

- Principle 1: Justify the purpose(s) for using confidential information
- Principle 2: Use confidential information only when it is necessary
- Principle 3: Use the minimum necessary confidential information
- Principle 4: Access to confidential information should be on a strict need-to-know basis
- Principle 5: Everyone with access to confidential information should be aware of their responsibilities
- Principle 6: Comply with the law
- Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality
- Principle 8: Inform service users about how their confidential information is used

Comfort Care Recruitment and Training Limited will ensure that our clients, employees and stakeholders are informed of how their information will be processed and secured and we will ask consent to share information if there is a legitimate reason to do this.

Comfort Care Recruitment and Training Limited will ensure that all employees complete Data Protection training.

Comfort Care Recruitment and Training Limited will investigate all incidents of breaches of Data Protection. Breaches of Data Protection may result in disciplinary action being taken in accordance with Comfort Care Recruitment and Training Limited's Disciplinary Policy and Procedure.

The Registered Manager is responsible for Data Protection within Comfort Care Recruitment and Training Limited.

Comfort Care Recruitment and Training Limited is committed to implementing this Policy and the practices it sets out.

Procedure

Client Information

All clients must be given information about how their personal information will be used by Comfort Care Recruitment and Training Limited.

Clients must be informed how their information will be processed, stored and shared.

Clients must be asked to consent to the sharing of their personal information.

The Registered Manager is responsible for ensuring that all clients are provided with this information.

Maintaining Data Protection and Security

Employees must always work within the requirements of the Data Protection Act, General Data Protection Regulation and the Caldicott Principles.

Employees must follow the instruction and guidance provided in Data Protection training.

Employees must only access the information they need to carry out their role.

Employees must ensure that they use passwords on electronic systems and ensure that other people do not see their screens.

Employees must lock their computer screens when they leave the computer unattended.

Employees must not share passwords with any other person.

Employees must not leave personal data where it can be viewed by others.

Employees must not take personal data home with them.

Employees must not discuss clients, employees or stakeholders with others including employee's family members.

Employees must make telephone calls in private and ensure they are not overheard by others.

Employees must not dispose of written information containing personal data and confidential information in general waste bins or recycling. The Registered Manager must make arrangements for the secure shredding of confidential written information.

Employees must comply with Comfort Care Recruitment and Training Limited's Social Media Policy and Procedure when using business and personal social media.

Subject Access Requests

All individuals are entitled to see the information held about them by Comfort Care Recruitment and Training Limited. This includes clients, employees and stakeholders. Individuals can submit a Subject Access Request (SAR) to Comfort Care Recruitment and Training Limited to request a copy of the information held about them. A Subject Access Request can be made verbally or in writing.

If a client or stakeholder requests access to their personal information the employee receiving the request must inform the Registered Manager as soon as possible.

Employees can make Subject Access Requests to the Registered Manager.

The Registered Manager must manage the request in accordance with data protection and GDPR regulations and must respond within one month of the receipt of the request.

Third Party Requests for Information

If an employee is asked for information by a third party such as the Police, Local Authority or other professional, they must respectfully decline the request and explain that they will need to pass the request on to the Registered Manager.

The Registered Manager must manage the request in accordance with data protection regulations. Information will normally only be shared with a client's consent unless sharing information is essential for the safety and wellbeing of a client or others.

If information is shared the Registered Manager must ensure that:

- Information is necessary for the purpose
- Information is only shared with the people who need to have access to it
- Information is shared securely
- A record of the decision to share is made

Employee Confidentiality Agreements

All employees must sign a Confidentiality Agreement when they commence employment with Comfort Care Recruitment and Training Limited.

If an employee breaches the Confidentiality Agreement the Registered Manager must take action in accordance with Comfort Care Recruitment and Training Limited's Disciplinary Policy and Procedure.

Employees Leaving or Absent

The Registered Manager must remove access to all electronic data systems for employees who are on long term absence.

If an employee is suspended from their employment at Comfort Care Recruitment and Training Limited their access to electronic systems must be removed immediately.

If an employee is ending their employment with Comfort Care Recruitment and Training Limited the Registered Manager must ensure that access to electronic systems is removed on their last working day.

If employees have access to electronic communication forums such as WhatsApp groups the access to these must be removed if any of the above situations apply.

If employees have keys to premises these must also be returned if any of the above situations apply.

Breaches of Data Protection

Employees must report all concerns of data protection breaches, or near misses, to the Registered Manager as soon as possible.

If it is suspected that a breach of data protection has occurred, the Registered Manager must ensure that an investigation is completed and action is taken to manage the incident.

The Registered Manager must inform the Nominated Individual of the breach.

The Registered must inform all the people that are affected by the breach.

The Registered Manager must report the breach to the Information Commissioner's Office (ICO).

The Registered Manager must identify lessons learned from the incident and implement any actions identified to reduce the risk of further incidents.

The Registered Manager must maintain a log of all data protection breaches.

Breaches of data protection by employees must be managed in accordance with Comfort Care Recruitment and Training Limited's Disciplinary Policy and Procedure.

The Nominated Individual must assess the risks to the business from the breach and must update the Business Continuity Plan if necessary.

Employee Training

As part of the induction process employees will be given training in Data Protection.

Employees will be required to attend refresher training.

The Registered Manager is responsible for ensuring that Data Protection is covered during induction and ensuring that all employees are up to date with training.

Roles and Responsibilities

All employees are responsible for:

- Following the Data Protection Policy and Procedure.
- Ensuring personal data is processed and secured in accordance with the Data Protection principles.
- Informing the Registered Manager of breaches of Data Protection, or any near misses.

- Informing the Registered Manager of any Subject Access Requests or requests for information from third parties.
- Attending training relating to Data Protection.

The Registered Manager is responsible for:

- Ensuring this Data Protection Policy and Procedure is implemented.
- Ensuring that new employees are made aware of Data Protection during their induction.
- Ensuring employees are provided with Data Protection refresher training.
- Managing Subject Access Requests.
- Ensuring that all breaches of Data Protection are investigated and managed.
- Reporting Data Protection breaches to the Information Commissioner's Office (ICO).
- Informing the Nominated Individual of all breaches of Data Protection.

The Provider/Nominated Individual is responsible for:

- Supporting the Registered Manager to manage Data Protection breaches.
- Assessing and managing risks to the business from breaches.
- Ensuring the Business Continuity Plan is updated.

Breaches of Policy

For employees, failure to adhere to the Data Protection Policy and Procedure could lead to possible disciplinary action being taken.

For others (volunteers, agency staff, contractors) their individual relationship with the organisation may be terminated.

Monitoring and Review

This Policy will be reviewed annually or sooner if necessary due to legislative or regulatory requirements.