GDPR Policy

Response Healthcare Solutions Ltd

Date of Issue: June 2025

Policy Review Date: June 2026

Document Classification: Internal - Confidential

Status: Approved

---

1. Introduction and Purpose

1.1 Policy Overview

This General Data Protection Regulation (GDPR) Policy sets out the legal and ethical obligations of Response Healthcare Solutions Ltd ("RHS", "the Company") and its employees, contractors, volunteers, and agents regarding the processing, protection, and confidential handling of personal data, health information, and sensitive information in compliance with the UK GDPR and associated legislation.

1.2 Legal Framework

This Policy is established to ensure compliance with:

- General Data Protection Regulation (UK GDPR) - as retained in UK law post-Brexit
- Data Protection Act 2018 (including Schedule 3 for health and social care provisions)
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 and subsequent amendments
- Health and Social Work (Scotland) Act 2015 and relevant Scottish Health and Care Standards
- Public Services Reform (Scotland) Act 2010 - particular relevance to Care Inspectorate standards
- Data (Use and Access) Act 2025 - including digital information standards for health and social care
- The Common Law Duty of Confidentiality
- Home Office Statutory Guidance on Records Retention - particularly regarding right to work and compliance documentation
- Care Inspectorate Standards and Guidance - statutory requirements for registered social care services in Scotland
- Human Rights Act 1998 - Article 8: Right to respect for private and family life
- General Data Protection Regulation (Overseas Transfers) Regulations 2019 - where applicable

1.3 Scope of Application

This Policy applies to:

- All employees of RHS, whether permanent, temporary, contract-based, or casual
- All workers engaged on agency, consultancy, or zero-hours arrangements
- All volunteers and students on placement
- All contractors and service providers processing personal data on behalf of RHS
- All external parties accessing RHS systems or facilities
- All individuals involved in RHS service delivery and operations
- Board members and governing bodies

The Policy applies to all personal data and sensitive information processed by RHS, regardless of the form, medium, or location of storage (paper, electronic, cloud-based, mobile devices, etc.).

1.4 Key Definitions

Personal Data: Any information relating to an identified or identifiable natural person. Includes name, identification number, location data, online identifier, factors specific to physical, physiological, genetic, mental, economic, cultural or social identity.

Special Category Data (Sensitive Data): Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation.

Health Data: Personal data relating to the health of an individual, including physical or mental health conditions, treatments, diagnoses, disabilities, medical history, and information about health services.

Processing: Any operation performed on personal data including collection, recording, storage, retrieval, use, disclosure, transmission, or deletion.

Data Controller: The natural or legal person who determines the purposes and means of processing personal data. For RHS purposes, the Company is the Data Controller.

Data Processor: A natural or legal person processing personal data on behalf of a Data Controller.

Data Subject: The individual to whom personal data relates.

Confidential Information: Any information about individuals, clients, service users, patients, employees, or business operations that is not publicly available and is entrusted to the organisation.

Employee: For the purposes of this Policy, includes all workers regardless of employment status including employees, contractors, volunteers, agency staff, and temporary workers.

———

2. GDPR Core Principles (Article 5)

RHS commits to processing all personal data in accordance with the six core principles mandated by Article 5 of the UK GDPR:

2.1 Lawfulness, Fairness and Transparency

- All personal data processing must have a lawful basis (Article 6)
- Processing must be fair and transparent
- Data subjects must be informed about processing activities
- Information must be provided in clear, accessible language
- No deceptive or misleading practices permitted
- Processing must not be arbitrary or discriminatory

2.2 Purpose Limitation

- Personal data must be collected for specified, explicit and legitimate purposes
- Data cannot be further processed for purposes incompatible with original collection purposes
- Archiving for public interest, scientific research, historical research, or statistical purposes are permitted exceptions subject to appropriate safeguards
- Any new purpose requires clear legal basis and may require new privacy information

2.3 Data Minimisation

- Personal data collected must be adequate, relevant, and limited to what is necessary
- Excessive data collection is prohibited
- Only collect information actually required for specified purposes
- Regular reviews ensure data holdings remain necessary
- Minimise special category data collection

2.4 Accuracy

- Personal data must be accurate and kept up to date
- Reasonable steps must be taken to rectify inaccurate data
- Data subjects have the right to request correction of inaccurate information
- Context must be maintained - incomplete data cannot be misused
- Outdated data must not be used for decisions affecting data subjects

2.5 Storage Limitation

- Personal data kept in a form which permits identification of data subjects must not be kept longer than necessary
- RHS maintains specific retention schedules for different categories of data
- Retention periods comply with health and social care sector requirements
- Archived data must be protected with equivalent safeguards
- Regular review and secure deletion required

2.6 Integrity and Confidentiality

- Personal data must be processed securely
- Appropriate technical and organisational measures must protect against unauthorised processing
- Protection against accidental loss, destruction, or damage required
- All employees must maintain strict confidentiality
- Only personnel with legitimate need-to-know may access personal data
- Confidentiality obligations survive termination of employment

2.7 Accountability

RHS maintains:

- Clear records of all processing activities (Records of Processing Activities)
- Data Protection Impact Assessments (DPIA) for high-risk processing
- Regular compliance audits and monitoring
- Training records demonstrating staff understanding
- Incident investigation and reporting records
- Documentation of legal bases for processing
- Consent records where applicable

---

3. Lawful Basis for Processing (Article 6)

Processing of personal data is only lawful where at least one of the following applies:

3.1 Consent

- The data subject has given clear, specific, informed, and unambiguous consent
- Consent must be freely given - no pressure or coercion
- Consent must be separate from other matters

- Withdrawal of consent must be as easy as provision
- Particularly important for special category data processing
- RHS maintains records of all consent obtained

3.2 Contract

- Processing is necessary to enter into or perform a contract with the data subject
- Includes employment contracts with employees
- Includes service contracts with clients and service users

3.3 Legal Obligation

- Processing is necessary to comply with legal obligations binding on the Company
- Includes statutory health and safety duties
- Includes regulatory reporting obligations to Care Inspectorate
- Includes financial and tax obligations to HMRC
- Includes employment law obligations
- Includes retention requirements under Home Office regulations for right-to-work documentation

3.4 Protection of Vital Interests

- Processing is necessary to protect vital interests of a data subject or another natural person
- Applies in emergency situations where life or physical integrity is threatened
- Rarely used but essential for safeguarding situations

3.5 Performance of a Public Task

- Processing is necessary for performance of official functions or public task with legal basis
- For health and social care providers, includes care delivery and service commissioning
- Particularly relevant to Scottish registered services

3.6 Legitimate Interests

- Processing is necessary for legitimate interests pursued by the Company
- Legitimate interests must be balanced against data subject rights and freedoms
- Three-step test: identify interest, demonstrate necessity, balance against data subject rights
- Health and safety of employees is a legitimate interest
- Security of premises and data systems is a legitimate interest
- Prevention and detection of fraud is a legitimate interest
- RHS maintains records of Legitimate Interest Assessments

3.7 Special Category Data Processing

Processing of special category data (including health data) is prohibited unless one of 10 specified exceptions applies:

- **Explicit Consent:** where data subject has given explicit consent
- **Employment Law:** processing necessary to exercise employment law obligations
- **Vital Interests:** protection of vital interests where data subject unable to consent
- **Data Published by Data Subject:** where data subject has manifestly made it public
- **Legal Claims:** exercise or defence of legal claims
- **Substantial Public Interest:** certain conditions met as specified in schedule 1 DPA 2018
- **Health and Social Care:** necessary for healthcare or occupational health purposes (Schedule 3 DPA 2018)
- **Public Health:** necessary for public health interests under Schedule 3 DPA 2018
- **Safeguarding:** protection of children or vulnerable persons under Schedule 3 DPA 2018

- **Security and Crime Prevention:** prevention or detection of crime under Schedule 3 DPA 2018

---

4. Data Subject Rights

Data subjects are entitled to exercise the following rights under the UK GDPR:

4.1 Right to be Informed

Data subjects have the right to receive clear, transparent information about processing:

- Information provided at point of collection
- Privacy notices explaining purposes, legal basis, recipients, retention, and data subject rights
- Information provided in concise, transparent, intelligible manner
- Available in plain language and clear format
- Specific information requirements where data not obtained from data subject
- Information refreshed at appropriate intervals

RHS provides privacy notices to:
- Clients and service users receiving care services
- Patients and health service users
- Employees and workers
- Contractors and service providers
- Volunteers and students

4.2 Right of Access (Subject Access Request - Article 15)

Data subjects may request access to personal data RHS holds about them:

- Requests must be responded to within one calendar month of receipt (extendable to 3 months for complex requests)
- Information provided in commonly used electronic format where possible
- Information provided in clear, understandable language
- RHS may request reasonable further information to verify identity
- Identifiable information of third parties may be withheld unless consent obtained
- Access provided free of charge unless requests manifestly unfounded or excessive
- RHS maintains request records and response documentation

4.3 Right to Rectification (Article 16)

Data subjects may request correction of inaccurate or incomplete personal data:

- RHS must rectify inaccurate data without undue delay
- Data subjects may request that incomplete data is supplemented
- RHS provides statement of action taken in response to rectification request
- Third parties previously notified of inaccurate data must be informed of rectification where possible
- RHS maintains records of all rectification requests

4.4 Right to Erasure/Right to be Forgotten (Article 17)

Data subjects may request deletion of their personal data:

- Must be granted where data is no longer necessary for original purpose
- Must be granted where data subject withdraws consent
- Must be granted where data subject objects to processing
- Must be granted where processing unlawful
- Must be granted where legal obligation to delete exists

- May be refused where data retention required for legal compliance or other lawful grounds
- RHS maintains records of erasure requests and outcomes

4.5 Right to Restrict Processing (Article 18)

Data subjects may request that processing be suspended:

- Applies where data subject contests accuracy of data
- Applies where data subject objects to processing
- Applies where RHS no longer needs data but data subject requires retention for legal claim
- Applies where data subject has objected to processing pending verification of legitimate interests
- RHS may only process restricted data for storage or with consent
- RHS maintains records of restriction requests

4.6 Right to Data Portability (Article 20)

Data subjects may request their personal data in structured, commonly used, machine-readable format:

- Available where processing based on consent or contract
- Data provided in portable electronic format
- Data provided directly to data subject
- Data provided to another controller where technically feasible
- Right does not extend to data derived from processing
- RHS maintains records of portability requests

4.7 Right to Object (Article 21)

Data subjects may object to processing for legitimate interests or public task purposes:

- RHS must stop processing unless can demonstrate compelling legitimate grounds
- RHS must stop processing for direct marketing without exception
- Data subjects must be informed of right to object in all communications
- RHS maintains records of objection requests

4.8 Rights in Relation to Automated Decision-Making (Article 22)

Data subjects have rights regarding automated decision-making and profiling:

- Automated decision-making affecting legal rights requires human intervention
- Profiling on the basis of special category data prohibited except in limited circumstances
- Data subject has right to explanation of automated decisions
- Data subject may challenge automated decisions
- RHS ensures humans review algorithmic decisions before implementation

4.9 Exercising Rights

Data subjects may exercise rights by:

- Written request to: Data Protection Officer, Response Healthcare Solutions Ltd, Office 2.6, 1 Barrack Street, Hamilton, ML3 0DG
- Email to: maz.manager@responseheathcare.co.uk
- Telephone to: 07588444915

Requests must identify data subject and specify which right(s) are being exercised. RHS responds without undue delay and provides evidence of action taken.

———

5. Employee Recording and Confidentiality Obligations

5.1 Prohibition on Unauthorised Recording

5.1.1 Complete Prohibition on Personal Device Recording

Employees are strictly prohibited from:

- Recording audio, video, or any other content on personal mobile devices, phones, tablets, laptops, or any personal technology
- Making recordings using any personal equipment of:
  - Clients, service users, or patients (regardless of consent)
  - Other employees or colleagues
  - Visitors or third parties on RHS premises
  - Any RHS services, operations, activities, or communications
  - Any meetings, training, or briefings
  - Any confidential information or data

This prohibition applies without exception regardless of:

- Stated purpose or intention
- Whether recording is "for personal use only"
- Whether consent from recorded parties has been obtained
- Whether recording is for "safeguarding purposes"
- Whether employee believes the recording is in the public interest
- Any claim that recording is necessary for employment protection

Breach of this prohibition will result in disciplinary action up to and including immediate dismissal without notice.

5.1.2 Legal Basis for Recording Prohibition

Recording on personal devices without explicit authorisation constitutes:

- GDPR Violation - Unauthorised processing of personal data violating Article 5 principles (lawfulness, transparency, purpose limitation)
- Data Protection Act 2018 Breach - Unlawful processing of personal data, potentially including special category data
- Breach of Duty of Confidentiality - Violation of common law and contractual confidentiality obligations
- GDPR Article 3 Violation - Covert recording negates the fundamental principle of transparency
- Potential Criminal Offence - May constitute offence under Regulation of Investigatory Powers Act 2000 or common law
- Workplace Rights Violation - Infringement of colleagues' right to work in safe environment free from covert surveillance
- Potential Defamation Liability - Personal recording may create liability for defamatory content
- Employment Contract Breach - Violation of standard employment contract confidentiality clauses
- Professional Standards Breach - Where applicable, breach of healthcare professional codes of conduct (GMC, NMC, HCPC, etc.)

Employees who make unauthorised recordings may face:

- Criminal prosecution

- Civil legal action by affected parties
- Disciplinary action including dismissal
- Referral to professional regulatory bodies
- Loss of professional qualifications or registration
- Personal financial liability for damages

5.1.3 Distinction: Authorised Recording

Where recording is necessary and lawful, explicit authorisation must be obtained:

- Recording only permitted where:
  - Clear business need exists (e.g., quality assurance, training, safeguarding)
  - Written approval obtained from Data Protection Officer and Senior Management
  - Legal basis clearly documented and justified
  - All data subjects informed in advance and consent obtained in writing
  - Recording conducted using approved Company equipment only
  - Technical and organisational security measures implemented
  - Data retention schedule maintained
  - Records of Processing Activity completed

- Authorised recordings require:
  - GDPR Lawful Basis assessment
  - Legitimate Interest Assessment (LIA)
  - Consent documentation (where applicable)
  - Data Protection Impact Assessment (DPIA)

The complete prohibition above applies to all personal device recording. Authorised recording is limited to specific operational circumstances and requires DPO approval.

5.2 Confidentiality Obligations

5.2.1 Confidentiality Requirement

All employees are required to maintain strict and absolute confidentiality regarding:

- All information about clients, service users, and patients
- All health and care records and clinical information
- All employee personal data and HR information
- All financial and business information
- All supplier and partner information
- All system access credentials and passwords
- All strategic, operational, and planning information
- All information obtained in the course of employment
- Any information not publicly available or formally designated as non-confidential

This confidentiality obligation:

- Applies during employment and survives indefinitely after termination
- Applies regardless of whether information is classified as "confidential"
- Applies regardless of physical form (paper, electronic, verbal, etc.)
- Applies to all conversations, meetings, emails, and communications
- Cannot be waived or overridden except by explicit senior management written authorisation
- Is a strict liability obligation - careless disclosure is as serious as intentional

5.2.2 Third-Party Disclosure Prohibition

Employees are absolutely prohibited from:

- Disclosing any personal data, confidential information, or client information to any third party
- Sharing information with family members, friends, or social contacts
- Posting information on social media platforms (Facebook, Twitter, LinkedIn, Instagram, TikTok, etc.)
- Discussing specific clients, patients, or service users in public places, on public transport, or where others may overhear
- Sharing information via WhatsApp, Telegram, Signal, or other messaging applications
- Forwarding emails or documents to personal email accounts
- Discussing employment matters with media or journalists
- Speaking to external organisations about RHS activities without authorisation
- Disclosing information to solicitors, regulatory bodies, or investigators without authorisation from senior management or legal counsel
- Any form of "whistleblowing" outside formal RHS channels

Exceptions only exist for:

- **Public Interest Disclosure:** Protected disclosures to regulator or law enforcement (Care Inspectorate, CQC, Police) where genuine safeguarding concern exists AND made through formal channels with legal advice
- **Legal Process:** Disclosures compelled by court order, tribunal order, or statutory legal process (with immediate notification to RHS)
- **Whistleblowing Protection:** Limited protection under Employment Rights Act 1996 for qualifying disclosures made in good faith through prescribed procedures
- **Data Subject Requests:** Disclosures made in response to lawful data subject requests for their own information

Unauthorised third-party disclosure will result in:

- Immediate disciplinary action including summary dismissal
- Potential legal action for damages
- Referral to police for criminal investigation
- Referral to professional regulatory body
- Personal liability for breaches of confidentiality
- Potential criminal prosecution under Computer Misuse Act 1990 or Data Protection Act 2018

5.2.3 Solicitation and Third-Party Requests

Employees must not:

- Respond to requests from family members to discuss individual cases
- Provide information to insurance companies, legal firms, or private investigators
- Confirm or deny details to journalists or media representatives
- Discuss cases with friends, colleagues from other organisations, or social contacts
- Share information with trade unions or employee representatives without management authorisation
- Provide records or documentation to any external party (including legal advisors)

All external requests for information must be:

- Reported immediately to senior management or Data Protection Officer
- Directed to the formal Subject Access Request process if from the data subject
- Handled through legal procedures if from external authorities
- Documented and recorded for audit purposes

5.3 Social Media and Electronic Communications

Employees must not:

- Post information about work, clients, patients, or RHS on any social media platform

- Use social media to discuss RHS, colleagues, clients, or patients
- Connect with clients, patients, or service users on personal social media accounts
- Use RHS information in LinkedIn profiles, TikTok content, or other public platforms
- Create video or audio content featuring RHS activities, premises, or people
- Discuss employment grievances or issues via social media
- Share links to internal documents or systems on social media
- Photograph or video record RHS premises without explicit authorisation
- Use instant messaging applications (WhatsApp, Signal, Telegram) for work-related confidential information

Breach of social media confidentiality restrictions will result in disciplinary action including dismissal.

5.4 Personal Security Responsibilities

Employees are responsible for:

- Keeping passwords confidential and changing them regularly
- Never sharing login credentials with colleagues
- Logging off systems when away from desk
- Not leaving personal data unattended
- Securing devices (laptop, tablet, phone) when not in use
- Using secure encrypted connections for remote working
- Reporting security incidents immediately
- Not downloading confidential data to personal devices
- Complying with device security policies (password protection, encryption, etc.)
- Immediately reporting loss or theft of any RHS equipment

———

6. Third-Party Disclosure Restrictions

6.1 General Prohibition

Personal data held by RHS must not be disclosed to third parties except where:

- The data subject has given explicit written consent
- Legal obligation or court order requires disclosure
- Public interest justification exists and has been documented
- Contract with third party provides data processing agreement and appropriate safeguards

6.2 Permitted Disclosures

Internal RHS Personnel Only:

- Other RHS staff with legitimate professional "need-to-know"
- Staff must only access data necessary for their role

External Organisations (only where legally required or with explicit consent):

- **Regulator Communications:**
  - Care Inspectorate (for registered services in Scotland)
  - CQC (for registered services in England)
  - Local Authority Safeguarding Teams
  - NHS Bodies (for integrated care purposes)
  - Data Protection Officer communications to ICO

- **Legal Process:**
  - Court orders and tribunal proceedings

- Police investigations (with proper legal authority)
- Regulatory investigations (with proper legal authority)
- Coroner/Procurator Fiscal inquiries

- **Healthcare Coordination:**
  - NHS services providing integrated care (with data subject notification)
  - GP practices for continuity of care (with data subject notification)
  - Emergency services in life-threatening situations

- **Safeguarding Obligations:**
  - Safeguarding children services where child abuse suspected or at risk
  - Adult protection services where adult at risk
  - Police for crime prevention/detection

- **Contract Partners:**
  - Data processors with Data Processing Agreements in place
  - Subcontractors with appropriate contractual protections
  - Cloud storage providers with encryption and security measures

- **Financial/Regulatory:**
  - HMRC for tax compliance (limited employment data)
  - DBS (Disclosure and Barring Service) for background checks
  - Occupational Health Services for employee health matters
  - Insurance providers for relevant claims

6.3 Prohibited Disclosures

Disclosures are absolutely prohibited to:

- Media and journalists (except through formal public relations channels)
- Competitors or other healthcare providers
- Marketing firms or market research companies
- Any third party without explicit legal basis
- Family members of data subjects
- Friends or social acquaintances of staff
- Debt collection agencies or creditors
- Landlords or housing authorities
- Educational institutions (except with consent)
- Volunteer or charitable organisations
- Any party not bound by confidentiality agreement
- External legal advisors without client authorisation
- Private investigators
- Security firms (except for immediate safety threats)
- Any overseas recipient (unless adequacy determination or appropriate safeguards in place)

6.4 Data Processing Agreements

Where third parties process RHS personal data, written Data Processing Agreements must be in place specifying:

- The subject matter and duration of processing
- The nature and purpose of processing
- The types of personal data and categories of data subjects
- The rights and obligations of both parties
- Requirement for sub-processor approval
- Security and confidentiality obligations
- Data subject rights and procedures
- Liability and indemnification clauses
- Audit and inspection rights

- Return or deletion of data upon termination
- International transfer restrictions if applicable

No personal data processing by third parties occurs without a Data Processing Agreement.

6.5 Data Sharing Agreements

Where personal data is shared with external organisations for joint purposes, Data Sharing Agreements must specify:

- Purpose of data sharing
- Legal basis for sharing
- Data minimisation principles
- Duration of sharing
- Security measures
- Data subject notification
- Complaint procedures
- Termination provisions
- Compliance with GDPR Article 26 (joint controller arrangements)

———

7. Special Care Settings: Client and Patient Data

7.1 Client Confidentiality

All client and service user information is held in absolute confidence:

- Clients have the right to expect complete confidentiality
- No information disclosed to family members without explicit written consent
- No discussion of clients outside professional contexts
- No photographs or recordings without explicit written consent
- Confidentiality maintained indefinitely after service termination

7.2 Patient Health Records

Health records are protected under:

- UK GDPR special category data protections
- Data Protection Act 2018 Schedule 3 provisions
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Common law duty of confidentiality

Patient information may only be:

- Accessed by staff with legitimate care-related need-to-know
- Shared within care team on implied consent basis (unless patient objected)
- Disclosed beyond care team only with explicit patient consent
- Disclosed to emergency services in life-threatening situations
- Disclosed under legal process or statutory authority

7.3 Subject Access Requests from Clients

Clients have the right to request access to their own records:

- Requests responded to within one calendar month (extendable to three months)
- Information provided in clear, understandable format
- Third party information withheld unless consent obtained
- Access provided free of charge

- Records of all requests maintained

7.4 Care Inspectorate Access

Care Inspectorate inspectors have statutory power to access service records:

- Access limited to purposes of regulation and improvement
- Information protected under GDPR and DPA 2018
- Access documented and recorded
- Inspectors subject to confidentiality obligations

---

8. Employee Data and HR Matters

8.1 Employee Data Processing

RHS processes employee data for:

- Recruitment and employment administration
- Payroll and tax compliance
- Pension and benefits administration
- Performance management and appraisals
- Training and development
- Health and safety management
- Occupational health services
- Absence and leave management
- Disciplinary and grievance procedures
- Right to work verification (Home Office requirements)
- Security and premises access control
- Reference provision for future employers

8.2 Sensitive Employee Data

Special category employee data (health, diversity monitoring, etc.) is processed:

- Only with explicit consent or where employment law requires it
- With enhanced security measures
- With limited access to HR personnel only
- With secure separate storage
- With restricted retention periods

8.3 Right to Work Documentation

RHS retains right-to-work verification documentation as required by:

- Home Office Immigration, Asylum and Nationality Act 2006
- Statutory Instruments on Employment of Foreign Workers
- Standard retention period: throughout employment plus 2 years after termination
- Security measures equivalent to health and social care standards

8.4 References

Employment references provided to prospective employers:

- Limited to job-related factual information
- Only with employee's written permission (where possible)
- Confidential between organisations

- Factual accuracy maintained

8.5 Disciplinary and Grievance Records

Records relating to disciplinary or grievance matters:

- Retained for personnel files
- Accessed only by HR and relevant managers
- Protected under confidentiality and legal privilege where applicable
- Retention period: length of employment plus statutory limitation period

---

9. Safeguarding Obligations and Public Interest Disclosure

9.1 Safeguarding Duty

Nothing in this Policy overrides the statutory duty to protect children and vulnerable adults:

- Suspected abuse must be reported to appropriate authorities:
  - Local Authority Safeguarding Children or Adults at Risk services
  - Police (for serious crime)
  - Care Inspectorate (for registered service breaches)
- Reporting safeguarding concerns is a protected public interest disclosure
- Confidentiality of alleged abuser does not prevent safeguarding disclosure
- Employees have absolute duty to report genuine safeguarding concerns

9.2 Public Interest Disclosures (Whistleblowing)

Employees may disclose information where:

- Made in good faith on matters of genuine public concern
- Related to illegal activity, miscarriage of justice, or other wrongdoing
- Made through prescribed procedures:
  - Firstly to employer or management (preferred)
  - Then to relevant regulator (Care Inspectorate, CQC)
  - Then to legal authorities if appropriate
  - External disclosure only where prior channels unsuccessful
- Protected under Employment Rights Act 1996 (qualifying disclosures)
- Must be accompanied by legal advice before external disclosure
- Must demonstrate genuine reasonable belief of wrong-doing

Misuse of whistleblowing procedures for personal grievances or to disclose personal information is not protected and may result in disciplinary action.

9.3 Legal Compulsion

Where legally compelled to disclose information:

- Court orders and tribunal orders must be obeyed
- Police requests with proper legal authority must be complied with
- Regulatory authority requests must be assessed for legal authority
- RHS Data Protection Officer must be notified immediately
- Minimal information necessary must be disclosed
- Cooperation with legal process documented

---

10. Retention and Deletion of Data

10.1 General Principle

Personal data is not retained longer than necessary for specified purposes.

10.2 Retention Schedules

RHS maintains specific retention schedules:

Client and Patient Records:

- Active records: retained during care provision
- Closed records: retained for 3 years after last contact minimum (varies by service type and legal requirement)
- Deceased clients: retained per statutory requirements (minimum 3 years post-death)
- Mental health records: 6 years minimum
- Children's services records: until age 25 minimum

Employee Records:

- Personnel files: retained for employment duration plus 7 years post-termination
- Payroll records: retained for 6 years (HMRC requirement)
- Health records: retained for 6 years post-termination
- Disciplinary records: retained for length of employment plus 6 years
- Right-to-work documentation: retained throughout employment plus 2 years

Financial Records:

- Invoices and receipts: 6 years (tax requirement)
- Contracts: 6-12 years after termination
- Payment records: 6 years

IT and Communications:

- Email records: 3 years (non-business emails may be deleted sooner)
- Logs and security records: 1 year minimum
- Call recordings (if any): 3 months minimum to 12 months maximum

Regulatory and Compliance:

- Incident reports: 3-7 years depending on severity and legal claims risk
- Inspection reports: 7 years minimum
- Training records: length of employment plus 3 years
- Audit reports: 7 years

10.3 Data Deletion

When retention period expires:

- Data is securely deleted or anonymised
- Deletion method appropriate to data sensitivity (secure shredding, hard drive wiping, data destruction)
- Deletion recorded in data management system
- Backup and archive systems reviewed
- Data subjects notified if deletion relates to specific retention obligation

10.4 Archival and Research Use

In exceptional cases, archived data may be retained for:

- Historical research
- Statistical analysis
- Public interest research
- Where anonymised and appropriate safeguards in place

Archived data retains all data protection protections even where original retention period expired.

---

11. Security and Data Protection Measures

11.1 Technical Measures

RHS implements:

- **Encryption:**
  - Data at rest: encrypted using AES 256-bit or equivalent
  - Data in transit: encrypted using 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 for sensitive systems
  - Secure password policies (minimum 12 characters, complexity requirements)
  - Regular password resets
  - Automatic session timeout (15 minutes for public areas, 30 minutes for clinical areas)

- **System Security:**
  - Firewalls and intrusion detection
  - Antivirus and malware protection
  - Vulnerability scanning and patching
  - Software kept up to date
  - Secure configuration standards
  - Regular security updates

- **Backup and Recovery:**
  - Automated daily backups
  - Off-site backup storage
  - Tested recovery procedures
  - Ransomware protection measures

- **Network Security:**
  - Secure WiFi (WPA2/WPA3 encryption)
  - VPN for remote working
  - Network segmentation
  - Monitoring and alerting

11.2 Organisational Measures

RHS implements:

- **Policies and Procedures:**
  - Information security policy

  - Incident response procedure
  - Breach notification procedure
  - Clean desk policy
  - Clear screen policy

- **Personnel Security:**
  - DBS checks and background verification
  - Confidentiality agreements
  - Training and awareness
  - Disciplinary procedures for breaches
  - Exit procedures and access removal

- **Physical Security:**
  - Locked filing cabinets
  - Secure disposal facilities (shredders)
  - Access control to buildings
  - CCTV (where lawful and appropriate)
  - Visitor management
  - Badge or ID systems

- **Vendor Management:**
  - Data Processing Agreements with all processors
  - Vendor security assessments
  - Contract terms requiring security measures
  - Regular audits and compliance checks

11.3 Data Protection by Design and Default

New systems or processes include:

- Data Protection Impact Assessment (DPIA) before implementation
- Minimisation of personal data collection and processing
- Privacy considerations integrated from outset
- Default privacy settings
- Transparency built in
- Regular privacy reviews

———

12. Data Protection Breaches

12.1 Definition

A personal data breach is: "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed."

12.2 Breach Reporting Obligation

RHS must report breaches to:

Information Commissioner's Office (ICO):

- Where breach likely to result in risk to data subjects' rights and freedoms
- Notification within 72 hours of breach discovery
- Notification includes: description of breach, likely consequences, measures taken to remedy

Data Subjects:

- Where high risk to data subject rights/freedoms
- Without undue delay
- Clear communication in plain language
- Including nature of breach, advice on protection measures

Supervisory Authority:

- Regulator must be notified if breach affects regulated services

12.3 Breach Investigation

All breaches trigger:

- Immediate incident response (containment, assessment)
- Investigation into cause and extent
- Evaluation of likelihood and severity of risk
- Identification of affected data subjects
- Documentation of incident and response
- Root cause analysis
- Remedial actions to prevent recurrence

12.4 Breach Prevention

RHS maintains procedures to:

- Detect breaches rapidly
- Alert Data Protection Officer and managers
- Isolate affected systems
- Preserve evidence
- Engage with affected parties
- Cooperate with regulators

12.5 Employee Breach Consequences

Employees causing breaches through:

- Negligence or carelessness: disciplinary action, retraining
- Deliberate violation: summary dismissal
- Criminal activity: referral to police
- Regulatory breach: referral to professional body

---

13. Data Protection Officer Role

13.1 Appointment

RHS appoints a qualified Data Protection Officer responsible for:

- Monitoring and ensuring compliance with data protection law
- Advising on data protection obligations
- Conducting Data Protection Impact Assessments
- Receiving and investigating data subject requests
- Coordinating with Information Commissioner's Office
- Maintaining records of processing activities
- Providing training and awareness
- Conducting audits and inspections

13.2 Contact

Data Protection Officer: Mazher Khan

Email: maz.manager@responseheathcare.co.uk

Telephone: 07588444915

Address: Office 2.6, 1 Barrack Street, Hamilton, ML3 0DG

13.3 Role Independence

The Data Protection Officer:

- Works independently
- Reports directly to senior management
- Cannot be penalised for performing DPO functions
- Must have no conflict of interest with other roles
- Is accessible to all staff and data subjects

———

14. International Data Transfers

14.1 General Restriction

Personal data may not be transferred outside the United Kingdom except where:

- Recipient country has "adequate" data protection standard (adequacy decision)
- Appropriate safeguards in place (Standard Contractual Clauses, Binding Corporate Rules)
- Derogation for specific limited circumstances applies

14.2 Permitted Recipients

Data may be transferred to:

- **Adequate Countries:** European Economic Area (adequacy decision applies)
- **UK Organisations:** No restriction

14.3 Restricted Transfers

Transfers to countries without adequacy decision require:

- Standard Contractual Clauses in contracts
- Transfer Impact Assessment
- Supplementary measures
- Data subject notification
- ICO notification where required

14.4 No US Cloud Transfers

Data stored on US cloud providers requires:

- Impact assessment on surveillance laws
- Supplementary contractual protections
- Data subject notification where feasible
- Caution regarding sensitive data (health, special categories)

---

15. Compliance with Health and Social Care Regulations

15.1 Care Inspectorate Standards (Scotland)

For registered services in Scotland, RHS complies with:

- Health and Social Care Standards - Information and Consent standard
- Care Inspectorate Inspection Framework - Data protection and information security criteria
- Requirements for registration - Including data protection and information governance obligations
- Safeguarding and Reporting Obligations - Including duty to report certain matters

15.2 Health and Social Care Act 2008 (Regulated Activities) Regulations 2014

For registered activities, RHS complies with:

- Regulation 17 (Good Governance) - Including information management and data protection
- Regulation 19 (Fit and Proper Persons) - Background checks and confidentiality
- Regulation 20 (Remote Monitoring) - Technology security and privacy
- Requirement for information to be "secure, complete and accurate"

15.3 Data (Use and Access) Act 2025

For health and social care services, RHS:

- Complies with digital information standards (Section 121)
- Enables interoperability with NHS and social care systems
- Implements data protection reforms and automated decision safeguards
- Cooperates with ICO audits and inspections
- Complies with higher penalty regime for breaches

15.4 Health Records Access Guidance

Patient health records access complies with:

- Right of access under UK GDPR
- Subject Access Request procedures
- Access to Health Records Act 1990 principles
- NHS policy on health records access
- Timescales and exemptions

---

16. Privacy Impact Assessments and Audits

16.1 Data Protection Impact Assessment (DPIA)

DPIA required for:

- Processing of special category data (health data, etc.)
- Large-scale systematic monitoring
- Automated decision-making affecting legal rights
- Processing likely to result in high risk to data subjects

- Significant organisational change affecting data
- New technology implementation

DPIA includes:

- Description of processing and purposes
- Assessment of necessity and proportionality
- Identification of risks to data subject rights
- Evaluation of measures to mitigate risks
- Consultation with stakeholders where appropriate

16.2 Legitimate Interest Assessment (LIA)

LIA required where processing based on legitimate interests:

- Identification of legitimate interest
- Assessment of necessity
- Balance of interests test (organisation vs. data subject rights)
- Documentation of assessment
- Regular review and updating

16.3 Compliance Audits

RHS conducts regular audits:

- Annual data protection compliance audit
- Quarterly security audits
- Ad hoc audits in response to concerns
- External audit by third parties where appropriate

16.4 Records of Processing Activities (ROPA)

RHS maintains comprehensive records including:

- What personal data is processed
- Why it is processed (legal basis)
- Who it is shared with
- How long it is retained
- What security measures protect it
- Accessible to Data Protection Officer and ICO

---

17. Training and Awareness

17.1 Data Protection Training

All employees receive:

- Induction training on data protection obligations
- Annual refresher training
- Specific role-related training (clinical staff, admin staff, etc.)
- Training on confidentiality and third-party disclosure prohibition
- Training on employee recording prohibition and consequences
- Incident and breach response training

17.2 Training Records

RHS maintains records of:

- Training attendance
- Training content and date
- Competency assessment
- Refresher training dates
- Compliance with training requirements

17.3 Awareness Campaign

RHS promotes data protection awareness through:

- Posters and notices
- Regular updates and reminders
- Case studies and scenarios
- Email bulletins
- Team meetings
- Management reinforcement

———

18. Incident Management and Response

18.1 Incident Identification

Staff report any of:

- Suspected unauthorised access
- Loss or theft of personal data
- Security vulnerability or weakness
- Breach of confidentiality
- Suspected malware or cyber attack
- Accidental data disclosure

18.2 Incident Response Procedure

Upon identification:

1. Immediate Containment:
- Isolate affected system
- Secure premises if physical breach
- Preserve evidence
- Notify Data Protection Officer

2. Investigation:
- Determine scope of incident
- Identify affected data subjects
- Establish timeline and cause
- Evaluate risks to data subjects
- Interview relevant personnel

3. Notification:
- ICO notification if required (within 72 hours)
- Data subject notification if required
- Regulator notification if required
- Internal notification to management

4. Remediation:
- Implement corrective measures

- Inform affected parties of protective steps
- Restore systems to normal operation
- Review security controls

5. Post-Incident:
- Root cause analysis
- Implement preventive measures
- Update security procedures
- Conduct follow-up training
- Document lessons learned

18.3 Breach Log

RHS maintains:

- Log of all personal data breaches (regardless of reporting threshold)
- Date and time of breach
- Description of breach
- Data subjects affected
- Cause and contributing factors
- Response actions taken
- Outcomes and learnings

---

19. Third Party Confidentiality Obligation

All third parties, contractors, service providers, and agents working with RHS must:

- Execute Confidentiality Agreements
- Comply with this Policy
- Comply with data protection law
- Implement equivalent security measures
- Not disclose RHS information
- Maintain confidentiality indefinitely
- Cooperate with audits and inspections
- Understand breach of confidentiality results in contract termination and potential legal action

---

20. Disciplinary Framework for Policy Violations

20.1 Employee Recording Violation

Recording anything on personal devices without authorisation:

First violation:
- Immediate disciplinary hearing
- Likely outcomes: Suspension without pay (1-2 weeks), final written warning, or dismissal
- Investigation of all recordings made
- Potential recovery of damages

Second violation within 2 years:
- Summary dismissal without notice
- Referral to police
- Referral to professional regulatory body

20.2 Confidentiality Breach

Unauthorised disclosure of confidential information:

Accidental minor disclosure:
- Verbal warning, retraining, monitoring

Negligent confidentiality breach:
- Written warning, disciplinary action, potential suspension
- Mandatory retraining
- Performance improvement plan

Intentional disclosure:
- Suspension pending investigation
- Summary dismissal without notice
- Potential legal action for damages
- Referral to police (if criminal breach)
- Referral to professional body

Disclosure on social media:
- Immediate suspension
- Summary dismissal
- Potential legal action
- Referral to police (harassment/defamation)

20.3 Third-Party Disclosure Without Authority

Providing RHS information to external parties:

Without explicit authority:
- Formal disciplinary process
- Written warning or dismissal depending on sensitivity
- Investigation of all disclosures made
- Potential legal action

To media or journalists:
- Immediate summary dismissal
- Potential legal action for damages
- Criminal referral possible

20.4 Failure to Report Incidents

Failure to report personal data breach or security incident:

Within competency zone:
- Written warning
- Mandatory training
- Performance monitoring

Deliberate non-reporting:
- Formal discipline
- Likely dismissal
- Referral to regulator

20.5 Persistent Policy Violations

Multiple violations within employment period:

- Cumulative disciplinary framework applied
- Escalation to summary dismissal
- Referral to professional regulatory bodies

- Potential criminal referral

---

21. Fairness and Procedural Safeguards

21.1 Procedural Fairness

All disciplinary action for data protection violations follows:

- Clear notice of alleged breach
- Investigation period with employee input
- Right to representation at hearing
- Opportunity to present defence
- Written decision with clear reasoning
- Right of appeal
- Appeal heard by independent manager
- Documentation of entire process

21.2 Protection Against Arbitrary Enforcement

This Policy is designed to be:

- Clear and Specific: Every prohibition clearly stated
- Necessary and Proportionate: Measures justified by legal requirements and risk
- Applied Consistently: Same standard applied to all employees
- Not Arbitrary: Discretionary decisions documented with clear reasoning
- Transparent: Policy available to all staff
- Procedurally Fair: Disciplinary process follows natural justice principles
- Legally Compliant: Procedures comply with employment law, GDPR, common law fairness
- Subject to Appeal: Appeals process available
- Challengeable: Employees may seek external legal advice
- Reviewable: Policy reviewed regularly and updated as law changes

21.3 Proportionality

Disciplinary action is proportionate to:

- Severity of breach
- Deliberateness or negligence
- Impact on data subjects
- Prior warnings and breaches
- Mitigating circumstances
- Employee seniority and responsibility

21.4 Legal Compliance

This Policy complies with:

- Employment Rights Act 1996 - Fair dismissal procedures
- Equality Act 2010 - Non-discrimination in enforcement
- Data Protection Act 2018 - Fair processing
- UK GDPR - Lawful, fair, transparent processing
- Common Law - Natural justice and procedural fairness
- Human Rights Act 1998 - Fair trial and due process

---

22. Policy Governance and Review

22.1 Policy Owner

Data Protection Officer: Mazher Khan

Responsible for policy maintenance, updates, and enforcement

22.2 Review Schedule

This Policy is reviewed:

- Annually as standard
- Immediately upon legislative change affecting data protection
- Upon significant organisational change
- Upon data protection incident or breach
- Upon regulator guidance or requirement change
- At least every 24 months regardless of circumstances

22.3 Version Control

Policy updates tracked and documented:

- Version number and date recorded
- Changes identified and communicated
- Previous versions archived (minimum 3 years)
- Staff notified of material changes
- Training updated accordingly

22.4 Approval

Policy approved by:

- Data Protection Officer
- Senior Management
- Board or Governance Body
- External review (periodically)

22.5 Communication

Policy communicated to:

- All new employees at induction
- All existing employees upon revision
- All contractors and service providers
- Clients and service users (summary)
- Regulatory bodies upon request
- Data subjects upon request

———

23. Key Definitions and Clarifications

23.1 "Absolute Prohibition"

Where Policy states something is "absolutely prohibited" or "strictly prohibited," this means:

- Complete ban on activity
- No exceptions unless explicitly stated elsewhere in Policy
- No discretion to permit under normal circumstances

- Breach results in disciplinary action including dismissal

Examples: Recording on personal devices, unauthorised third-party disclosure

23.2 "Strict Liability"

Where Policy applies "strict liability":

- No need to prove intentional breach
- Careless or negligent breach equally prohibited
- No mitigation for unintentional breach
- Applies regardless of actual harm caused

Example: Confidentiality obligation applies regardless of whether information actually disclosed or whether recipient used it

23.3 "Indefinitely"

Where Policy states confidentiality obligation survives "indefinitely":

- Obligation continues after employment termination
- No time limit on confidentiality duty
- Applies even after Policy termination
- Common law confidentiality may also apply

23.4 "Without Exception"

Where Policy states prohibition applies "without exception":

- No circumstance permits breach
- Even stated good intentions don't permit breach
- No emergency override (except legal compulsion)

Example: Recording prohibition applies "without exception" regardless of stated purpose

———

24. Appeal Rights and External Redress

24.1 Appeal Rights

Employees may appeal:

- Disciplinary decision within 10 working days
- Appeal to manager independent of original decision-maker
- Right to representation at appeal
- Written decision within 5 working days
- Final decision recorded in personnel file

24.2 External Redress

Employees may pursue:

- Employment Tribunal claim for unfair dismissal
- ICO complaint regarding data protection practices
- Legal action for breach of contract
- Trade union representation and support
- Professional body complaints (where applicable)

- Whistleblowing protection claim (if appropriate)

24.3 Dispute Resolution

For disputes regarding Policy interpretation:

- Initial discussion with line manager
- Escalation to HR/Management
- Discussion with Data Protection Officer
- Mediation where appropriate
- Formal grievance procedure if necessary
- Independent external adjudication available

24.4 Policy Challenge

Employees may challenge:

- Fairness of specific Policy provision
- Necessity of specific requirement
- Proportionality of enforcement
- Procedural compliance
- Consistency of application

Challenge process:

- Written statement of concern to Data Protection Officer
- Investigation by independent manager (if concerning DPO)
- Written response within 10 working days
- Appeal to senior management if unsatisfied
- External legal advice available

———

25. Implementation and Contact Information

25.1 Effective Date

This Policy is effective from: **June 2025**

25.2 Staff Implementation

- **Week 1:** Policy circulated to all staff
- **Week 2:** Mandatory training commenced
- **Week 4:** Training completion deadline
- **Week 5:** Compliance monitoring commenced
- **Month 2 onwards:** Full enforcement of Policy

25.3 Contractor Implementation

- **Week 2:** Policy provided to all contractors
- **Week 4:** Confidentiality agreements signed
- **Week 5:** Contractor training completed
- **Month 2 onwards:** Contractor compliance

25.4 Contact Information

Response Healthcare Solutions Ltd

Data Protection Queries:
- Data Protection Officer: Mazher Khan
- Email: maz.manager@responseheathcare.co.uk
- Telephone: 07588444915
- Address: Office 2.6, 1 Barrack Street, Hamilton, ML3 0DG

Subject Access Requests:
- Written requests to: Office 2.6, 1 Barrack Street, Hamilton, ML3 0DG
- Email: admin@responsehealthcare.co.uk
- Requests responded to within one calendar month

Complaints about Data Protection:

Complaints may be made to:

- **Internal:** Data Protection Officer
- **External:** Information Commissioner's Office (ICO)
  - Website: www.ico.org.uk
  - Telephone: 0303 123 1113
  - Address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

———

26. Acknowledgment of Policy

All employees must acknowledge receipt and understanding of this Policy through:

- Electronic acknowledgment in HR system
- Signed acknowledgment form (paper copy maintained)
- Completion of mandatory training
- Record maintained in personnel file

Failure to acknowledge Policy does not exempt employees from compliance.

———

27. References and Statutory Framework

[1] General Data Protection Regulation (UK GDPR) - Retained in UK law via Data Protection Act 2018

[2] Data Protection Act 2018 - UK legislation implementing GDPR and pre-existing data protection law

[3] Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 - Regulation 17 (Good Governance) and related provisions

[4] Data (Use and Access) Act 2025 - Recent legislation introducing digital standards and data protection reforms

[5] Public Services Reform (Scotland) Act 2010 - Statutory basis for Care Inspectorate powers and obligations

[6] Health and Social Work (Scotland) Act 2015 - Social Work and social care standards framework for Scotland

[7] Care Inspectorate Standards and Guidance - Regulatory standards for registered services in Scotland

[8] Health Records Access - Access to Health Records Act 1990 and NHS guidance

[9] Whistleblowing - Employment Rights Act 1996, Part IVA (Public Interest Disclosure)

[10] Employment Law - Equality Act 2010, Employment Rights Act 1996, relevant amendments

[11] Information Commissioner's Office Guidance - UK GDPR practical guidance and regulatory expectations

[12] Common Law Duty of Confidentiality - Case law establishing confidentiality obligations in employment

[13] Human Rights Act 1998 - Article 8 Right to respect for private and family life

[14] Home Office Statutory Guidance - Right to work verification and retention requirements

---

Document Control

- **Issue Date:** June 2025
- **Next Review:** June 2026
- **Classification:** Internal - Confidential
- **Document Owner:** Data Protection Officer

Approval Signatures:

- **Operations Officer:** Falaknaz Khan and Sean Carter | Date: 02/June/2025
- **Data Protection Officer:** Mazher Khan | Date: 02/June/2025

This policy is confidential and intended for internal use by Response Healthcare Solutions Ltd only.