

Policy Statement

This policy outlines TruComfort Homecare's commitment to safeguarding the confidentiality and privacy of information concerning service users, employees and operations. It is for all staff, managers and any service users who may be concerned about how their personal information is handled.

We are fully committed to protecting sensitive information in line with legal obligations and ethical standards, while ensuring transparency and trust throughout our services.

Legal Framework

TruComfort Homecare adheres to the principles set in the **UK General Data Protection Regulation (GDPR) & Data Protection Act 2018** as well as the **Freedom of Information Act 2000**. These laws govern the lawful handling, storage and sharing of personal data.

All personal data held by TruComfort must be:

- Collected and used fairly and lawfully
- Stored only for specific, clear purposes
- Relevant and limited to what is necessary
- Accurate and regularly updated
- Retained only for as long as needed
- Protected against unauthorised access or misuse
- Processed in line with individuals' rights
- Not transferred outside the UK or EEA unless adequate data protection is in place

TruComfort Homecare is registered as a data controller and the **Registered Manager** is responsible for data protection compliance across the organisation.

Confidential Information and Storage

Some confidential data may be accessed by staff beyond the individual care worker. To manage this responsibly we ensure the following measures:

1. **Lockable filing systems** are used for physical records.
2. **Digital records** are password-protected and accessible only by authorised personnel.
3. **Office equipment** such as screens and printers is positioned to prevent unauthorised viewing of personal information.

Access to Personal Data

Employees have the right to request access to their own personal information held by TruComfort, the process is as follows:

05/03/2025

- a. Requests must be submitted to the **Registered Manager** acting as the Data Protection Coordinator. In their absence the request may go to the Registered Person.
- b. A standard form must be completed to initiate the request.
- c. If an authorised representative makes the request, confirmation of consent will be required.
- d. TruComfort will respond to access requests **within 10 working days**.
- e. Viewing of documents will occur in the presence of the Registered Manager for security purposes.
- f. Employees should notify the company of any changes that may affect their personal data.
- g. If a dispute arise regarding data accuracy or use, the member of staff are encouraged to use the formal **grievance procedure**.

Exceptions to Confidentiality

In emergency situations, where maintaining confidentiality would pose a serious risk to a service user or another individual, staff may breach confidentiality in **good faith**. Examples include:

- Preventing serious harm and/or danger
- Responding to any safeguarding concerns

In such cases:

- Staff must use professional judgement
- Inform a manager or relevant authority as soon as possible
- Document the reason for the breach appropriately

Training and Staff Responsibilities

All staff will be trained in our confidentiality policies during **induction** period and receive refresher training as per need. Managers are responsible for ensuring staff:

- Understand the implications of data protection laws
- Know how to manage personal data securely
- Feel supported in addressing any challenges related to confidentiality

Supervisors will offer guidance and opportunities in issues related to information handling during ongoing supervision.