

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

Policy implemented: April 2025

Last reviewed: New

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 In these rare occasions, the out-of-date policy will remain **VALID** until it is reviewed by the policy sponsor.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 strategy outlines our approach to Information Governance (IG) and Data Protection across the Salutem group. It sets out how we will ensure that personal, sensitive, and corporate information is handled securely, legally, efficiently, and effectively to support safe, high-quality care and organisational excellence.

This strategy applies to:

- All staff, contractors, volunteers, and partners.
- All information processed in any format, including electronic, paper, audio, visual, or verbal.
- All systems and processes used to store or manage information across clinical, operational, and corporate functions

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 1.0
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

1. Summary	1
2. Document Control	2
3. Contents	3
4. Definitions	4
5. Strategic Aims.....	4
6. Governance Framework.....	4
7. Strategic Objectives and Key Actions.....	5
8. Legal and Regulatory Compliance	6
9. Risk Management	6
10. Monitoring and Review.....	6
11. Version Control	6

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. Strategic Aims

We are committed to:

- Maintaining the confidentiality, integrity, and availability of all data we hold.
- Ensuring compliance with UK GDPR, Data Protection Act 2018, Caldicott Principles, Freedom of Information Act 2000 (where applicable), and the common law duty of confidentiality.
- Supporting transparency, accountability, and service user trust.
- Enabling digital innovation, secure information sharing, and modernised service delivery.

6. Governance Framework

Senior Leadership and Accountability

- Senior Information Risk Owner (SIRO): Board-level responsibility for information risk management.
- Caldicott Guardian: Oversight of individual user confidentiality.
- Data Protection Officer (DPO): Independent advice, assurance, and oversight of compliance. Day-to-day management of IG compliance and awareness.

Committees and Reporting

- The Senior Leadership Team will oversee strategy implementation and risk management, reporting into the Board.
- Regular internal reporting on compliance, incidents, training, and audits.

7. Strategic Objectives and Key Actions

Objective 1: Strengthen Data Protection Compliance

- Maintain a lawful basis for all processing activities under UK GDPR.
- Conduct Data Protection Impact Assessments (DPIAs) for new or high-risk projects.
- Maintain and regularly review our Record of Processing Activities (ROPA).

Objective 2: Promote a Culture of Accountability and Awareness

- Mandatory annual training for all staff, with specialist training for high-risk roles.
- Clear policies, procedures, and accessible guidance.
- Regular communications and campaigns to reinforce data protection principles.

Objective 3: Enhance Information Security

- Implement and maintain robust technical and organisational controls.
- Cybersecurity aligned with the NHS DSPT and Cyber Essentials standards.
- Regular penetration testing, incident response planning, and business continuity exercises.

Objective 4: Improve Data Quality and Record Management

- Standardise record-keeping practices across services.
- Introduce data quality audits and ownership responsibilities.
- Implement a clear retention schedule based on NHS Records Management Code of Practice.

Objective 5: Facilitate Secure and Lawful Data Sharing

- Ensure all data sharing is transparent, necessary, and proportionate.
- Use Data Sharing Agreements (DSAs) and Data Processing Agreements (DPAs) for third-party processors.
- Participate in regional or national data sharing initiatives with appropriate safeguards.

Objective 6: Embed Privacy by Design and Default

- Include IG and privacy considerations from the outset of all projects.
- Integrate IG into digital transformation, AI, and system procurement.

8. Legal and Regulatory Compliance

This strategy supports our compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Common Law Duty of Confidentiality
- Freedom of Information Act 2000 (where applicable)
- NHS Data Security and Protection Toolkit (DSPT)
- Information Commissioner's Office (ICO) and all regulators (Care Quality Commission (CQC), Ofsted, Estyn, Care Inspector Wales (CIW) expectations

9. Risk Management

- Information risks will be incorporated into corporate and local risk registers.
- Regular reviews and audits of IG compliance and controls.
- Learning from incidents, near-misses, and ICO guidance to inform continuous improvement.

10. Monitoring and Review

- This strategy will be reviewed annually or in response to significant changes in law, regulation, or business operations.
- Progress will be monitored through KPIs such as training compliance, incident rates, and audit outcomes.

11. 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
V1.0	April 2025	Draft	New