IT AND COMMUNICATION POLICY

Response Healthcare Solutions Ltd

Date of Issue: June 2025
Review Date: June 2026
Classification: Internal – Confidential
Status: Approved

---

1. Purpose and Scope

1.1 Purpose

This IT and Communication Policy sets out Response Healthcare Solutions Ltd's ("RHS", "the Company") rules, standards and staff responsibilities in relation to the use of IT systems, electronic communications and digital information. It supports and must be read alongside the RHS **Data Protection and Confidentiality Policy (June 2025)** and is designed to ensure:

- Compliance with:
    - UK GDPR and Data Protection Act 2018
    - Health and Social Work (Scotland) Act 2015
    - Public Services Reform (Scotland) Act 2010
    - Care Inspectorate standards and inspection frameworks
    - Data (Use and Access) Act 2025 (digital information standards)
    - Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 where relevant
    - Human Rights Act 1998 (Article 8 – respect for private and family life)
    - Common law duty of confidentiality
- Protection of client, patient, service user, employee and business information.
- Safe, secure and effective use of technology to deliver high-quality, person-centred care in line with the Health and Social Care Standards.

1.2 Scope

This Policy applies to:

- All employees of RHS (permanent, temporary, bank, agency and zero-hours).
- All contractors, consultants, volunteers, trainees and students on placement.

- All third parties with access to RHS information systems or data.

It covers all use of:

- Company-owned devices (PCs, laptops, tablets, phones), networks and applications.
- Personal devices used in connection with work (BYOD – Bring Your Own Device), where permitted.
- Email, instant messaging, telephony, video conferencing, social media and any electronic communication channel used for RHS business.
- Cloud services, storage media and any system processing personal or confidential information on behalf of RHS.

---

2. Legal and Regulatory Framework

2.1 Data Protection and Confidentiality

All IT and communication activities must comply with:

- RHS Data Protection and Confidentiality Policy (June 2025).
- UK GDPR and Data Protection Act 2018, including special category data provisions for health and social care (Schedule 3).
- Common law duty of confidentiality.

The Company is the **Data Controller** for personal data processed through its systems. All employees are "Employees" for data protection purposes (as defined in the Data Protection and Confidentiality Policy) and are personally responsible for compliance.

2.2 Health and Social Care Framework (Scotland)

IT and communication practices must support and not undermine:

- **Health and Social Care Standards: My support, my life**, particularly:
    - Standard 1: Dignity and respect
    - Standard 2: Compassion
    - Standard 3: Be included
    - Standard 4: Responsive care and support
    - Standard 5: Wellbeing
- **Care Inspectorate** registration, inspection and enforcement requirements, including information governance, record-keeping, confidentiality and security expectations.

2.3 Employment and Human Rights

All monitoring and controls under this Policy will be:

- Necessary, proportionate and transparent.

- Compliant with the Employment Rights Act 1996, Equality Act 2010 and Human Rights Act 1998.
- Implemented in line with RHS fairness and disciplinary safeguards described in the Data Protection and Confidentiality Policy.

---

3. Roles and Responsibilities

3.1 Board and Senior Management

- Approve and oversee implementation of this Policy.
- Ensure sufficient resources for secure IT, training and incident response.
- Support a culture of confidentiality, data protection and safe digital practice.

3.2 Data Protection Officer (DPO)

- Policy owner for data protection aspects.
- Advises on lawful processing, security and breach management.
- Reviews high-risk IT changes (e.g. new systems, new data flows) via Data Protection Impact Assessments (DPIAs).

Contact Details:

- **Name:** Mazher Khan
- **Email:** maz.manager@responseheathcare.co.uk
- **Telephone:** 07588 444915
- **Address:** Office 2.6, 1 Barrack Street, Hamilton, ML3 0DG

3.3 IT Lead / System Administrator

- Implements technical security controls described in the Data Protection and Confidentiality Policy (Section 11), including encryption, backups, access controls and patching.
- Ensures systems support retention schedules and secure deletion.
- Maintains system logs for security and audit purposes.
- Coordinates with DPO on security incident response.

3.4 Line Managers

- Ensure staff understand and comply with this Policy.
- Authorise access rights based on role and "need-to-know" principles.
- Monitor compliance with IT and communication rules.
- Escalate incidents and suspected breaches promptly.

3.5 All Employees, Contractors and Volunteers

Every user of RHS systems must:

- Read, understand and comply with this Policy and the Data Protection and Confidentiality Policy.
- Complete mandatory training and annual refresher training.
- Use systems only for lawful, authorised business purposes.
- Protect passwords, devices and information from unauthorised access.
- Report suspected incidents, breaches, loss or theft of devices, and phishing attempts immediately.
- Be personally accountable for their own compliance and the security of systems they use.

---

4. Acceptable Use of IT Systems

4.1 General Principles

- Company IT systems are primarily for business use in support of safe, high-quality care.
- Limited personal use may be permitted where:
    - It does not interfere with work duties.
    - It does not breach this Policy, the Data Protection and Confidentiality Policy or any law.
    - It does not introduce security risks (e.g. unsafe websites, downloads or unapproved applications).

4.2 Permitted Uses

Users may use RHS IT systems for:

- Direct service delivery and care-related activities.
- Clinical, administrative and business tasks necessary for their role.
- Learning and development directly relevant to RHS business.
- Brief, occasional personal use (e.g. checking personal email) where not disruptive.

4.3 Prohibited Uses

Users must **not**:

- Access, view, store or transmit material that is illegal, discriminatory, harassing, abusive, defamatory, sexually explicit or otherwise inappropriate.
- Bypass or attempt to bypass security controls, monitoring tools or system restrictions.

- Install software, applications or tools on RHS devices without explicit authorisation from IT.
- Use RHS systems for personal business ventures or external commercial activities.
- Use RHS systems for political campaigning, unauthorised lobbying or religious proselytising.
- Copy, move or store personal data onto unencrypted devices, USB sticks or unapproved cloud services.
- Deliberately exceed permitted access or attempt to access systems or data beyond their role.
- Engage in any activity that might compromise system integrity, confidentiality or availability.

4.4 Consequences of Breach

Breaches may lead to disciplinary action up to and including summary dismissal, in accordance with the disciplinary framework set out in the Data Protection and Confidentiality Policy (Section 20).

---

5. Email, Messaging and Telephony

5.1 Business Email Use

- Use only authorised RHS email accounts for work-related communications involving clients, patients, service users, staff or confidential data.
- Do **not** forward work emails or attachments to personal email accounts.
- Ensure email recipients are correct before sending; use secure methods and encryption where required for sensitive information.
- Include appropriate email disclaimers as mandated by RHS.
- Retain sent emails in accordance with retention schedules (Section 10 of the Data Protection and Confidentiality Policy); do not delete work-related emails prematurely or inappropriately.

5.2 Confidentiality in Communications

In accordance with Sections 5 and 6 of the Data Protection and Confidentiality Policy:

- Do not include unnecessary personal or special category data in emails or messages.
- Avoid discussing identifiable client or employee information over unsecured channels or in public places.
- Use initials, unique identifiers or anonymised descriptors where full identity is not needed.
- Avoid sending sensitive data in unencrypted SMS or consumer messaging platforms.
- Be aware that email is not fully secure; treat sensitive information accordingly.

5.3 Instant Messaging and Consumer Apps

In accordance with Section 5.3 of the Data Protection and Confidentiality Policy:

- Do **not** use WhatsApp, Telegram, Signal, Facebook Messenger, Viber or similar consumer messaging apps for work-related confidential information or personal data.
- Only use Company-approved secure messaging or collaboration tools, following IT and DPO guidance.
- When approved tools are used, ensure conversations are retained where required for record-keeping, and deleted securely when no longer needed.

5.4 Telephone and Video Calls

- Verify identity before disclosing personal or confidential information over the telephone.
- Conduct calls in private areas where conversations cannot be overheard by unauthorised persons.
- Use clear, professional language appropriate to the context.
- For video calls involving personal data (e.g. remote consultations, case discussions), use approved platforms only and ensure screens and surroundings maintain client/ service user privacy.
- Be aware that calls may be monitored or recorded for quality assurance, training or compliance purposes (where lawful); ensure this is communicated to callers.

5.5 Call and Meeting Recording

- Any recording of telephone calls, video calls, in-person meetings or video conferences is subject to the **absolute prohibition on unauthorised recording** set out in Section 5.1 of the Data Protection and Confidentiality Policy.
- Personal devices **must not** be used to record any work-related conversation or meeting.
- Authorised recording (if ever used) must:
    - Be formally justified and approved in writing by the DPO and senior management.
    - Use Company-approved equipment and secure storage only.
    - Be documented in Records of Processing Activities and Data Protection Impact Assessments.
    - Comply with the lawful basis for processing and transparency requirements (all parties informed in advance).
    - Follow retention and secure deletion schedules (Section 10 of the Data Protection and Confidentiality Policy).

---

6. Social Media and Public Communications

6.1 Personal Social Media Use

In accordance with Section 5.3 of the Data Protection and Confidentiality Policy, employees must **not**:

- Post, share, comment on or otherwise publish any information about RHS clients, patients, service users, colleagues, internal processes, incidents or operations.
- Discuss employment grievances, internal matters, disputes or investigations on social media, blogs or public forums.
- Use photographs, videos, audio or other content taken on RHS premises or during work, without explicit written authorisation from senior management and the DPO.
- Connect with clients, patients or service users on personal social media accounts, or accept such connections.
- Identify themselves as RHS staff in ways that create risk of unwanted personal contact by service users.
- Post derogatory comments about RHS, competitors, service users or colleagues on social media.
- Engage in behaviour on social media that brings RHS into disrepute or undermines public confidence in care quality.

6.2 Official Social Media and Marketing

- Only designated, trained staff authorised by management may post on official RHS accounts.
- All content must follow approved RHS branding, tone, style and content guidelines.
- Content must never disclose identifiable health, social care or personal information without explicit written, informed consent, documented lawful basis and DPO review.
- Marketing material featuring individuals must include signed consent forms retained for data protection purposes.
- All content must respect the dignity, privacy and rights of people who experience care, in line with the Health and Social Care Standards.
- Social media accounts must not be used to make claims about service quality, clinical outcomes or regulatory standing without evidence and prior review.

6.3 Engagement and Comments

- Official RHS social media accounts must have clear moderation policies.
- Inappropriate comments, posts or messages (containing confidential information, abusive language, defamatory content) must be removed and reported.
- Staff must not engage in public debate on social media on behalf of RHS without prior authorisation.

6.4 Media Enquiries

- Any approach from journalists, bloggers, researchers, media organisations or external parties seeking information about RHS, its services, incidents or individuals must be reported **immediately** to senior management.
- Staff must **not** provide statements, information, confirmation, denial or comment to media representatives without prior authorisation.
- All external media contact must be directed to a designated spokesperson approved by management.
- Third-party disclosure prohibitions in Sections 5.2 and 6.3 of the Data Protection and Confidentiality Policy apply in full.

---

7. Personal Devices and Recording

7.1 Use of Personal Devices for Work (BYOD)

- Personal devices must **not** be used to access, store or process personal data, confidential information or care records unless explicitly authorised by the DPO and IT, and only under strict technical controls (e.g. mobile device management, encryption, remote wipe capability, passcode protection).
- Under **no circumstances** may staff:
    - Copy care records, health information, HR files, financial records or other personal data to personal devices.
    - Use personal cloud storage (Google Drive, Dropbox, OneDrive, iCloud, etc.) to store or transmit work-related personal or confidential data.
    - Transfer client, patient or employee information to personal USB sticks, memory cards or external drives.
    - Use personal email accounts to send or receive personal data, confidential documents or care information.
- Where personal devices are approved for work, they remain subject to:
    - This Policy and the Data Protection and Confidentiality Policy in full.
    - IT security requirements (Section 10).
    - Monitoring for compliance (Section 11.2).
    - Potential remote access, monitoring or deletion by RHS IT for security purposes.

7.2 Absolute Prohibition on Personal Recording

In strict accordance with Section 5.1 of the Data Protection and Confidentiality Policy:

7.2.1 Complete Prohibition

Employees are **absolutely prohibited** from recording any audio, video, photograph, image or other content on personal devices or any personal equipment that relates to:

- Clients, patients, service users, their families, friends or any visitors.
- Colleagues, managers, other staff members or third parties working with RHS.
- RHS premises, buildings, facilities or locations.
- Any meetings, training sessions, briefings, case conferences or discussions.
- Any confidential information, personal data, care records or business information.
- Any RHS activities, services, operations, events or communications.

7.2.2 No Exceptions

This prohibition applies **without exception**, regardless of:

- The stated purpose or intention of the person making the recording.
- Whether the recording is claimed to be "for personal use only" or "for safeguarding purposes".
- Whether consent has been obtained from the person(s) being recorded.
- Whether the employee believes the recording is in the public interest.
- Whether the employee claims the recording is necessary for self-protection or employment protection.
- Any emergency or crisis situation.
- Professional codes or perceived professional duties.
- Claims that recording is needed for "evidence".

7.2.3 Legal Basis

Unauthorised recording on personal devices without explicit authorisation constitutes:

- **GDPR Violation** – Unauthorised processing of personal data, violating Article 5 (lawfulness, fairness, transparency, purpose limitation).
- **Data Protection Act 2018 Breach** – Unlawful processing of personal data, potentially including special category data (health, biometric).
- **Breach of Duty of Confidentiality** – Violation of common law and contractual confidentiality obligations.
- **GDPR Article 3 Violation** – Covert recording fundamentally negates transparency, a cornerstone of GDPR.
- **Potential Criminal Offence** – May constitute:
    - Offence under Regulation of Investigatory Powers Act 2000 (unauthorised surveillance).
    - Common law offence (privacy breach).
    - Computer Misuse Act 1990 (unauthorised access, if system is involved).
- **Workplace Rights Violation** – Infringement of colleagues' right to work in an environment free from covert surveillance.

- **Defamation Liability** – Personal recording may create civil liability for defamatory, false or misleading content.
- **Employment Contract Breach** – Violation of employment contract confidentiality clauses.
- **Professional Standards Breach** – Where applicable, violation of healthcare professional codes (GMC, NMC, HCPC, etc.).

7.2.4 Disciplinary and Legal Consequences

Employees who make unauthorised recordings face:

- **Summary dismissal** without notice.
- **Criminal prosecution** by police or prosecution service.
- **Civil legal action** by affected parties (privacy claims, defamation, breach of confidence).
- **Referral to professional regulatory bodies** (GMC, NMC, HCPC, social work bodies).
- **Loss of professional qualifications or registration**.
- **Personal financial liability** for damages, legal costs and compensation.
- **Potential civil restraining orders** to prevent publication or further disclosure.

7.2.5 Reporting Personal Recording

Any suspected unauthorised recording must be reported immediately to:

- Line manager or senior management, or
- Data Protection Officer (DPO): Mazher Khan, maz.manager@responseheathcare.co.uk, 07588 444915, or
- Police (if criminal behaviour suspected).

RHS will investigate promptly and take appropriate action.

7.3 Authorised Recording (Exceptional Circumstances Only)

Where recording is genuinely necessary for legitimate, lawful business purposes (e.g. agreed clinical use, approved training, quality assurance, safeguarding investigation with legal advice):

- **Explicit written approval** must be obtained **in advance** from:
    - Data Protection Officer (DPO)
    - Senior management and/or Board
- A **Data Protection Impact Assessment (DPIA)** must be completed.
- A **Legitimate Interest Assessment (LIA)** must be completed and documented.

- **Lawful basis** for processing must be clearly identified and documented (e.g. explicit consent, legal obligation, vital interests, performance of public task, legitimate interests).
- **All data subjects** must be informed **in advance** that recording will take place.
- **Explicit written consent** must be obtained from each person being recorded (where consent is the lawful basis).
- **Company equipment only** must be used; personal devices are not permitted.
- **Technical and organisational security measures** must be implemented (encryption, secure storage, access controls).
- **Records of Processing Activity** must be maintained and filed with DPO.
- **Retention schedule** must be specified (Section 10).
- **Secure deletion** or anonymisation must occur when retention period expires.

Authorised recording is rare and exceptional. The default position is the absolute prohibition in Section 7.2.

---

8. Access Control, Passwords and User Accounts

8.1 Principles

- Access to RHS systems and data is granted strictly on a "need-to-know" basis and role-based access control (RBAC), as described in Section 11.1 of the Data Protection and Confidentiality Policy.
- Users must only access systems, applications, data and records required to perform their specific duties.
- Access is reviewed and updated when roles change; unnecessary access is removed.

8.2 Password and Authentication Requirements

Users must:

- Keep passwords confidential; never share them with anyone, including:
    - Managers, supervisors or senior staff
    - IT staff or system administrators
    - Colleagues or friends
    - Family members or external parties
- Use strong passwords compliant with Company standards:
    - Minimum length: 12 characters
    - Mix of uppercase, lowercase, numbers and special characters
    - Avoid dictionary words, names, dates or easy-to-guess patterns

    - Never reuse recent passwords
- Change passwords immediately if compromise is suspected.
- Change passwords at intervals specified by IT (typically 90 days or as mandated).
- Use multi-factor authentication (MFA) where provided and enabled by RHS.
- Never write passwords down or store them in unsecured locations.

8.3 Account Management

- Users are personally responsible for activity on their account; shared accounts are prohibited.
- Do not attempt to guess, crack or discover other users' passwords.
- Do not attempt to access systems or data on behalf of another user.
- Report suspected password compromise or account misuse immediately to IT.

8.4 Session Management

- Lock or log off devices when stepping away from the workstation, even briefly.
- Do not leave screens displaying personal, confidential or sensitive information unattended or visible to unauthorised persons.
- Comply with automatic session timeout settings configured by IT.
- Clear desk policy: remove paper documents and lock cabinets when leaving the workstation.

8.5 Joiners, Movers and Leavers

Joiners:

- IT access requests must be submitted by line manager on first day, specifying systems and data required for the role.
- Access is granted only after:
    - Successful background check (DBS) and safeguarding clearance (where required).
    - Completion of confidentiality, data protection and IT security training.
    - Signed acknowledgement of this Policy and the Data Protection and Confidentiality Policy.

Movers (role changes):

- When staff change roles, line managers must request updated access (additions and removals).
- Old access must be removed before or immediately after new access is granted; "over-provisioning" is prohibited.
- Data access must be reviewed and documented.

Leavers (resignation, dismissal, retirement):

- On final day or before, **all access must be disabled** immediately:
    - Computer accounts locked or deleted
    - Email access revoked
    - VPN and remote access disabled
    - Mobile devices remotely wiped if required
    - Physical access cards, badges and keys returned
- All Company equipment, documents, storage media and devices must be returned.
- Personal data on devices must be securely deleted.
- Offboarding checklist must be completed and signed.

---

9. Data Storage, Retention, Transfer and Deletion

9.1 Data Storage

- Store personal data, confidential information and care records **only on approved Company systems and secure cloud services** contracted by RHS.
- Approved systems include:
    - Company network drives (with appropriate access controls).
    - Approved secure cloud services (with data processing agreements and encryption).
    - Authorised case management, health or electronic health record systems.
- Do **not** store personal or confidential data on:
    - Local desktop drives or temporary folders
    - Unencrypted laptops or portable devices
    - USB sticks, memory cards or external hard drives
    - Personal cloud accounts (Google Drive, Dropbox, OneDrive, iCloud, etc.)
    - Consumer file-sharing or backup services
    - Personal email accounts
    - Home computers or domestic broadband connections (unless authorised and with proper encryption and security controls)

9.2 Retention and Archiving

All electronic records (emails, documents, databases, systems) must comply with the **retention schedules** set out in **Section 10 of the Data Protection and Confidentiality Policy**, including:

- **Client and patient records:** 3+ years after last contact (varies by service type).
- **Employee records:** employment duration plus 7 years post-termination.
- **Payroll records:** 6 years (HMRC requirement).
- **Email:** 3 years (general business emails may be deleted sooner with IT approval).
- **IT logs and security records:** 1 year minimum.
- **Financial records:** 6 years.
- **Incident reports:** 3–7 years depending on severity.

Systems must be designed and configured to:

- Support automatic archiving and deletion schedules.
- Prevent users from circumventing retention requirements by deleting records inappropriately.
- Generate audit trails showing when data was retained, archived, or deleted.

Managers and IT must periodically review data holdings to ensure active records remain necessary.

9.3 Data Transfer and Sharing

Externally sharing personal data must follow the **third-party disclosure rules** set out in **Section 6 of the Data Protection and Confidentiality Policy**.

Data may only be shared with external recipients (NHS, local authority, other healthcare providers, regulatory bodies) where:

- The data subject has consented (where required).
- A lawful basis exists (e.g. legal obligation, vital interests, public task, legitimate interests, health and social care purpose).
- The recipient has proper legal authority to request the information.
- A Data Processing Agreement or Data Sharing Agreement is in place (where the recipient is processing data on RHS's behalf).

When transferring personal data:

- Use secure transfer methods:
    - Encrypted email (with strong passwords).
    - Secure file transfer portals (approved by RHS).
    - NHS-approved transfer mechanisms (e.g. NHS secure email).
    - Direct systems integration with proper authentication.
- Do **not** use:
    - Unencrypted email for sensitive personal data.
    - Personal email accounts.
    - Consumer file-sharing or messaging apps (WhatsApp, WeTransfer, etc.).
    - Unencrypted USB or external storage.

9.4 International Data Transfers

Where personal data is transferred outside the UK (including to the EU):

- An **adequacy decision** or appropriate legal mechanism must be in place (Standard Contractual Clauses, Binding Corporate Rules, etc.).
- The **DPO must be consulted and approve** the transfer.
- Data subjects must be notified where required.
- Records of Processing Activities must document the transfer safeguards.

See **Section 14 – International Data Transfers** of the Data Protection and Confidentiality Policy for full details.

9.5 Secure Deletion and Anonymisation

When retention periods expire or when data is no longer needed:

- Data must be **securely deleted** or **irreversibly anonymised** in accordance with **Section 10.3 of the Data Protection and Confidentiality Policy**.
- Secure deletion methods must be appropriate to the data type and sensitivity:
    - Paper records: cross-cut shredding, incineration, or secure disposal service.
    - Electronic data: cryptographic deletion, overwriting (multi-pass), degaussing or secure hard drive destruction.
    - Databases: secure deletion of records with verification of permanent removal.
- Backup and archive copies must be identified and managed to prevent unintended retention.
- Deletion must be recorded in the data management system or audit trail.
- Data subjects may be notified of deletion if required by the Data Protection and Confidentiality Policy.

---

10. Information Security and Incident Management

10.1 Technical Controls

RHS implements the **technical measures** described in **Section 11.1 of the Data Protection and Confidentiality Policy**, including:

- **Encryption:**
    - Data at rest: AES 256-bit or equivalent
    - Data in transit: TLS 1.2 or higher
    - End-to-end encryption for sensitive communications

- **Access Controls:**
    - Role-based access control (RBAC)
    - Principle of least privilege
    - Multi-factor authentication (MFA) for sensitive systems
    - Secure password policies (minimum 12 characters)
    - Regular password resets
    - Automatic session timeouts (15 minutes for public areas, 30 minutes for clinical data)
- **System Security:**
    - Firewalls and intrusion detection systems
    - Antivirus and anti-malware protection
    - Regular vulnerability scanning and patching
    - Software kept up to date with security patches
    - Secure configuration standards
    - Regular security updates and maintenance
- **Backup and Disaster Recovery:**
    - Automated daily backups
    - Off-site backup storage (geographically separate)
    - Tested recovery procedures
    - Ransomware protection and detection measures
- **Network Security:**
    - Secure Wi-Fi (WPA2/WPA3 encryption)
    - VPN for remote working
    - Network segmentation (separating clinical, HR and financial data)
    - Monitoring and alerting for suspicious activity

10.2 Organisational and Procedural Controls

RHS implements the **organisational measures** described in **Section 11.2 of the Data Protection and Confidentiality Policy**, including:

- **Policies and Procedures:**
    - Information Security Policy
    - Incident Response Procedure
    - Data Breach Notification Procedure
    - Clean Desk Policy
    - Clear Screen Policy

- **Personnel Security:**
    - Disclosure and Barring Service (DBS) checks and background verification
    - Confidentiality agreements (signed on joining)
    - Data protection and IT security training
    - Disciplinary procedures for breaches
    - Exit procedures and access removal for leavers
- **Physical Security:**
    - Locked filing cabinets for paper records
    - Secure disposal facilities (cross-cut shredders, secure disposal services)
    - Access control to buildings and sensitive areas
    - CCTV where lawful and appropriate
    - Visitor management and signing-in procedures
    - Identification or badge systems for staff
- **Vendor and Third-Party Management:**
    - Data Processing Agreements with all processors
    - Vendor security assessments and due diligence
    - Contract terms requiring security measures and compliance
    - Regular audits and compliance checks
    - Sub-processor approval requirements

10.3 Staff Responsibilities for Security

All users must:

- Use Company devices and software only for authorised, lawful business purposes.
- Not disable, circumvent, bypass or defeat antivirus, firewalls, access controls or security tools.
- Keep operating systems, software and applications up to date with security patches.
- Be cautious with emails, especially:
    - Unsolicited messages from unknown senders
    - Messages requesting passwords, personal data or system access
    - Attachments from untrusted sources
    - Links to unfamiliar websites
    - Emails claiming to be from banks, IT support or management with urgent requests
- Not open suspicious attachments or click on suspicious links.
- Not download unauthorised software or applications.
- Promptly report suspected phishing, malware, security incidents or system anomalies.

10.4 Incident and Breach Reporting

Any suspected or confirmed incident affecting IT systems, data security, confidentiality or integrity must be reported **immediately** via:

- **Immediate verbal report** to line manager and IT
- **Written incident report** to:
    - Data Protection Officer: maz.manager@responseheathcare.co.uk, 07588 444915
    - Senior management or nominated incident coordinator
- **Do not delay** reporting; early reporting allows faster containment and mitigation.

What to report:

- Suspected unauthorised access to systems or data
- Loss or theft of devices, equipment, documents or storage media
- Suspected malware, ransomware or virus infection
- Phishing or social engineering attempts
- Breaches of confidentiality (unauthorised disclosure, discussion of clients/staff in public, etc.)
- Suspected unauthorised recording or surveillance
- System failures, downtime or data corruption
- Suspicious user activity or access
- Physical security breaches (door left open, badge missing, etc.)

Incident Investigation and Response:

The **DPO and IT will:**

- Investigate the incident promptly
- Contain and mitigate the breach to prevent further harm
- Assess the risk to data subjects and RHS
- Determine if regulatory notification is required (ICO, Care Inspectorate)
- Notify affected data subjects if there is high risk (Section 12 of the Data Protection and Confidentiality Policy)
- Document the incident, investigation and remediation
- Implement preventative measures to reduce recurrence risk

See **Section 12 – Data Protection Breaches** of the Data Protection and Confidentiality Policy for full breach reporting requirements.

10.5 Consequences of Security Breaches

- **Negligent breaches** (carelessness, failure to follow procedures) may result in:
    - Retraining and supervision

    - Disciplinary action (written warning, suspension, etc.)
    - Mandatory refresher training
- **Deliberate or reckless breaches** (intentional security bypass, deliberate disclosure, unauthorised recording) may result in:
    - Summary dismissal without notice
    - Investigation by police for criminal offences
    - Civil action by affected parties (privacy claims, defamation, etc.)
    - Referral to professional regulatory bodies (GMC, NMC, HCPC, social work bodies)
    - Personal financial liability for damages and legal costs

All breaches will be investigated, documented and considered in disciplinary proceedings per **Section 20 of the Data Protection and Confidentiality Policy**.

---

11. Training, Monitoring and Audit

11.1 Training Requirements

All staff must complete:

Induction Training (before commencing work):

- Data Protection and Confidentiality Policy overview
- IT security and safe use of systems
- Password and access control best practice
- Phishing and social engineering awareness
- Incident and breach reporting procedures
- Acknowledgement of this Policy and Data Protection and Confidentiality Policy

Annual Refresher Training:

- Data protection and confidentiality principles
- IT security updates and new threats
- Social media and communication responsibilities
- Incident reporting
- Case studies of real breaches and lessons learned

Targeted Training:

- New systems or technology implementation
- Following security incidents or breaches
- For roles handling particularly sensitive data (clinical, HR, financial)

Records:

- Training completion will be recorded, monitored and reported to management.
- Non-completion may be addressed through disciplinary procedures.
- Training records will be retained per retention schedules.

11.2 Monitoring

Subject to employment law, data protection law and human rights law, RHS may monitor IT and communications usage for:

- Security and data protection compliance
- Investigation of suspected misconduct or policy breaches
- Regulatory or legal requirements (e.g. HMRC, Care Inspectorate requests)
- Prevention and detection of crime
- Performance and productivity management

Monitoring activities may include:

- Email headers and metadata (sender, recipient, subject, size, date/time), though not routinely the content of business emails (content review may occur following incident or suspected breach).
- Internet access logs and blocked/suspicious websites
- System access logs (who logged in, when, what data accessed)
- Call logs and metadata (duration, participant identities)
- Device usage logs (applications, files accessed)
- Network traffic analysis for security threats
- Physical access logs (badge swipes, CCTV)

Monitoring principles:

- Targeted and proportionate, not blanket surveillance
- Documented and subject to oversight by line management or DPO
- Compliant with the **Investigatory Powers Act 2016** and **Employment Rights Act 1996**
- Not used for harassment, discrimination or excessive control
- Communicated to staff via this Policy and privacy notices
- Personal data in monitoring logs protected under data protection law

Legitimate purposes for email/content review:

- Suspected breach of confidentiality or unauthorised disclosure
- Investigation of alleged misconduct (e.g. discrimination, harassment, bullying, theft, gross negligence)
- Criminal investigation by police (with proper legal authority)
- Regulatory investigation (with proper legal authority)

- Subject Access Request from the staff member themselves

11.3 Audit and Compliance

Regular Audits:

- Periodic audits (at least annually) will assess:
    - IT security controls (firewalls, antivirus, patches, MFA)
    - Access control (appropriate access based on role, timely removal when roles change)
    - Data protection compliance (retention, deletion, third-party disclosure)
    - Incident response and breach notification procedures
    - Training completion and effectiveness
    - Policy compliance by staff sample
- Audits may be conducted by:
    - Internal IT and Data Protection teams
    - External auditors or security specialists
    - Regulatory bodies (Care Inspectorate, CQC)

Audit Findings:

- Findings will be reported to management and the Board.
- Non-conformances will result in:
    - Remediation action plans
    - Retraining where needed
    - Disciplinary action for serious breaches
    - Improvements to systems and controls
- Audit records will be retained per retention schedules.

---

12. Disciplinary Framework and Fairness

12.1 Disciplinary Action for Policy Breaches

Breaches of this Policy will be managed under the **disciplinary framework** set out in **Section 20 of the Data Protection and Confidentiality Policy**.

Severity and Outcomes:

- **Minor breaches** (e.g. first instance of non-compliance with guidance, careless security error):
    - Verbal warning and retraining
    - Supervision for a period
    - Documented in personnel file
- **Serious breaches** (e.g. repeated breaches despite warnings, reckless security failures, unauthorised access to data):
    - Written warning
    - Mandatory refresher training
    - Potential suspension
    - Disciplinary hearing
- **Gross misconduct** (summary dismissal offences):
    - Unauthorised recording (personal devices)
    - Deliberate or reckless confidentiality breach (unauthorised disclosure)
    - Deliberate security bypass or system damage
    - Intentional misuse of access rights or accessing data outside role
    - Deliberate failure to report a breach
    - Using personal messaging platforms for confidential information knowingly
    - Creating, distributing or possessing illegal or defamatory content

Gross misconduct allegations may also result in:

- **Immediate suspension** pending investigation
- **Summary dismissal** without notice and without pay in lieu
- **Police referral** for criminal investigation
- **Referral to professional regulatory bodies** (GMC, NMC, HCPC, social work bodies)
- **Civil legal claims** by affected individuals

12.2 Procedural Safeguards and Fairness

All investigations and disciplinary actions will strictly follow the procedural protections set out in **Sections 21–24 of the Data Protection and Confidentiality Policy**, ensuring:

- **Clear, specific notice** of allegations or concerns.
- **Reasonable time to respond** (minimum 5 working days) with supporting evidence.
- **Right to be accompanied** at disciplinary meetings by a colleague, friend or union representative (if eligible).
- **Right to present evidence** and to question witnesses where relevant.
- **Impartial investigator and decision-maker** (usually different people).

- **Right to appeal** to a senior manager or Board member not involved in the original decision.
- **Written explanation** of outcomes and any sanction imposed.

These protections do not prevent **immediate action to protect people, data or systems** (e.g. immediate access removal for a serious security breach).

12.3 Criminal and Regulatory Referral

Staff should be aware that serious breaches of this Policy may result in:

- **Criminal prosecution** (e.g. unauthorised access under Computer Misuse Act 1990, privacy breaches under common law, offences under Regulation of Investigatory Powers Act 2000, breaches of Data Protection Act 2018).
- **Referral to professional regulatory bodies** (NMC, GMC, HCPC, social work bodies) which may lead to:
    - Investigations and hearings
    - Suspension or removal from register
    - Loss of professional qualification
- **Civil claims** by affected parties for damages (breach of confidence, defamation, privacy rights, etc.).

---

13. Policy Governance

13.1 Policy Owner

This Policy is owned and maintained by:

- **Data Protection Officer:** Mazher Khan
- **Role:** Responsible for content, updates and alignment with data protection law, UK GDPR, Data Protection Act 2018, and Scottish health and social care regulations.
- **Contact:** maz.manager@responseheathcare.co.uk, 07588 444915

13.2 Policy Approval

This Policy is approved by:

- **Data Protection Officer:** Mazher Khan (Data Protection compliance)
- **Operations Officer:** [Name] (Operations oversight)
- **Senior Management / Board Representative:** [Name] (Board governance)

Date of Approval: June 2025

13.3 Policy Review Schedule

This Policy will be reviewed:

- **Annually:** at minimum each June (aligned with Data Protection and Confidentiality Policy review cycle).
- **Following legislative changes:** when UK GDPR, Data Protection Act 2018, Health and Social Work (Scotland) Act 2015, Care Inspectorate standards or other relevant law changes.
- **Following significant incidents or breaches:** to identify gaps and implement improvements.
- **Following organisational changes:** when systems, services, staffing or structure materially change.
- **Following external recommendations:** by Care Inspectorate, CQC, ICO, auditors or other regulatory bodies.

Changes and updates will be documented, communicated to staff and recorded.

13.4 Communication and Staff Acknowledgement

Availability:

This Policy will be made available to all staff via:

- Staff intranet or shared drive
- Printed copy on request
- HR or management offices
- Induction packs for new staff

Staff Acknowledgement:

All staff must acknowledge they have read, understood and will comply with this Policy via:

- **Electronic acknowledgement** in the HR system or learning platform, or
- **Signed acknowledgement form** appended to employment contract or retained in personnel file.

Failure to acknowledge this Policy does not exempt any individual from compliance. All employees are expected to comply regardless of acknowledgement status.

13.5 Related Policies and Documents

This Policy should be read alongside:

- **Data Protection and Confidentiality Policy** (June 2025) – primary policy on legal compliance and confidentiality
- **Disciplinary Policy** – framework for investigation and disciplinary action
- **Data Breach Notification Procedure** – process for reporting and managing breaches
- **Information Security Policy** – technical and security standards
- **Acceptable Use Policy** (if separate IT policy exists)
- **Data Protection and Privacy Notices** – communications to data subjects

- **Records Retention Schedule** – specific retention periods for different data categories
- **Data Processing Agreements** – contracts with processors

In the event of conflict between policies, the **Data Protection and Confidentiality Policy (June 2025)** takes precedence for data protection and confidentiality matters.

---

14. Policy Statement and Commitment

Response Healthcare Solutions Ltd is committed to:

- **Protecting confidentiality and privacy** of all individuals (clients, patients, service users, staff, contractors) whose information we hold.
- **Complying fully** with UK GDPR, Data Protection Act 2018, Health and Social Work (Scotland) Act 2015, Care Inspectorate standards and Scottish law.
- **Using technology safely and securely** to support high-quality, person-centred care.
- **Ensuring every staff member understands their responsibilities** for data protection, IT security and confidentiality.
- **Investigating and addressing breaches** promptly and fairly, and taking corrective action to prevent recurrence.
- **Maintaining transparent, accountable processes** for managing personal data and responding to data subject rights requests.
- **Supporting staff** with training, guidance and clear procedures to enable compliance.
- **Cooperating with regulators** (Care Inspectorate, ICO, Police, NHS) when required.

This Policy reflects our organisational values of **dignity, respect, compassion and inclusion**, as set out in the Health and Social Care Standards: My support, my life.

---

15. Policy Review and Version Control

Version	Date Issued	Review Date	Changes / Notes
1.0	June 2025	June 2026	Policy creation, aligned to Data Protection and Confidentiality Policy (June 2025), Care Inspectorate standards and Scottish Health and Social Care Standards.

Appendices

Appendix A: Contact Information

Data Protection Officer:

- **Name:** Mazher Khan
- **Email:** maz.manager@responseheathcare.co.uk
- **Telephone:** 07588 444915
- **Address:** Office 2.6, 1 Barrack Street, Hamilton, ML3 0DG

Senior Management:

- **[Name]** – Operations Officer
- **[Name]** – [Other leadership role]

Subject Access Requests (SAR):

- Email: admin@responsehealthcare.co.uk
- Post: Office 2.6, 1 Barrack Street, Hamilton, ML3 0DG

Information Commissioner's Office (ICO) – Data Protection Authority:

- **Website:** www.ico.org.uk
- **Telephone:** 0303 123 1113
- **Address:** Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
- **Email:** casework@ico.org.uk

Care Inspectorate (Scotland):

- **Website:** www.careinspectorate.com
- **Telephone:** 0345 600 9527
- **Email:** enquiries@careinspectorate.com

Appendix B: Staff Acknowledgement Form

IT AND COMMUNICATION POLICY – STAFF ACKNOWLEDGEMENT

I acknowledge that I have received, read and understood the IT and Communication Policy (June 2025) of Response Healthcare Solutions Ltd.

I understand and agree that:

- I must comply with this Policy and the Data Protection and Confidentiality Policy in all my work.

- Failure to comply may result in disciplinary action up to and including dismissal.
- I am personally responsible for protecting confidential information and data security.
- I must report any suspected breaches or incidents immediately.
- I have received appropriate training and support to enable compliance.

I have had the opportunity to ask questions and receive clarification.

Staff Name: [Print]
Job Title: [Insert]
Employment Start Date: [Insert]

Signature: _____
Date: _____

Line Manager Name: [Print]
Line Manager Signature: _____

To be retained in personnel file.

Appendix C: Incident Report Template

DATA PROTECTION AND IT SECURITY INCIDENT REPORT

To be completed by the person discovering the incident and submitted immediately to the Data Protection Officer and line manager.

Incident Details:

- **Date/Time of Incident:** [Insert]
- **Date/Time Reported:** [Insert]
- **Your Name/Title:** [Insert]
- **Reported To:** [Names and titles of recipients]

Incident Description:

(Describe what happened, who was involved, what data or systems were affected)

[Insert description]

Type of Incident (tick all that apply):

- □ Unauthorised access to systems or data
- □ Loss or theft of device or documents
- □ Suspected malware or system compromise
- □ Suspected unauthorised disclosure of confidential information
- □ Suspected unauthorised recording or surveillance
- □ Phishing or social engineering

- □ Breach of password or authentication security
- □ Physical security breach
- □ Other (please describe): [Insert]

Data or Systems Affected:

- **Systems:** [Insert]
- **Data Types:** [Insert – e.g. client names and addresses, health information, employee records]
- **Approximate Number of People Affected:** [Insert]

Immediate Actions Taken:

[Describe any containment or mitigation steps already taken]

Suspected Cause:

[Describe how the incident may have occurred, if known]

Contact for Further Information:

- **Name:** [Insert]
- **Phone:** [Insert]
- **Email:** [Insert]

Report Signature: _____
Date/Time: _____

For DPO Use:

- **Incident Severity Assessment:** [Low / Medium / High / Critical]
- **Requires Investigation:** [Yes / No]
- **Requires Breach Notification:** [Yes / No / Pending]
- **Requires Regulatory Notification:** [Yes / No / Pending]
- **Investigation Lead:** [Name]
- **Initial Actions:** [Describe]

DPO Signature: _____
Date: _____

Appendix D: Email and Data Transfer Security Checklist

Use this checklist before sending emails or documents containing personal data or confidential information.

Pre-Send Checklist:

- [ ] **Recipient Verification:** Have I verified the recipient(s) are correct and authorised to receive this information? (Not to wrong email address or person?)
- [ ] **Data Minimisation:** Have I included only the minimum personal data necessary? (Avoided unnecessary names, addresses, health details, financial information?)
- [ ] **Necessity:** Is it necessary to send this data to this recipient? (Lawful basis exists – consent, contract, legal obligation, legitimate interest, vital interests, public task?)
- [ ] **Encryption:** If data is sensitive (health, financial, special category), have I encrypted the email or used secure transfer method?
    - [ ] Email encrypted and password sent separately?
    - [ ] Using NHS secure email or approved secure portal?
    - [ ] Using approved secure file transfer service?
- [ ] **Attachments:** Have I checked:
    - [ ] All attachments are intended and necessary?
    - [ ] File names do not disclose sensitive information?
    - [ ] Attachments are encrypted/password-protected if needed?
    - [ ] I'm not sending unnecessarily large files?
- [ ] **Third-Party Disclosure:** If sending to external organisation, have I:
    - [ ] Confirmed lawful basis for disclosure?
    - [ ] Verified the recipient is authorised?
    - [ ] Used secure transfer method?
    - [ ] Considered Data Processing Agreement or Data Sharing Agreement?
- [ ] **Accidental Disclosure Prevention:** Have I:
    - [ ] Used "Draft" or "Unsend" features in email system if available?
    - [ ] Been extra careful not to include sensitive information in subject line?
    - [ ] Avoided including names in subject line where possible?
    - [ ] Used "To" (not "Reply All" or "CC") to limit recipients?
- [ ] **Retention:** Have I:
    - [ ] Saved a copy to the appropriate work folder for record-keeping?
    - [ ] Set a retention reminder for deletion when no longer needed?
- [ ] **Disclaimer:** Does the email include an appropriate confidentiality disclaimer?

If you answer "No" to any of these, do not send. Seek guidance from your line manager or DPO.

Appendix E: Data Subject Rights Quick Reference

This summary outlines data subjects' key rights under UK GDPR. Full details are in the Data Protection and Confidentiality Policy (Section 4).

Right	What Does It Mean?	How to Request	Response Time
Right to be Informed	Must be told clearly how and why we use your data.	Privacy notice provided at point of collection.	N/A – ongoing
Right of Access (SAR)	Can request copy of all personal data RHS holds about them.	Written request to: maz.manager@responseheathcare.co.uk or admin@responsehealthcare.co.uk	1 calendar month (extendable to 3 months)
Right to Rectification	Can ask for inaccurate or incomplete data to be corrected.	Written request via DPO (contact details above).	Without undue delay
Right to Erasure	Can ask for data to be deleted.	Written request via DPO.	Without undue delay
Right to Restrict Processing	Can ask for processing to be paused/limited.	Written request via DPO.	Without undue delay
Right to Data Portability	Can request data in portable format, or transfer to another organisation.	Written request via DPO.	1 calendar month
Right to Object	Can object to processing (e.g. for marketing, automated decisions).	Written request via DPO.	Without undue delay
Rights in Automated Decision-Making	Can request human review of automated decisions affecting them.	Written request via DPO.	Without undue delay
Right to Lodge a Complaint	Can complain to the Information Commissioner's Office (ICO).	Contact ICO directly: www.ico.org.uk, 0303 123 1113	ICO's procedures apply

Data Subject Contact Details:

- **Data Protection Officer:** Mazher Khan, maz.manager@responseheathcare.co.uk, 07588 444915
- **Postal Address:** Office 2.6, 1 Barrack Street, Hamilton, ML3 0DG
- **Subject Access Requests:** admin@responsehealthcare.co.uk

END OF POLICY