UT COMPLIANCE

A TRADING NAME OF UNIQUE TENDERS LIMITED

POLICY DOCUMENT

GDPR and Data Protection Policy

UT Compliance

DOMICILIARY CARE

DOCUMENT REFERENCE —	EFFECTIVE DATE 18 January 2026
VERSION DC/GDP/001	REVIEW DATE —
STATUS Publish	APPROVED BY —

CONFIDENTIAL DOCUMENT

This document is intended for authorised personnel only. Unauthorised distribution is prohibited.

1. Scope

1.1 Purpose

This GDPR and Data Protection Policy establishes ‘s commitment to protecting personal data and complying with data protection legislation. The policy provides a comprehensive framework for the lawful, fair, and transparent processing of personal data in accordance with UK GDPR, the Data Protection Act 2018, and other relevant legislation.

The purpose of this policy is to:

- Ensure compliance with UK GDPR and Data Protection Act 2018
- Protect the privacy rights of service users, staff, and others whose personal data we process
- Establish clear procedures for collecting, processing, storing, sharing, and destroying personal data
- Define roles and responsibilities for data protection
- Ensure individuals can exercise their data protection rights
- Prevent data breaches and ensure appropriate response procedures
- Promote a culture of data protection awareness throughout the organisation

1.2 Application

This policy applies to:

- All personal data processed by , regardless of format (paper, electronic, audio, visual)
- All employees, volunteers, students, contractors, and third parties who process personal data on our behalf
- Personal data of service users, staff, job applicants, contractors, and any other individuals
- All locations where personal data is processed, including offices, service users’ homes, and remote working locations
- All systems and technologies used to process personal data

1.3 Regulatory Context

This policy supports compliance with:

- CQC Regulation 17: Good governance (requirement to maintain accurate, complete, and contemporaneous records)
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Health and Social Care Act 2008
- Care Act 2014 (information sharing for safeguarding)
- Common Law Duty of Confidentiality
- Caldicott Principles for health and social care data

1.4 Policy Review and Updates

This policy will be reviewed:

- Annually, or sooner if required by legislative or regulatory changes
- Following data breaches or near misses
- Following ICO enforcement action or recommendations
- Following CQC inspection feedback
- When significant changes to data processing activities occur

2. Legal and Regulatory Framework

operates within a comprehensive data protection legal framework. The following legislation and regulations inform this policy:

Legislation/Regulation	Requirements
UK General Data Protection Regulation (UK GDPR)	Primary data protection legislation post-Brexit. Establishes principles for lawful processing: lawfulness, fairness, transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability. Grants individuals rights: access, rectification, erasure, restriction, portability, objection. Requires legal basis for processing, data protection by design and default, Data Protection Impact Assessments for high-risk processing, and appointment of Data Protection Officer where required. Maximum fines up to £17.5 million or 4% of annual turnover.
Data Protection Act 2018 (DPA 2018)	UK implementation of GDPR. Supplements UK GDPR with additional provisions. Part 2 covers law enforcement processing. Part 3 covers intelligence services. Schedule 1 defines special category data conditions. Provides exemptions for various purposes including safeguarding, crime prevention, and regulatory functions. Establishes Information Commissioner's Office (ICO) powers and enforcement mechanisms. Creates criminal offences for unlawful obtaining/disclosure of personal data and re-identification of de-identified data.
Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 – Regulation 17	CQC fundamental standard requiring good governance. Must maintain accurate, complete, and contemporaneous records in respect of each service user, including care plans, risk assessments, and treatment records. Records must be kept securely, retained appropriately, and be available for inspection. Must have systems to assess, monitor, and improve quality and safety of services, which includes proper record-keeping and information governance. Poor record-keeping can result in CQC enforcement action.
Care Act 2014	Establishes legal framework for information sharing in adult social care. Local authorities have duty to share information for safeguarding purposes (Section 45). Information sharing must comply with Data Protection Act and common law duty of confidentiality. Permits information sharing without consent where necessary to protect adults at risk. Requires information governance arrangements to be in place. Supports multi-agency working through appropriate information sharing.
Common Law Duty of Confidentiality	Long-established legal obligation to protect confidential information. Applies to information given in confidence, particularly in healthcare/care relationships. Can be breached only with consent, under legal obligation, or in public interest (e.g., safeguarding, prevention of serious crime). Breach can result in civil action for damages. More stringent than GDPR in some respects – must consider both GDPR and confidentiality when sharing information.

Human Rights Act 1998 – Article 8	Right to respect for private and family life. Processing of personal data must respect privacy rights. Must be justified, necessary, and proportionate. Particularly relevant to sharing sensitive health and care information. Can be overridden in certain circumstances (e.g., safeguarding, crime prevention) but interference must be lawful and necessary. Applies to all public authorities and private organisations providing public functions.
Privacy and Electronic Communications Regulations 2003 (PECR)	Regulates marketing communications (email, text, automated calls). Requires consent for direct marketing via electronic communications (with limited exceptions for existing customers). Applies to care providers sending marketing materials or newsletters. Breach can result in ICO fines up to £500,000. Cookies and similar technologies also covered (though less relevant to domiciliary care).
Computer Misuse Act 1990	Makes it criminal offence to access computer systems without authorisation. Applies to staff accessing service user records without legitimate reason. Unauthorised access, modification of data, or facilitating access are criminal offences. Can result in imprisonment. Reinforces need for access controls and audit trails on electronic systems.
Freedom of Information Act 2000 (FOIA)	Applies to public authorities (may apply to care providers delivering public services). Provides right of public access to information held by public authorities. Must respond to requests within 20 working days. Some exemptions apply (personal data, commercial interests, legal privilege). Must have publication scheme. ICO can enforce compliance.
Caldicott Principles	Not legislation but authoritative guidance for health and social care. Seven principles: justify purpose, use minimum necessary data, access on need-to-know basis, everyone with access has responsibilities, understand and comply with law, duty to share information can be as important as duty to protect, inform people about how data is used. Caldicott Guardian role (senior person responsible for data protection) recommended for organisations.
NHS Data Security and Protection Toolkit	Mandatory for NHS-funded care providers. Set of standards for data security and information governance. Providers must complete annual assessment. Covers ten standards including people, processes, and technology. Failure can result in contract suspension. Demonstrates commitment to data security. Although named ‘NHS’, applies to all organisations providing NHS-funded care.
Records Management Code of Practice for Health and Social Care 2016	Statutory code under Section 16 of Health and Social Care Act 2008. Sets out standards for managing records. Covers entire lifecycle: creation, use, retention, disposal. Requires documented retention schedules. Mandates secure disposal. Specifies minimum retention periods (e.g., adult care records minimum 8 years, safeguarding records long-term retention). CQC inspects compliance.

3. Definitions of Key Terms

The following definitions clarify key data protection terms used throughout this policy:

Term	Definition
Personal Data	Any information relating to an identified or identifiable living individual (data subject). Includes name, address, date of birth, NHS number, medical information, care records, photographs, video recordings, email addresses, IP addresses, location data. An identifiable person is one who can be identified directly or indirectly by reference to an identifier such as a name, identification number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. Deceased individuals’ data is not personal data under UK GDPR but may be protected by confidentiality.

Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed to uniquely identify a person, health data, or data concerning a person's sex life or sexual orientation. Requires higher level of protection and stricter conditions for processing. In care sector, most service user information is special category data (health/care data). Requires both a lawful basis under Article 6 UK GDPR AND a special category condition under Article 9 UK GDPR.
Data Subject	The living individual to whom personal data relates. In domiciliary care context, includes service users, staff, job applicants, family members (when their data is recorded), contractors, and anyone else whose personal data is processed. Data subjects have rights under UK GDPR including access, rectification, erasure, restriction, portability, and objection.
Data Controller	as an organisation. The legal entity that determines the purposes and means of processing personal data. Makes decisions about what data to collect, why, how it will be used, who it will be shared with, and how long to keep it. Has overall responsibility for compliance with data protection legislation. Must ensure lawful processing, implement appropriate security, respond to data subject requests, report breaches, and maintain records of processing activities.
Data Processor	Organisation or person who processes personal data on behalf of the data controller. Examples include: payroll providers, IT support companies, cloud storage providers, secure destruction companies, electronic care management system providers. Must process data only on documented instructions from controller. Must implement appropriate security measures. Must assist controller with data subject requests and breach notifications. Must have written contract with controller specifying processing terms.
Processing	Any operation performed on personal data, whether automated or manual. Includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Simply viewing personal data is processing. Creating care records is processing. Storing data is processing. Sharing with health professionals is processing. All processing must have lawful basis.
Lawful Basis	Legal ground for processing personal data required by Article 6 UK GDPR. Six bases: (1) Consent – clear affirmative action, freely given, specific, informed, unambiguous; (2) Contract – necessary for contract with data subject or to take steps before contract; (3) Legal obligation – required by law; (4) Vital interests – necessary to protect life; (5) Public task – necessary for public interest or official function; (6) Legitimate interests – necessary for legitimate interests (not available for public authorities). For special category data, also need Article 9 condition (e.g., health/social care purposes, safeguarding).
Consent	Freely given, specific, informed, and unambiguous indication of wishes by which data subject signifies agreement to processing of their personal data. Must be clear affirmative action (opt-in, not opt-out). Cannot be bundled with other terms. Must be easy to withdraw. Cannot be precondition of service where not necessary. Pre-ticked boxes invalid. Children under 13 require parental consent (16 for some purposes). Records of consent must be kept. Not always required – often processing is under different lawful basis (e.g., care provision is under contract or legal obligation).
Data Protection Impact Assessment (DPIA)	Process to identify and minimise data protection risks of a project or system. Required for processing likely to result in high risk to individuals' rights and freedoms, particularly when using new technologies, systematic monitoring, large-scale processing of special category data, or when processing affects vulnerable people. Must describe processing, assess necessity and proportionality, identify risks, and outline mitigation measures. Must consult Data Protection Officer. If high risk remains after mitigation, must consult ICO before proceeding.
Data Breach	Breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples: emailing personal data to wrong recipient, losing unencrypted device containing personal data, unauthorised access to care records, ransomware attack, loss of paper records, leaving records in service user's home, discussing service user in public. Must report to ICO within 72 hours if risk to individuals' rights and freedoms. Must notify affected individuals if high risk. Must maintain internal breach register. Prevention better than cure – implement appropriate security measures.

Data Subject Rights	Rights granted to individuals under UK GDPR. (1) Right to be informed – how data is used; (2) Right of access – obtain copy of data (Subject Access Request); (3) Right to rectification – correct inaccurate data; (4) Right to erasure – 'right to be forgotten' in certain circumstances; (5) Right to restrict processing – limit how data is used; (6) Right to data portability – receive data in machine-readable format; (7) Right to object – stop processing in certain circumstances; (8) Rights related to automated decision-making. Must respond within one month. Cannot charge fee unless request manifestly unfounded or excessive. Exemptions apply (e.g., cannot erase data needed for legal compliance or safeguarding).
Data Protection Officer (DPO)	Person with expert knowledge of data protection law and practices. Required for public authorities, organisations whose core activities involve systematic monitoring of data subjects on large scale, or large-scale processing of special category data. Many care providers require DPO. Can be staff member or external appointment. Must be independent, report to highest management, have adequate resources, not receive instructions regarding tasks, and not be dismissed for performing duties. Responsibilities include monitoring compliance, advising on DPIAs, cooperating with ICO, and being contact point for data subjects and ICO.
Retention Period	Length of time personal data is kept before deletion or anonymisation. Must not keep data longer than necessary for purpose. Different data types have different retention requirements. Adult social care records: minimum 8 years after last contact (Records Management Code of Practice). Safeguarding records: long-term retention may be necessary. Employment records: typically 6 years after employment ends (7 for payroll). Accident records: 3 years for adults, until age 21 for children. Must have documented retention schedule. Must review data regularly. Must securely destroy data at end of retention period. Some records have permanent retention for historical purposes.
Information Asset	Body of information that has value to the organisation and/or must be protected. Examples: care records, staff personnel files, training records, financial records, complaints records, policies, IT systems, databases, email systems. Each asset should have designated owner responsible for appropriate protection. Should maintain Information Asset Register documenting what data is held, where, how protected, who has access, and retention period. Helps understand data landscape and manage risks.
Privacy Notice	Document (also called 'fair processing notice' or 'privacy policy') explaining how personal data is processed. Must provide: controller identity, DPO contact details, purposes of processing, lawful basis, recipients of data, retention period, data subject rights, right to complain to ICO, whether providing data is statutory/contractual requirement, any automated decision-making. Must be concise, transparent, intelligible, easily accessible, and in plain language. Must provide at point of data collection. Separate notices for different audiences (service users, staff, job applicants). Must update when processing changes.

4. Policy Statement

4.1 Organisational Commitment

is committed to protecting the privacy and security of personal data. We recognise that processing personal data is essential to delivering high-quality care and running our organisation effectively, and we are committed to doing so in compliance with data protection legislation and ethical best practices.

We will:

- Process personal data lawfully, fairly, and transparently
- Collect data only for specified, explicit, and legitimate purposes
- Ensure data is adequate, relevant, and limited to what is necessary
- Keep data accurate and up to date

- Retain data only for as long as necessary
- Implement appropriate technical and organisational security measures
- Demonstrate accountability and maintain records of our processing activities
- Respect and facilitate the exercise of data subject rights
- Report data breaches to the ICO and affected individuals as required
- Provide regular training to all staff on data protection

4.2 Data Protection Principles

Our data protection practices are guided by the seven principles of UK GDPR:

Principle 1: Lawfulness, Fairness, and Transparency – We will process personal data lawfully (with valid legal basis), fairly (not in ways that are unduly detrimental, unexpected, or misleading), and transparently (individuals are informed about how their data is used through clear privacy notices).

Principle 2: Purpose Limitation – We will collect personal data for specified, explicit, and legitimate purposes and not process it in ways incompatible with those purposes. We will not use service user care data for unrelated purposes without obtaining appropriate consent or having another lawful basis.

Principle 3: Data Minimisation – We will ensure data collected is adequate, relevant, and limited to what is necessary for the purposes for which it is processed. We will not collect excessive information 'just in case' or retain data beyond its useful purpose.

Principle 4: Accuracy – We will take reasonable steps to ensure personal data is accurate and, where necessary, kept up to date. Inaccurate data will be rectified or erased without delay. Staff must record information accurately and report any inaccuracies identified.

Principle 5: Storage Limitation – We will keep personal data in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data is processed. We maintain documented retention schedules and securely dispose of data at the end of retention periods.

Principle 6: Integrity and Confidentiality (Security) – We will process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. We implement appropriate technical and organisational measures including encryption, access controls, staff training, and secure disposal.

Principle 7: Accountability – We will demonstrate compliance with the data protection principles through documented policies, procedures, training records, Data Protection Impact Assessments, records of processing activities, and audit trails. The burden is on us to prove we comply, not on regulators to prove we don't.

5. Roles and Responsibilities

Data protection is everyone's responsibility. The following table outlines specific responsibilities:

Role	Responsibilities

All Staff	– Understand and comply with this policy and data protection legislation – Process personal data only for legitimate work purposes – Access only data necessary for role (need-to-know basis) – Keep passwords secure and never share login credentials – Lock screens when leaving workstations unattended – Ensure paper records are stored securely in locked cabinets – Never remove personal data from premises without authorisation – Report suspected data breaches immediately to line manager and DPO – Report inaccuracies in personal data – Complete mandatory data protection training – Respect confidentiality of service users and colleagues – Follow secure email and communication protocols – Challenge colleagues who are not following data protection procedures – Be aware of social engineering and phishing attempts
Registered Manager	– Overall accountability for data protection compliance – Ensure adequate resources allocated to data protection – Champion data protection culture throughout organisation – Ensure Data Protection Officer appointed and supported – Approve new data processing activities and systems – Review Data Protection Impact Assessments – Approve data sharing agreements with third parties – Ensure appropriate cyber security insurance in place – Report significant data protection issues to board/owners – Respond to ICO enforcement action – Ensure compliance with CQC Regulation 17 record-keeping requirements – Review data protection audit findings and ensure action plans implemented – Approve Subject Access Request responses where sensitive/complex – Ensure contracts with data processors include appropriate clauses
Duty Manager	– Ensure staff follow data protection procedures during operational shifts – Monitor compliance with secure record-keeping practices – Respond to immediate data protection concerns (e.g., suspected breach during out-of-hours) – Ensure confidential conversations are held in private – Ensure paper records in use during shifts are stored securely at end of shift – Ensure devices (tablets, laptops, phones) are secured when not in use – Coordinate initial response to data breaches occurring during shift (contain breach, preserve evidence, notify DPO/senior management) – Ensure visitors (e.g., health professionals, assessors) sign confidentiality agreements – Monitor staff use of personal devices for work purposes – Ensure staff do not discuss service users in public or semi-public spaces – Brief staff on any data protection incidents and learning points
Data Protection Officer	– Lead and coordinate data protection compliance activities – Provide expert advice on data protection legislation and best practice – Maintain Records of Processing Activities (Article 30 register) – Conduct Data Protection Impact Assessments for high-risk processing – Review and update data protection policies and procedures – Coordinate response to data breaches (log, investigate, report to ICO if required, notify affected individuals if high risk) – Investigate data protection complaints – Act as point of contact with Information Commissioner's Office – Respond to data subject requests (Subject Access Requests, rectification, erasure, etc.) – Maintain privacy notices and ensure kept up to date – Deliver and coordinate data protection training – Conduct data protection audits and inspections – Review contracts with data processors – Advise on data sharing agreements – Monitor changes in legislation and assess impact – Maintain data breach register – Produce data protection reports for senior management

Health and Safety Officer	– Ensure health and safety records comply with data protection requirements – Maintain confidentiality of accident and incident reports – Securely store occupational health information – Ensure RIDDOR reports do not contain excessive personal data – Liaise with DPO on retention of health and safety records – Ensure risk assessments containing personal data are stored securely – Maintain confidentiality when investigating accidents – Ensure health surveillance records are kept confidential and secure
Safeguarding Lead	– Balance safeguarding duties with data protection obligations – Understand legal basis for sharing information for safeguarding (Care Act Section 45, vital interests, legal obligation) – Share information appropriately with local authority safeguarding team, police, and other agencies – Maintain confidentiality of safeguarding concerns and investigations – Ensure safeguarding records are stored securely with restricted access – Liaise with DPO on safeguarding information sharing queries – Document decisions about information sharing – Understand when information can be shared without consent – Ensure long-term retention of safeguarding records where appropriate – Train staff on balancing confidentiality with duty to share information for safeguarding
IT Manager/Administrator	– Implement technical security measures (firewalls, encryption, access controls, anti-virus, patching) – Monitor systems for unauthorised access attempts – Manage user accounts, access rights, and password policies – Ensure regular backups and test restoration procedures – Securely dispose of IT equipment containing personal data (hard drive destruction/wiping) – Log and monitor system access – Implement email security (spam filters, encryption for sensitive data) – Ensure mobile devices have remote wipe capability – Conduct vulnerability assessments – Ensure cloud services have appropriate security and data protection terms – Maintain audit trails of data access – Report suspected cyber security incidents to DPO immediately – Ensure systems log off automatically after period of inactivity
Human Resources	– Maintain confidentiality of employee personal data – Process job applications in compliance with data protection legislation – Conduct DBS checks appropriately and securely – Securely store personnel files – Ensure employment contracts include data protection clauses – Manage Subject Access Requests for employee data – Ensure appropriate retention and disposal of employee records – Maintain confidentiality during disciplinary and grievance procedures – Ensure occupational health referrals comply with data protection requirements – Provide data protection information to new starters – Coordinate data protection training for all staff

6. Data Protection Procedures

The following procedures ensure compliant processing of personal data throughout its lifecycle.

6.1 Lawful Basis for Processing

All processing of personal data must have a valid lawful basis under Article 6 UK GDPR. For special category data (health/care data), we also need a condition under Article 9.

Our lawful bases for processing:

- Service user care data: Contract (provision of care services) + Article 9(2)(h) (health/social care purposes)
- Safeguarding information sharing: Legal obligation (Care Act 2014) + Article 9(2)(b) (social protection) or Article 9(2)(f) (vital interests)
- Employee data: Contract (employment) + Article 9(2)(b) (employment law obligations) for special category data
- Job applicant data: Steps before contract (recruitment process) + Article 9(2)(b) (employment law) for DBS checks
- CCTV (if used): Legitimate interests (security of premises and service users)
- Marketing to existing service users/families: Legitimate interests (maintaining relationships with customers)

6.2 Privacy Notices

We maintain separate privacy notices for different audiences:

- Service User Privacy Notice – provided at assessment/start of service
- Employee Privacy Notice – provided on commencement of employment
- Job Applicant Privacy Notice – provided at application stage
- Website Privacy Notice – available on our website

Each privacy notice includes: identity of controller, DPO contact details, purposes of processing, lawful basis, data sharing, retention periods, data subject rights, right to complain to ICO.

6.3 Data Collection

When collecting personal data, staff must:

- Collect only data that is necessary for the specified purpose
- Ensure individual is provided with privacy notice at point of collection
- Explain how the data will be used
- Record data accurately and completely
- Obtain consent where this is the lawful basis for processing
- Never collect data that is not relevant to the purpose
- Record data in designated systems (care management system, HR system) not on personal devices or unofficial systems

6.4 Data Storage and Security

Electronic Data:

- Store on secure, password-protected systems
- Use strong passwords (minimum 12 characters, mixture of upper/lower case, numbers, symbols)
- Change passwords every 90 days
- Never share passwords

- Enable two-factor authentication where available
- Lock screens when leaving workstation (Windows key + L)
- Encrypt sensitive data, especially on portable devices
- Use secure cloud storage providers with UK data centers
- Regular backups stored securely and separately
- Anti-virus and anti-malware software kept up to date
- Automatic system updates and patching

Paper Records:

- Store in locked filing cabinets when not in use
- Keep filing cabinets in secure areas with restricted access
- Never leave confidential documents on desks overnight
- Use privacy screens or folders when transporting documents
- Do not remove documents from premises without authorisation
- Shred confidential documents when no longer needed
- Clear desk policy – no confidential information left visible

6.5 Data Sharing and Disclosure

Personal data may be shared with third parties only where there is a lawful basis and appropriate safeguards are in place.

Circumstances for data sharing:

- With service user's explicit consent
- For safeguarding purposes (Care Act 2014 Section 45 duty to share)
- With healthcare professionals involved in service user's care (consent implied through care provision)
- With local authority commissioners (contractual requirement)
- With CQC (regulatory requirement)
- With police or courts (legal obligation)
- For vital interests (life or death situations)

Information sharing procedures:

- Share minimum amount of information necessary
- Ensure recipient has legitimate need to know
- Use secure methods (encrypted email, secure portal, hand delivery)
- Never send personal data via unencrypted email unless low risk
- Document all information sharing decisions and rationale
- Obtain written data sharing agreements with regular recipients

- Check recipient has appropriate security measures in place
- Mark documents ‘Confidential’ when sharing

Safeguarding information sharing:

When there are safeguarding concerns, duty to share information may override confidentiality. Staff should:

- Share information promptly with local authority safeguarding team
- Share information without consent where necessary to protect adult at risk
- Document decision to share and legal basis
- Consider proportionality – share only what is relevant
- Record what information was shared, with whom, when, and why
- Inform service user information has been shared unless doing so would increase risk

6.6 Subject Access Requests (SARs)

Individuals have the right to request access to their personal data under Article 15 UK GDPR. We must respond within one calendar month.

Procedure:

- SAR can be made verbally or in writing (email, letter, in person)
- Forward all SARs immediately to Data Protection Officer
- DPO verifies identity of requester (two forms of ID)
- If request made by representative, verify authority to act (e.g., lasting power of attorney)
- DPO searches all systems and locations for personal data
- Review data to identify any exemptions (e.g., third party data, legal privilege)
- Compile data into accessible format (usually PDF copies)
- Provide data with covering letter explaining what is provided
- Send securely (encrypted email, secure post, collection in person)
- Record SAR in SAR register with dates and actions taken

Timeframes:

- Respond within one calendar month from receipt
- Can extend by two further months if complex/multiple requests (inform requester within one month)
- If refuse request, explain reasons and right to complain to ICO

Fees:

- No fee for first request
- Can charge reasonable fee for: manifestly unfounded/excessive requests, further copies of same information, administrative costs

6.7 Rectification and Erasure

Right to Rectification:

Individuals can request correction of inaccurate or incomplete personal data.

- Must respond within one month
- If agree data is inaccurate, correct immediately
- Inform any third parties to whom data was disclosed
- If disagree, explain why and inform of right to complain to ICO
- Record request and action taken

Right to Erasure ('Right to be Forgotten'):

Individuals can request deletion of their personal data in certain circumstances:

- Data no longer necessary for original purpose
- Consent withdrawn and no other lawful basis
- Object to processing and no overriding legitimate grounds
- Data processed unlawfully
- Legal obligation requires erasure

However, we may refuse erasure if data needed for:

- Compliance with legal obligation (e.g., care records retention)
- Exercise/defence of legal claims
- Safeguarding purposes
- Public health purposes

If erase data, must inform any third parties unless impossible or disproportionate effort.

6.8 Data Retention

We retain personal data only for as long as necessary. Our retention schedule is based on legal requirements, regulatory guidance, and business needs.

Record Type	Retention Period
Adult social care records (care plans, risk assessments, care notes, correspondence)	Minimum 8 years after last contact with service (Records Management Code of Practice). May retain longer for continuing care or legal reasons.
Safeguarding records	Long-term retention (25+ years). Safeguarding Adult Reviews may require access to historical records. Maintain until individual reaches age 100 or 25 years after death if sooner.

Staff personnel files	6 years after employment ends (includes contracts, performance reviews, training records, correspondence).
Payroll records	Minimum 6 years after end of tax year (HMRC requirement). Some organisations retain 7 years.
Accident/incident records (staff)	3 years from date of accident/incident (adults). Until age 21 for anyone under 18 at time of incident.
DBS checks	Do not retain DBS certificates. Record date of check, certificate number, and decision. Destroy certificate securely once checked.
Job applications (unsuccessful)	6-12 months after recruitment decision (allow for any discrimination claims).
Complaints records	Minimum 3 years after complaint resolved. May retain longer if serious or repeat issues.
Financial records (invoices, receipts, accounts)	Minimum 6 years from end of financial year (legal requirement for tax purposes).
Policy documents	Permanent retention of current version. Superseded versions: 3 years after replacement.
Training records	Duration of employment plus 6 years. May retain longer for regulated training (e.g., moving and handling).
Email correspondence containing care/business information	Apply same retention as subject matter (e.g., care-related emails: 8 years; routine admin: delete when no longer needed).
CCTV footage (if used)	Maximum 31 days unless needed for investigation, then retain until investigation concluded.

The Data Protection Officer maintains the full retention schedule and ensures compliance. Staff must not delete or destroy records before the end of the retention period without DPO authorisation.

6.9 Secure Data Disposal

At the end of the retention period, personal data must be securely destroyed to prevent unauthorised access.

Paper records:

- Shred using cross-cut shredder (minimum DIN P-4 standard)
- For large volumes, use certified secure destruction service
- Obtain certificate of destruction for audit trail
- Never place confidential documents in general waste or recycling

Electronic data:

- Permanently delete files (empty recycle bin)
- For sensitive data, use secure deletion software (overwrites data multiple times)
- When disposing of computers/hard drives, use certified data destruction service

- Hard drives must be physically destroyed or wiped to military standard
- Obtain certificate of destruction
- Remove/destroy storage media from printers/copiers before disposal

Mobile devices:

- Perform factory reset
- Remove SIM cards and memory cards
- Physically destroy if containing highly sensitive data

All disposal activities must be logged, noting what data was destroyed, when, how, and by whom.

7. Data Breaches

A data breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Breaches must be taken seriously and handled promptly.

7.1 Identifying Data Breaches

Examples of data breaches include:

- Sending personal data to wrong email recipient
- Losing paper records or leaving them in service user's home
- Losing laptop, tablet, phone, or USB stick containing personal data
- Unauthorised access to care records by staff member
- Ransomware or cyber attack
- Discussing service users in public place
- Posting confidential information on social media
- Theft of devices or documents
- Accidental disclosure to family member not entitled to information
- Leaving filing cabinet unlocked overnight

All staff must report suspected breaches immediately – do not wait to investigate. Early reporting is essential.

7.2 Breach Containment

Immediate actions when breach identified:

- Stop the breach – prevent further disclosure (e.g., recall email if possible, retrieve lost documents, disable compromised account)
- Secure any affected systems
- Preserve evidence (do not delete emails, screenshots, logs)

- Notify Data Protection Officer immediately by phone
- Notify Registered Manager and Duty Manager
- Do not attempt to ‘fix’ the breach without DPO guidance
- For cyber incidents, isolate affected systems from network

7.3 Breach Notification

Internal notification:

- Report all suspected breaches to DPO within 1 hour of discovery
- Complete Data Breach Report Form with all known details
- DPO logs breach in Data Breach Register

ICO notification:

We must report breaches to the ICO within 72 hours if there is a risk to individuals’ rights and freedoms.

- DPO assesses risk based on: severity of breach, sensitivity of data, number of individuals affected, potential consequences, safeguards in place
- If reportable, DPO notifies ICO within 72 hours via ICO website
- Notification includes: nature of breach, categories and number of individuals affected, likely consequences, measures taken/proposed
- If cannot provide all information within 72 hours, provide initial report then update

Individual notification:

We must notify affected individuals if breach likely to result in high risk to their rights and freedoms (e.g., identity theft, financial loss, discrimination, damage to reputation).

- Notify individuals without undue delay
- Use clear, plain language
- Explain: nature of breach, contact point for more information, likely consequences, measures taken/proposed
- Provide advice on steps individuals can take to protect themselves

7.4 Breach Investigation

The DPO investigates all breaches to establish:

- Exactly what happened and when
- How breach occurred (root cause analysis)
- What data was affected and how many individuals
- Who was responsible (if relevant)
- Whether policies/procedures were followed

- What immediate actions were taken
- Whether breach could have been prevented
- What lessons can be learned

Investigation findings are documented in Data Breach Investigation Report, which includes recommendations for preventing recurrence.

7.5 Breach Prevention

Preventing breaches is far better than responding to them. Prevention measures include:

- Regular data protection training for all staff
- Clear policies and procedures
- Access controls – staff can only access data they need
- Strong password policies
- Encryption of portable devices
- Secure email protocols (check recipients before sending)
- Physical security (locked cabinets, clear desk policy)
- Regular security audits and vulnerability assessments
- Cyber security measures (firewalls, anti-virus, patching)
- Data protection impact assessments for new systems
- Learning from previous breaches
- Staff awareness campaigns and reminders

The Data Breach Register is reviewed quarterly to identify trends and systemic issues requiring action.

8. Training and Awareness

8.1 Mandatory Training

All staff must complete data protection training appropriate to their role.

Induction Training:

All new staff complete data protection module at induction covering:

- Overview of UK GDPR and Data Protection Act 2018
- This policy and how to access it
- Lawful basis for processing in care sector
- Confidentiality and information sharing
- Secure handling of records (paper and electronic)

- Password security and IT security
- Recognising and reporting data breaches
- Subject access requests
- Consequences of non-compliance

Annual Refresher Training:

All staff complete annual data protection refresher training covering:

- Updates to legislation and procedures
- Case studies and learning from breaches
- New systems or processing activities
- Reinforcement of key principles

Role-Specific Training:

- Data Protection Officer: Advanced training in GDPR compliance, breach management, DPIAs
- Managers: Training on supervision of data protection compliance, breach response, SARs
- Care Coordinators: Information sharing for care coordination, capacity and consent
- IT staff: Technical security measures, cyber security, secure disposal
- Safeguarding Lead: Information sharing for safeguarding purposes

8.2 Competency Assessment

Competency in data protection is assessed through:

- Training assessments (quiz at end of modules)
- Observation of practice during supervision
- Spot checks of record-keeping
- Audit findings
- Annual competency review as part of appraisal

Staff who demonstrate poor understanding or repeated non-compliance receive additional training and support. Serious or persistent breaches may result in disciplinary action.

8.3 Ongoing Awareness

Data protection awareness is maintained through:

- Regular bulletins and reminders via email/notice boards
- Discussion of data protection at team meetings
- Sharing lessons learned from breaches
- Data Protection Awareness Week (annually in January)

- Posters and visual reminders (e.g., ‘Lock your screen’ stickers)
- Inclusion in supervision discussions
- Updates when legislation or procedures change

9. Monitoring and Review

9.1 Audits and Inspections

Data protection compliance is monitored through:

Internal audits:

- Annual comprehensive data protection audit by DPO
- Quarterly spot checks of record storage and security
- Monthly review of access logs for unusual activity
- Regular review of retention schedule compliance
- Annual review of data sharing agreements

External audits:

- CQC inspections assess record-keeping and information governance
- Local authority contract monitoring reviews data protection compliance
- ICO may conduct compliance checks (routine or following complaint/breach)
- NHS Data Security and Protection Toolkit (if applicable)
- External data protection specialists conduct periodic reviews

9.2 Performance Indicators

We monitor data protection performance through key indicators:

- Number of data breaches reported (target: year-on-year reduction)
- Number of breaches reportable to ICO (target: zero)
- Percentage of staff up to date with data protection training (target: 100%)
- Subject Access Request response times (target: 100% within one month)
- Number of ICO complaints (target: zero)
- Audit compliance scores (target: 95%+)
- Retention schedule compliance (target: 100%)
- Number of repeat breaches of same type (target: zero)

Performance data is reviewed quarterly by senior management team and annually by board/owners.

9.3 Continuous Improvement

We are committed to continuously improving our data protection practices through:

- Learning from breaches and near misses
- Acting on audit recommendations
- Responding to changes in legislation and ICO guidance
- Implementing new technologies to enhance security
- Benchmarking against sector best practice
- Seeking staff feedback on policies and procedures
- Reviewing and updating policies annually
- Engaging with professional networks and forums

Action plans from audits, breaches, and reviews are tracked to completion with assigned responsibilities and deadlines.

10. Reporting Concerns

10.1 Internal Reporting

Staff who identify data protection concerns must report them promptly:

Data breaches:

- Report immediately to Data Protection Officer
- Also notify line manager and Duty Manager
- Complete Data Breach Report Form
- Do not delay reporting while investigating

Other concerns:

- Poor record-keeping practices
- Insecure storage of personal data
- Unauthorised access to records
- Non-compliance with policies
- Inaccurate personal data
- Systems not fit for purpose

Report to Data Protection Officer or line manager. All concerns will be taken seriously and investigated appropriately.

10.2 Whistleblowing Protection

Staff who report data protection concerns in good faith are protected under whistleblowing legislation (Public Interest Disclosure Act 1998). You will not suffer any detriment for raising legitimate concerns.

If you are uncomfortable raising concerns internally, you can:

- Contact our confidential whistleblowing hotline
- Report to CQC: 03000 61 61 61 or www.cqc.org.uk/contact-us
- Report to ICO: 0303 123 1113 or ico.org.uk/make-a-complaint
- Seek advice from Public Concern at Work: 020 7404 6609

10.3 Complaints to the ICO

Individuals who are unhappy with how we have handled their personal data can complain to the Information Commissioner's Office:

Information Commissioner's Office

Wycliffe House, Water Lane

Wilmslow, Cheshire SK9 5AF

Tel: 0303 123 1113

Email: casework@ico.org.uk

Website: ico.org.uk

We encourage individuals to contact us first so we can try to resolve concerns, but they have the right to complain directly to the ICO at any time.

11. Related Policies and Procedures

This policy should be read in conjunction with:

- Records Management Policy
- Confidentiality Policy
- Information Security Policy
- Information Sharing Policy
- Adult Safeguarding Policy
- Consent Policy
- Mental Capacity Act Policy
- Subject Access Request Procedure
- Data Breach Response Procedure

- Secure Email Protocol
- Password Policy
- Social Media Policy
- Bring Your Own Device (BYOD) Policy
- Data Retention Schedule
- Privacy Notices (Service Users, Staff, Job Applicants)

12. Document Information

Policy Owner	**Data Protection Officer**
Approved By	Board of Directors / Senior Management Team
Review Date	Annual or sooner if legislative/regulatory changes
Related Legislation	UK GDPR, Data Protection Act 2018, Health and Social Care Act 2008, Care Act 2014, Human Rights Act 1998, Computer Misuse Act 1990, Common Law Duty of Confidentiality, Records Management Code of Practice 2016
CQC Standards	Regulation 17: Good Governance
Distribution	All staff (mandatory reading) CQC (on request) ICO (on request) Service users (on request)
Key Contacts	Data Protection Officer: Registered Manager: ICO Helpline: 0303 123 1113 ICO Website: ico.org.uk

Policy Approval & Review

APPROVED BY	SIGNATURE
Not Specified	*No signature on file*
REVIEW DATE	NEXT REVIEW DATE
1 January 1970	**18 February 2027**