TOTAL INFORMATION SECURITY & PROFESSIONAL COMMUNICATIONS POLICY

Policy implemented:	May 2026
Last reviewed:	May 2026 (New Policy)
Next review due:	April 2028

EQUALITY AND DIVERSITY STATEMENT

Salutem Care & Education is committed to the fair and equitable treatment of all individuals in accordance with the Equality Act 2010. An Equality Impact Assessment has been completed for this policy to ensure it can be applied consistently and without discrimination. Salutem Care & Education is committed to safe, high-quality, person-centred services that uphold people's rights and dignity.

All colleagues (including volunteers, agency workers and contractors) must follow this policy, guided by our values. Policies are reviewed every two years; if a review is delayed, the current version remains in force until approved by the Policy Sponsor.

Training will support understanding, and people we support will be involved in reviews. Local procedures may support this policy, but corporate policies must not be changed locally without formal approval.

This policy must be shared with all colleagues. The controlled version is on BLINK; printed/downloaded copies may be out of date.

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

1. Summary

This policy sets out how Salutem Care and Education protects information across **physical, digital and communication environments**. It defines clear expectations for colleagues on:

- Secure working and acceptable use of systems
- Email, messaging, calls and professional communications
- Cyber security controls (devices, access, patching, monitoring)
- Physical security (buildings, keys, visitors, records)
- CCTV/surveillance and recordings
- Use of personal devices (BYOD) and personal mobile phones at locations
- Artificial Intelligence (AI) and emerging risks
- Incident reporting, investigation and learning

This is an overarching policy that replaces legacy policies (e.g., Information Security, Physical Security, Acceptable Use, Email, Personal Devices) and links to specialist procedures for operational detail.

Salutem is committed to maintaining the **confidentiality, integrity and availability** of all information assets and to meeting its legal, regulatory and contractual obligations (including UK GDPR, DPA 2018, ICO guidance and National Data Guardian (NDG) Data Security Standards / DSPT expectations where applicable).

"It also sets out incident reporting requirements, cyber security expectations, monitoring and audit arrangements, and mandatory training requirements, and links to records management, breach management and surveillance procedures.

This policy applies to anyone who accesses Salutem information, systems, sites, devices, or communications channels, including:

- Employees (permanent, fixed-term, bank)
- Agency staff
- Contractors/consultants
- Volunteers, students/placements (where applicable)
- Third parties acting on behalf of Salutem (subject to contract and due diligence)

This policy applies to:

- Paper and electronic records

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- All Salutem systems and business applications (e.g., care/education/HR systems, SharePoint/M365, Nourish, BLINK)
- All devices used for work (Salutem-issued and authorised BYOD)
- All communications undertaken for work purposes (email, Teams, approved platforms, calls, messaging)
- All locations (offices, services, supported living, education sites) and remote working

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

2. Document Control

Policy Sponsor (Name & Role):	Melinda Glover, Quality Assurance Inspection & Regulation Director
Policy Reviewer (Name & Role):	Chris Bell, Improvement and Development Manager (Data Protection Officer)
Approved by (Name/Role):	Melinda Glover, Quality Assurance Inspection & Regulation Director
Date Implemented:	May 2026
Last Reviewed:	New
Next Review Due:	May 2028
Version Number:	V1.0
Controlled Copy Location:	☒ BLINK ☐ Education Policy Hub
Policy category (tick):	☐Safeguarding ☐ Care practice ☐ Education ☐ Other: [ ] ☐ Health & Safety ☐ HR/People ☒ Information Governance
Policy Applies to:	**People we Support** ☒ Children/young people ☒ Adults ☒ Learners ☒ Families/Carers **Workforce** ☒ Permanent ☒ Bank ☒ Agency ☒ Other: [ ] ☒ Volunteers ☒ Contractors

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

3. Contents

1. Summary 2
2. Document Control 4
3. Contents 5
4. Definitions 6
5. Principles 8
6. Information Security Incident & Data Breach Response 9
7. Email and Electronic Communications 11
8. Cyber Security 12
9. CCTV & Surveillance 16
10. Data Security and Safe Working Practices (Homes, Offices & Clear Desk) 16
11. Learning and Development 19
12. Areas of Responsibility 19
13. Monitoring and Compliance 21
14. Associated Documents 21
15. Legal, Regulatory & Standards Framework 21
16. Version Control 22
17. Appendices 23

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

4. Definitions

Key terms used in this policy include (non-exhaustive):

4.1 Salutem Data / Organisational Data: Any information created, received, accessed, stored, shared or otherwise processed in connection with Salutem business. This includes (but is not limited to) personal data and special category data; safeguarding information; care, support and education records; HR and workforce information; financial and operational information; and commercially sensitive or strategic information—whether held in paper, digital, audio, visual, or any other format.

4.2 Personal Data / Special Category Data: Terms with the meanings set out in the **UK GDPR** and the **Data Protection Act 2018**. *Personal data* is information relating to an identified or identifiable living individual. *Special category data* is a subset of personal data that requires additional protection due to its sensitivity (for example, health, disability, ethnicity, religious beliefs, or safeguarding-related information).

4.3 Information Security Incident: Any actual or suspected event that could compromise the **confidentiality, integrity or availability** of Salutem information or systems. Examples include loss or theft of devices or records, misdirected communications, unauthorised access, credential compromise, phishing, malware/ransomware, system outages, or any other event that may result in unauthorised disclosure, alteration, loss, or unavailability of information.

4.4 Data Breach (Personal Data Breach): A type of security incident involving personal data, meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches affecting **confidentiality**, **integrity** and/or **availability** of personal data.

4.5 BYOD (Bring Your Own Device / Personal Device): A privately owned device (e.g., smartphone, tablet, laptop) used to access Salutem systems or data **only where explicitly authorised in writing**, subject to a completed BYOD agreement and the implementation of required security controls (such as encryption, strong authentication, and remote management where applicable).

4.6 MFA (Multi-Factor Authentication): An additional security control that requires users to verify their identity using two or more factors (for example, something they know such as a password, and something they have such as an authenticator app or one-time code), reducing the risk of unauthorised access if a password is compromised.

4.7 EDRM / Records Systems: Salutem-approved electronic document and records management systems (and associated platforms) used to create, store, organise, manage access to, retain,

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

archive and securely dispose of organisational records in line with retention schedules, audit requirements, and legal/regulatory obligations.

4.8 Individual We Support: Any child, young person, adult, or learner who receives care, education, support, or services from Salutem.

4.9 Artificial Intelligence (AI) / Large Language Models (LLMs): Technologies that analyse, generate, summarise, or interpret content using automated or algorithmic processes (e.g. generative or conversational AI). Colleagues must not input personal data, confidential information, or organisationally sensitive information into AI or LLM tools unless explicitly authorised. Use must comply with the AI Ethical Usage Policy.

4.10 Access: The ability to view, create, edit, store, transmit, or otherwise interact with Salutem systems, applications, email services, or data.

4.11 Approved Access: Access to Salutem systems or data that has been explicitly authorised by a line manager and, where required, IT Support or the Information Governance Team, subject to compliance with this policy.

4.12 Encryption: The process of converting data into a coded form to prevent unauthorised access. Encrypted data can only be accessed by authorised users with the appropriate decryption key.

4.13 Access Controls: Measures designed to prevent unauthorised access to records, systems, buildings, devices, or information. This includes physical controls (such as keys and lockable cabinets) and technical controls (such as passwords, role-based access, and MFA).

4.14 Devices: Technological assets such as laptops, printers, scanners, desktop computers, tablets, and mobile phones.

4.15 Removable Devices: Portable storage media used to store or transfer data, including USB sticks, CDs, DVDs, and external hard drives.

4.16 Physical Security: Measures designed to physically protect assets, including secure buildings, locks, keys, cabinets, and controlled access areas.

4.17 Cyber Security: Technical measures designed to protect systems and data from cyber threats, including firewalls, malware protection, access controls, and monitoring.

4.18 Safeguarding: Actions taken to protect children, young people, and adults at risk from harm, abuse, neglect, or exploitation.

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

4.19 IT Support Company: An external organisation contracted by Salutem to support and manage IT systems. These include providers responsible for systems such as SharePoint, Wi-Fi, devices, and EDRM platforms (e.g. Acuutech, Nourish, BLINK, iTrent, ESPHR, Salesforce, MyHipp, and Cranborne Tech Support for education services).
4.20 EDRM (Electronic Document and Records Management):
Any system used for the storage, organisation, retention, and retrieval of electronic information and records.

4.20 Shared Email Mailboxes: Email accounts (for example, those using an "Data.Protection@" address) accessed by multiple authorised colleagues. Where colleagues leave the organisation, individual mailboxes may be converted to shared mailboxes with appropriate security permissions applied.

4.21 Clear Desk: A set of physical information security practices designed to ensure that paper records, devices, and sensitive information are secured when not in use or when a workstation is unattended, preventing unauthorised access, loss, or disclosure.

5. Principles

5.1 Salutem will protect information and systems through risk-based, proportionate controls, supported by ongoing monitoring, assurance and continuous improvement. Our approach is designed to maintain the confidentiality, integrity and availability of information, while enabling safe, effective care, education and business operations.

All colleagues must:

- **Process information lawfully, fairly and transparently**, in line with UK GDPR, the Data Protection Act 2018 and organisational policy.

- **Access, use and share information strictly on a need-to-know basis**, ensuring it is only available to those with a legitimate role-related purpose.

- **Apply data minimisation**, accessing, recording and sharing only the minimum information necessary to achieve the intended purpose.

- **Use approved systems, devices and communication channels only**, and avoid unapproved workarounds (e.g., personal email, personal cloud storage, or unapproved messaging apps).

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- **Protect information and devices from unauthorised access, loss, disclosure or damage**, including by using strong authentication, locking screens, securing paper records, and following clear desk and secure disposal requirements.

- **Complete mandatory training and comply with procedures**, seeking advice promptly if unsure how to handle information safely.

- **Report information security incidents, near misses and suspected breaches immediately**, to enable swift containment, investigation and learning.

5.2 Security and privacy: will be embedded into all systems, services and ways of working **by design and by default**, ensuring safeguards are built in from the outset rather than added later.

6. Information Security Incident & Data Breach Response

6.1 Information Security Incidents, Data Events, Data Incidents and Data Breaches:
An Information Security Incident is any actual or suspected event that could compromise the confidentiality, integrity or availability of Salutem data, records, devices or systems.

For the purposes of reporting and management, issues are categorised as follows:

- **Data Event (Near Miss):** An occurrence involving data, records or systems that **could** have impacted information security, but where harm, loss or unauthorised disclosure **did not occur** (e.g., an email almost sent to the wrong recipient but stopped in time).
- **Data Incident:** An event that affects the security, availability or integrity of data or systems, but **does not meet the definition of a personal data breach** (e.g., temporary system outage, unsuccessful attempted access, or a device fault with no evidence of data compromise).
- **Data Breach (Personal Data Breach):** A confirmed breach of security leading to the accidental or unlawful **destruction, loss, alteration, unauthorised disclosure of, or access to personal data**.

All data events, data incidents and data breaches must be treated seriously and **reported immediately**. Prompt reporting enables containment, reduces harm, and supports compliance with statutory timescales (including the ICO's **72-hour** reporting requirement where applicable).

6.2 Responsibilities of All Colleagues (Immediate Actions): All colleagues must take the following actions as soon as they become aware of a data event, data incident, or suspected/confirmed data breach:

1. **Report immediately** to:
    - Your **line manager**, and

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- The **data protection officer (dpo) / information governance (ig) team**, without delay.
  Where devices, accounts, email or systems are involved, also notify the **IT Helpdesk/IT Support Provider** in line with local instructions.

2. **Record locally** by submitting a **Nourish interaction** (where required for local governance), ensuring key details are captured accurately.
3. **Do not investigate independently** and do not delete, alter, forward or "tidy up" evidence. Preserve relevant emails, screenshots, device details, logs, and timelines as instructed.
4. **Contain where safe to do so** and in line with IT/management instructions (for example, disconnecting a device from Wi-Fi, locking an account, or retrieving paperwork), without putting yourself or others at risk.
5. **Provide accurate information** when requested, including:
   - what happened and when (dates/times)
   - systems/devices involved
   - type of data affected (including whether special category/safeguarding data)
   - individuals potentially affected
   - immediate actions taken

Reporting timescale: Incidents should be reported **as soon as possible and, wherever practicable, on the same working day**. Reporting should not be delayed beyond **24 hours** from awareness. Delays increase risk to individuals and the organisation and may lead to regulatory non-compliance.

6.3 Contacting the Data Protection Officer (DPO): The DPO/IG Team must be contacted for all actual or suspected data events, data incidents and data breaches:
dataprotection@salutemsharedservices.co.uk

6.4 Recording and Oversight

- All data events, data incidents and data breaches are recorded centrally on the organisation's designated **incident and non-compliance system**.
- Local records must also be maintained where required (including via **Nourish interactions**) in line with local governance arrangements.
- Local and central records must be consistent to ensure effective oversight, assurance, trend analysis and organisational learning.

6.5 Role of the Data Protection Officer (DPO): The DPO is responsible for:

- Assessing reported events/incidents to determine whether they constitute a **personal data breach**
- Coordinating investigation, containment and remediation activity with relevant teams
- Maintaining the central incident/breach record and ensuring appropriate governance oversight

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- Determining whether notification is required to the **ICO**, other regulators/commissioners, and/or affected individuals
- Ensuring any required notifications are made within statutory timescales, including the ICO's **72-hour** requirement where applicable

This section must be read alongside the **Data Breach Management Procedure**, which sets out the detailed operational process for identifying, reporting, recording, investigating, escalating and managing data events, data incidents and data breaches.

Compliance with this policy and associated procedures is mandatory.

7. Email and Electronic Communications

Email and electronic communications are formal organisational records and must be managed professionally and securely.

7.1 Email – Core Requirements: Colleagues must:

- Use **work email accounts** for authorised business purposes only
- Communicate professionally, respectfully and appropriately at all times
- Check recipients carefully before sending (including CC/BCC) to prevent accidental disclosure
- Use **approved secure methods** (e.g., Microsoft 365 encryption/secure sharing) when sending sensitive or special category information
- Understand that emails may be monitored and/or disclosed where lawful and necessary (e.g., audits, investigations, Subject Access Requests), in line with the **Staff Privacy Notice**, applicable **DPIAs**, and UK GDPR requirements
- Escalate any suspected security or data protection concern identified through communications in line with incident/breach reporting processes

7.2 Professional Standards and Misuse: Inappropriate, unprofessional or unsafe communications may result in corrective action and/or disciplinary action in line with Salutem procedures.

7.3 Email is Not a Storage System: Email inboxes must not be used as long-term storage. Important emails and attachments that form part of the organisational record must be saved to approved shared locations in line with the **Records Management Policy** and retention schedule. Inboxes must be managed and "cleansed" in accordance with retention requirements.

7.4 Monitoring (Transparency and Proportionality): Salutem monitoring of email and communications (where undertaken) will be:

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- **Lawful, proportionate and risk-based**
- Subject to governance oversight and applied only where there is a legitimate business, safeguarding, security or compliance requirement
- Supported by a **DPIA** where required
- Transparent and aligned with the **Staff Privacy Notice**
- Not used for unfair or intrusive surveillance

7.5 Practical Email Safety Rules: Colleagues must:

- Not change approved email signatures or security settings without authorisation
- Not use work email for personal sign-ups (e.g., social media) or personal correspondence
- Use "recall" only as a mitigation step—**recall is not guaranteed**; report mis-sends immediately
- Review email chains before sending to avoid oversharing
- Use initials and minimise personal data where appropriate and lawful
- Attach and share only what is necessary for the purpose

7.6 Other Electronic Communications (Approved Platforms): Colleagues may communicate using approved platforms such as **Nourish, BLINK and Microsoft Teams**. Each platform has a defined purpose:

- **BLINK:** Staffing matters, general queries and internal colleague communications. **Must not** be used for special category data or sensitive IWS information.
- **Nourish:** Service management communications and information relating to Individuals We Support (IWS), as designed and authorised.
- **Microsoft Teams:** Meetings and business communications; may include service-related discussions where appropriate and necessary, using privacy controls and good practice (e.g., careful screen-sharing).

These platforms are auditable and access-controlled. Compliance is monitored through governance and audit activity.

8. Cyber Security

8.1 Anti-virus, Firewalls and Malware Protection: Salutem devices (laptops, desktops, tablets and mobiles where applicable) are protected by appropriate anti-virus/anti-malware controls. Security software is configured to update automatically and scan files on access. Controls are applied proportionately based on device type and risk.

8.2 Laptops and Tablets (Corporate Devices)

- Laptops and workstations use **Microsoft Defender for Endpoint** as standard.

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- Security updates are delivered via Microsoft services (including **Intune** and Defender policies).
- Devices perform security checks at start-up before user access is permitted.
- Devices are protected by local (personal) firewalls.

Salutem uses **Meraki** to manage boundary firewalls. These firewalls:

- Are not directly accessible from the internet
- Require **MFA** for administrative access
- Are managed via a secure cloud console
- Record and log access and configuration changes via the IT support desk

8.3 Nourish Devices

- Nourish devices are managed via **Mobile Device Management (MDM)**.
- Internet browsing and app downloads are restricted.
- Connectivity may be enabled for **synchronisation only** (e.g., SIM-enabled sync) and must not be used for general internet access.
- Any proposed change to restrictions must be risk assessed, tested and formally approved.

8.4 Salutem-Issued Mobile Phones: Salutem-issued mobile phones:

- Are protected by appropriate security controls (device security configuration and, where applicable, anti-malware protections)
- May access email and approved documents (e.g., SharePoint/Teams) where authorised
- Are configured to reduce local data storage and prevent insecure capture/sharing where technically possible
- Are supported by network-level protections in addition to device controls

8.5 Firewall Governance: The IT support provider:

- Maintains a central register of firewall rules
- Reviews, updates and removes rules in a controlled manner
- Blocks unauthenticated inbound connections by default

8.6 Internet and Wi-Fi Security

- Secure Wi-Fi connectivity is provided across Salutem sites to support authorised access to systems and services.
- Connections use appropriate encryption standards (e.g., TLS).
- Default passwords are changed and key network settings are secured and logged.

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- **Public Wi-Fi must not be used** to access Salutem systems unless an approved secure access method is in place (see Remote & Home Working Policy).

Service user/visitor Wi-Fi access:

- Must be provided only where there is a clear care-based or business need
- Must be controlled and may be withdrawn where misuse is identified

Web filtering:

- Access to known malicious or inappropriate sites is blocked.
- Additional restrictions may be requested through defined governance routes.

8.7 Network Configuration and Change Monitoring: The IT support provider:

- Maintains audit controls for network/system changes
- Ensures configurations are documented, monitored and secured

8.8 Web Applications: Salutem maintains a list of authorised web applications. Colleagues must not use unauthorised web applications to process Salutem data. Blocked applications are managed by IT.

8.9 Phishing and Malicious Email: If phishing is suspected:

- Do not click links or open attachments
- Do not reply to the email
- Forward/report the message to the IT helpdesk for assessment and instructions
- If you have clicked a link or entered credentials, report immediately—speed matters

8.10 Backups

- Core systems operate with UK-based backup arrangements (including offline protections where applicable).
- Backups occur at defined intervals and are tested at least annually.
- Nourish data is backed up incrementally with daily full backups.
- Where appropriate, devices and services can operate offline during short outages (subject to local procedures).

8.11 Penetration Testing: IT support providers are responsible for proportionate penetration testing of supported systems (at least annually, or as risk requires), and for providing results to Salutem for assurance and remediation tracking.

8.12 Patching and Updates

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- Endpoint management is used to patch laptops, PCs and tablets on a scheduled basis.
- Devices that fail to update are flagged and remediated.
- Devices falling out of compliance may be restricted or removed from the network.
- Unsupported/unpatched software is removed, isolated or risk-assessed with documented sign-off by the DPO/IT Manager/SIRO as appropriate.
- Nourish device security updates are applied automatically where supported.

8.13 External Vulnerabilities and Threat Intelligence: The IT support provider monitors external threats (e.g., ransomware campaigns, published vulnerabilities). Emerging risks are reported through governance routes, with immediate action taken where required.

8.14 Secure Application Design (OWASP): Where Salutem operates or commissions web applications, suppliers must align controls with the **OWASP Top 10** risks, supporting secure design and protection against common attack vectors.

8.15 Access Controls

- All users must have an individual named account.
- Access is restricted to trusted users and compliant devices (where applicable via MDM).
- Role-based access controls are applied and reviewed at least annually (and more frequently where risk requires).
- Access changes must be authorised by designated senior roles (e.g., Divisional Coordinator/Regional Director/Director/DPO as defined).
- System activity is logged and retained for a defined minimum period (minimum 90 days), supporting audit and investigation.
- Large or unusual downloads trigger alerts and escalation where appropriate.
- Colleagues are informed of monitoring through the Staff Privacy Notice and relevant guidance.

Further detail is available in the **Access Controls Guidance**.

8.16 Leavers: When a colleague leaves Salutem:

- Access termination is triggered promptly via defined HR/payroll processes
- All devices and organisational records must be returned on or before the final day of employment
- Managers must ensure leavers are removed from Nourish and local systems, with compliance monitored through governance routes

8.17 Enhanced Systems Rights (Privileged Access)

- Elevated permissions are granted strictly on a need-to-have basis.
- Global administrator accounts are not used for day-to-day activity.

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- Segregated privileged accounts are issued where elevated access is required.
- Privileged activity is logged and monitored.
- Privileged access may only be initiated from Salutem-owned or authorised IT support devices.

9. CCTV & Surveillance

9.1 CCTV Governance: CCTV must have a clear lawful purpose and be proportionate. Before installation or significant change:

- A **DPIA** must be completed
- The CCTV checklist must be completed
- Documentation must be reviewed and approved by the DPO/IG Team

CCTV must not intrude into private areas and must comply with ICO guidance and organisational procedures.

9.2 Surveillance & Audio Procedure: This section must be read in conjunction with the **Surveillance & Audio Procedure**.

9.3 Photography, Recording and Covert Recording

- Colleagues must not take photographs or videos for personal purposes in an IWS's home or other private spaces. This may constitute gross misconduct and may also be a criminal offence.
- Colleagues must not take photographs, videos or voice recordings for work purposes on a personal device, except in a genuine emergency. Any emergency content must be transferred to approved Salutem systems as soon as possible and deleted from the device.
- Covert recording of colleagues, IWSs or members of the public is prohibited unless explicitly authorised through the appropriate legal/ethical route.
- Any situation that may require covert recording must be discussed in advance and may require a **Mental Capacity Assessment** and **Best Interests Decision** where relevant. Advice must be sought from the DPO/IG Team to ensure the approach is lawful, proportionate and ethical.

9.4 Doorbell Cameras: Doorbell cameras must not be installed without prior DPIA completion and DPO/IG approval. Locations must follow the **Surveillance & Audio Procedure**.

10. Data Security and Safe Working Practices (Homes, Offices & Clear Desk)

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

10.1 Buildings and Access Control: All buildings must have lockable doors and windows. Doors must not be propped open unless a member of staff is present and actively supervising access.

Location managers (or nominated building leads) must maintain an up-to-date record of colleagues issued with keys and/or access codes.

When a colleague leaves:

- Keys must be returned
- Door codes must be changed without delay
- If keys are not returned, affected locks must be changed promptly

Where frequent code changes are operationally difficult, additional controls must be implemented (e.g., secure storage areas, removal of confidential items from accessible areas, supervision requirements) and risks recorded. Codes should still be changed periodically as a preventative measure.

10.2 Offices and Key Management: Offices must be locked when not in use. Access lists must be maintained. Keys must be stored securely (e.g., key safe) with access limited to authorised managers.

10.3 Visitors and Unauthorised Access: All locations must prevent unauthorised individuals from having unsupervised access to records, personal data or technology.

Visitor controls must include:

- Identity checks (where appropriate)
- Confirmation of authorisation by the person being visited
- Sign-in and sign-out processes (with previous entries concealed)
- Visitors escorted at all times

Colleagues should wear ID where required and challenge unaccompanied visitors politely and safely, following the **Visitor Policy**.

10.4 Supported Living Arrangements: In supported living, controls must be applied proportionately and must respect individuals' privacy and right to home life. Staff must:

- Follow clear desk principles
- Handle information securely
- Apply local remote working guidance where relevant
- Avoid introducing "office-style" controls that are inappropriate within a person's home

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

10.5 Physical Records Management: Paper records containing confidential information must be stored securely (locked cabinet/drawer/room). Managers must maintain a record of authorised access where required. Access must be restricted to legitimate business need.

10.6 Records Leaving the Premises: Physical records removed from a location must:

- Be authorised and signed in/out by the manager (or delegated authority)
- Be recorded accurately
- Be transported and stored securely (including use of a lockable records box for overnight/extended retention)

Where records are taken off-site, colleagues must follow the **Remote & Home Working Policy** and **Data Sharing Guidance**.

10.7 General Security Requirements (All Locations)

- Do not leave information unattended
- Clear workspaces when not in use
- Lock devices when unattended

10.8 Archiving and Closed Records: Closed records must be formally archived in line with the retention schedule. Closed records must not be stored informally or outside the approved archiving process. This applies to paper, electronic and hybrid records.

Managers are responsible for:

- Prompt archiving when records are closed
- Confirming disposal actions are completed and recorded when retention expires
- Participating in retention/disposal audits led by the IG Team

10.9 Security of Archived Information: Archived records must be protected by access controls equivalent to (or stronger than) live records, with restricted and auditable access.

10.10 Retrievability: Archived information must remain retrievable throughout its retention period to support inspections, audits and information rights requests (e.g., SARs).

10.11 Accountability, Retention and Disposal: Records must be retained only as long as required by law, regulation or legitimate business need, and disposed of securely in line with the **Records Retention and Disposal Policy**.

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

11. Learning and Development

Salutem is committed to ensuring colleagues understand their responsibilities and are supported to work securely and professionally. Learning and development supports compliance with UK GDPR accountability and ICO expectations.

11.1 Mandatory Learning: Where required by role, colleagues must complete mandatory learning covering:

- Data protection and UK GDPR principles
- Confidentiality and lawful processing
- Information security responsibilities and risk awareness
- Secure use of systems, devices and communication tools
- Safe, respectful and professional communication with colleagues, partners and people we support

Managers must ensure completion is monitored and recorded.

11.2 Role of Line Managers: Line managers are responsible for:

- Ensuring colleagues are aware of and understand this policy
- Reinforcing expectations through supervision, team meetings and performance discussions
- Identifying knowledge gaps and arranging additional support or escalation where required

12. Areas of Responsibility

Effective implementation depends on clear responsibilities aligned to the ICO's accountability principle.

12.1 Senior Leadership Team (SLT): The Senior Leadership Team holds overall accountability for compliance with this policy and for ensuring it is enforced consistently across the organisation. SLT approves any policy exceptions where these are justified by operational need and supported by an appropriate risk assessment. SLT is also responsible for ensuring adequate resources are available to deliver effective training, monitoring, assurance activity and IT support. In addition, SLT reviews audit outcomes, incident trends and improvement plans to ensure risks are understood and addressed and that information security continues to improve.

12.2 Information Governance Team: The Information Governance Team leads the implementation, monitoring and periodic review of this policy, ensuring it remains effective and aligned with legal and regulatory requirements. The team conducts audits and provides assurance reporting to support oversight and accountability. It also analyses incidents and near misses to identify themes, learning and improvement actions, and coordinates organisational responses to

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

reduce recurrence. Where applicable, the team maintains records of approved personal devices that are authorised to access Salutem systems.

12.3 IT Support Team / Providers: The IT Support Team and appointed IT providers are responsible for maintaining the technical controls that protect the confidentiality, integrity and availability of Salutem systems and data. This includes supporting secure access arrangements such as multi-factor authentication (MFA), remote access controls, and device compliance requirements. They also support incident containment and remediation actions as instructed, working closely with the DPO/Information Governance Team during investigations and recovery.

12.4 Data Protection Officer (DPO): The Data Protection Officer provides independent oversight and advice to ensure compliance with UK GDPR and related data protection requirements. The DPO assesses reported incidents to determine whether they constitute a personal data breach and advises on any notification requirements to the ICO, other regulators and/or affected individuals. The DPO also approves Data Protection Impact Assessments (DPIAs) where required and oversees the use of proportionate monitoring and remote wiping arrangements where these are necessary and lawful.

12.5 Line Managers / Supervisors: Managers and supervisors are responsible for ensuring this policy is implemented locally and followed day to day within their teams. They must ensure joiner/mover/leaver processes are completed promptly so that access rights remain appropriate and are removed when no longer required. Managers also address non-compliance through supervision, support, and appropriate management action, escalating concerns in line with organisational procedures where necessary.

12.6 Colleagues Using Personal Devices: Colleagues who are authorised to use personal devices for work purposes must obtain approval before connecting any personal device to Salutem systems or using it to access organisational data. They must comply with all required security controls and the terms of any personal device agreement. Any loss, theft or suspected compromise of a device used for work must be reported immediately so that protective action can be taken.

12.7 All Colleagues: All colleagues are responsible for maintaining professional standards and protecting confidentiality, including being mindful of safeguarding responsibilities when handling information. They must complete mandatory training, follow procedures and apply secure working practices at all times. Colleagues are also expected to contribute to a positive information governance culture by raising concerns early, reporting incidents promptly, and supporting continuous improvement in information security.

12.8 National Data Guardian (NDG) Data Security Standards (Digital Social Care): Salutem evidences compliance with the NDG 10 Data Security Standards through this policy, supporting procedures, technical controls and assurance activity. Standards are grouped across **People,**

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

Process and Technology, underpinned by Caldicott-style principles of appropriate and proportionate information sharing.

13. Monitoring and Compliance

13.1 Compliance with this policy is mandatory. Failure to comply may result in corrective action and/or disciplinary action, including withdrawal of access to systems and facilities, up to and including dismissal, and notification to regulators or law enforcement where required.

All actions will be proportionate, documented, and carried out in line with employment law, contractual terms and internal governance procedures.

14. Associated Documents

- AI Ethical Usage Policy
- Data Breach Management Procedure
- Records Management Policy
- Surveillance & Audio Procedure
- Remote & Home Working Policy
- Staff Privacy Notice
- Visitor Policy
- Cyber Security Policy

15. Legal, Regulatory & Standards Framework

- UK GDPR – lawful processing, accountability, data minimisation, security, rights
- Data Protection Act 2018 – UK enforcement, exemptions, safeguarding provisions
- Privacy and Electronic Communications Regulations (PECR)
- Regulator: Information Commissioner's Office (ICO)
- Health and Safety at Work etc. Act 1974 – safe digital systems of work
- Management of Health and Safety at Work Regulations 1999 – risk assessment (including IT and remote working)
- Employment Rights Act 1996 – fair and proportionate monitoring and access control
- Equality Act 2010 – non-discriminatory information handling and systems
- Care Act 2014 – safeguarding adults, lawful information sharing

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

- Children Act 1989 & 2004 – safeguarding and multi-agency information use
- Mental Capacity Act 2005 – best-interest decision-making where capacity is lacking
- CQC Fundamental Standards (England) – secure records and governance
- Care Inspectorate Wales (CIW) Regulations
- Ofsted Education Inspection Framework

16. 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	Author	Summary of Changes	Approved By
V1.0	May 2026	Chris Bell, improvement and Development Manager (DPO)	The attached policy **does not simply reference** the Physical Information Security Policy, Information Security Policy, and Personal Devices Policy, Email Management Policy, Acceptable Use Policy — it **replaces them** by: • Embedding physical, digital, and behavioural controls into one structure • Applying consistent principles across all environments • Strengthening governance and accountability • Making expectations clearer for colleagues • Improving compliance with UK GDPR, ICO, NDG, DSPT, and regulators	Melinda Glover, Quality Assurance Inspection & Regulation Director

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

17. Appendices

Appendix A:	Use of Personal Mobile Phones in Salutem Location
Appendix B:	Personal Device Agreement

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.