SALUTEM INFORMATION GOVERNANCE AND DATA PROTECTION POLICY

Policy implemented:	Aug 2019
Last reviewed:	April 2025
Next review due:	April 2026

At Salutem our policies are regularly updated and reviewed. However, occasionally policies may be reviewed after the set next review date after some consultation and research. In these rare occasions, the out-of-date policy will remain **VALID** until it is reviewed by the policy sponsor.

1. Summary

This policy outlines how Salutem Care & Education protects, manages, and uses personal and sensitive information in accordance with UK GDPR, the Data Protection Act 2018, and relevant health and social care guidance. It applies to all staff, contractors, and partners across complex care and mental health services.

Purpose

To ensure lawful, fair, and transparent data processing; protect the rights of service users and staff; and support compliance with the Data Security and Protection Toolkit (DSPT) and sector-specific standards.

A detailed breakdown of our principles, procedures, and implementation practices can be found in the Information Governance and Data Protection Procedure document.

This policy covers all information assets, including personal, confidential, corporate, and clinical data. It applies to information in all formats (electronic, paper, audio, visual) and systems including eMAR, rostering, and care planning tools.

2. Document Control

Initial purpose and scope of the new policy/procedure agreed by:	Quality Assurance Inspection & Regulation Director
Sponsor Technical review carried out:	Group Head of Regulatory Quality Compliance and Policy (DPO)
Final Information Governance quality check carried out:	Policy, Practice & Information Officer
Date implemented:	April 2025
Version Number:	V 4.1
Date of the next review:	April 2026
Department responsible:	Quality
Job Title of Lead Person:	Group Head of Regulatory Quality Compliance and Policy (DPO)

In addition to this policy, local authorities and other commissioners may have their own policies, procedures and guidance which Services must comply with. These policies should complement this policy.

However, there may be additional requirements put in place by local authorities and other commissioners and these must be adhered to. Changes must not be made to Salutem's policies and procedures without corporate approval but, where needed, local procedures should be developed to accompany these.

EQUALITY AND DIVERSITY STATEMENT

The Salutem Group is committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any such factors and all will be treated with dignity and respect.

3. Contents

This policy must be brought to the attention of all employees.
The controlled version of this policy and its associated documents are available on BLINK. Printed or downloaded copies are uncontrolled and may not be up to date.

4. Definitions

Data Protection

Data protection refers to the practices, policies, and technologies used to safeguard personal and sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. It's about ensuring that data is kept secure and used responsibly.

5. Principles

Legal and Regulatory Framework

This policy ensures compliance with:

- UK GDPR and Data Protection Act 2018

- Common Law Duty of Confidentiality

- Care Quality Commission (CQC) regulations

- NHS Records Management Code of Practice

- DSPT and ICO guidance

Data Protection Principles

We process personal data in accordance with the seven key principles of UK GDPR:

1. Lawfulness, fairness and transparency

2. Purpose limitation

3. Data minimisation

4. Accuracy

5. Storage limitation

6. Integrity and confidentiality (security)

7. Accountability

Individual Rights

Service users and staff have the right to:

- Access their data

- Request rectification or erasure

- Restrict or object to processing

- Data portability (where applicable)

- Raise complaints with the Information Commissioner's Office (ICO)

Data Security and Incident Management

We apply technical and organisational measures to protect data. All incidents, breaches, and near-misses must be reported to the DPO immediately. Significant breaches will be reported to the ICO within 72 hours as required. Notification will be given to individuals where there is a high risk to rights and freedoms.

Records Management

Records are retained in accordance with the NHS Records Management Code of Practice. Data is reviewed and disposed of securely when no longer needed.

Data Sharing and Consent

Information is shared on a lawful basis with consent or other legal justification. Data Sharing Agreements are required for all external sharing.

6. Areas of Governance

This policy has been written with expert contribution from appropriate stakeholders. The Information Governance Team will monitor, reflect on and gain organisational learning from the implementation of this policy. This policy will be reviewed and updated annually from implementation unless legal changes demand a more timely amendment.

The application of this policy and its associated documents is mandatory for all services staff, volunteers, agency staff and all other Salutem representatives. Staff understanding of this policy and associated documents will be assured through training, assessment of competency and supervision.

Staff understanding of this policy will be assured through training and the delivery of awareness raising workshops as deemed necessary by SLT. The people we support will be involved in the review to ensure it captures the important issues for them.

7. Areas of Responsibility

Senior Information Risk Owner (SIRO):

Oversees information risk at board level.

Caldicott Guardian:

Ensures appropriate access and confidentiality of individuals information.

Data Protection Officer (DPO):

Provides independent oversight and advice required under the UK GDPR and Data Protection Act 2018

Group Head of IT

Oversee the technical and organizational measures required under the UK GDPR and Data Protection Act 2018

All Staff:

Must complete training, follow procedures, and report incidents.

8. Learning and Development

Salutem is committed to ensuring that all staff are aware of what is expected of them so that everyone is appropriately supported. Staff should speak to their line manager in relation to their learning needs using supervision and through the appraisal process.

All staff must complete annual IG and data protection training. Role-specific training is provided for high-risk functions, including clinical staff using eMAR systems.

9. Associated Documents

Quality Data Policy

Quality Data Procedure

Salutem Care and Education Information Governance and Data Protection Strategy 2025–2028

10. Version Control

This is a controlled document. As a controlled document, any printed copies of this document, or saved onto local or network drives should be actively monitored to ensure the latest version is always available.

Version Number	Date	Status	Changes
V2.0	Aug 2019	Published	New policy
V3.0	March 2021	Published	Updated information regarding processes
V3.1	March 2022	Published	Updated information regarding UK adequacy
V4	February 2023	Published	SLT role
V4.1	April 2025	Draft	Complete Rewrite