UT COMPLIANCE

A TRADING NAME OF UNIQUE TENDERS LIMITED

POLICY DOCUMENT

Information Governance and Data Protection Policy

UT Compliance

BUNDLE PACKAGE | DOMICILIARY CARE

DOCUMENT REFERENCE —	EFFECTIVE DATE 15 January 2026
VERSION DC/IGD/002	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 policy establishes ‘s framework for information governance and data protection, ensuring personal and sensitive information is handled lawfully, securely, and ethically. It sets out our approach to protecting confidentiality, managing NHS care records, recording telephone and telehealth consultations, and complying with UK GDPR and Data Protection Act 2018. The policy protects service users’ privacy rights whilst enabling appropriate information sharing for safe, effective care delivery.

1.2 Application

This policy applies to all information processed by in any format including paper records, electronic systems, emails, photographs, audio recordings, and video recordings. It covers all staff, contractors, volunteers, students, and anyone acting on our behalf who access, use, or share personal information. The policy applies to all personal data including service user records, staff information, and business data.

1.3 Key Areas Covered

This policy specifically addresses:

NHS Care Records: Access to, use of, and sharing of NHS care records including Summary Care Record, GP Connect, and shared care records.

Recording of Telephone Calls: Policies and procedures for recording telephone conversations including consent requirements, storage, access, and retention.

Recording of Telehealth Consultations: Framework for recording remote consultations via video or telephone including clinical, legal, and technical requirements.

Confidentiality: Principles of confidentiality, when information can be shared, and management of confidential information.

Handling Personal Data: Lawful processing, data minimisation, accuracy, storage, security, and data subject rights.

1.4 Information Governance Principles

Our information governance is founded on:

Confidentiality: Information shared in confidence will be respected and protected

Integrity: Information will be accurate, complete, and reliable

Availability: Information will be accessible when needed for legitimate purposes

Accountability: Clear responsibility for information management and data protection

Transparency: Open about how we use personal information

Security: Robust measures protecting information from unauthorised access, loss, or damage

1.5 Interface with Clinical Practice

Information governance enables safe, effective care by ensuring clinicians have access to accurate information whilst protecting service users' privacy and dignity. This policy balances clinical need for information with legal and ethical duties of confidentiality.

2. Legal and Regulatory Framework

Information governance and data protection are governed by comprehensive legal frameworks:

Legislation/Framework	Data Protection Requirements
UK General Data Protection Regulation (UK GDPR)	Establishes data protection principles, lawful bases for processing, data subject rights, security requirements, breach notification, and accountability obligations. Directly applicable UK law post-Brexit.
Data Protection Act 2018	UK's implementation of GDPR including special category data provisions, law enforcement processing, and Information Commissioner powers. Supplements UK GDPR.
Common Law Duty of Confidentiality	Legal obligation to protect information shared in confidence. Breach can result in civil litigation. Applies to healthcare relationships with implied duty of confidence.
Human Rights Act 1998	Article 8 protects right to private and family life including confidentiality of personal information. Balances privacy with other rights and public interest.
Health and Social Care Act 2012 (Section 251)	Provides legal basis for sharing confidential patient information without consent in specific circumstances with appropriate authorisation.
Health and Social Care (Safety and Quality) Act 2015	Establishes duty of candour and requirements for transparency in healthcare including information provision to patients and families.
Care Act 2014	Requires information sharing for safeguarding, establishes information and advice duties, and supports integrated care through appropriate information sharing.
Regulation of Investigatory Powers Act 2000	Regulates interception of communications including telephone call recording. Establishes lawful purposes and safeguards for surveillance.
Computer Misuse Act 1990	Criminalises unauthorised access to computer systems, data modification, and cyber-attacks. Applies to electronic health record systems.
CQC Regulation 17 (Good Governance)	Requires systems ensuring integrity and confidentiality of information, accuracy of records, and compliance with data protection legislation.
NHS Digital Data Security and Protection Toolkit	Framework assessing information governance and cyber security standards for organisations accessing NHS patient data. Annual submission required.
Caldicott Principles (Updated 2013)	Seven principles governing use of confidential patient information: justify purpose, don't use unless necessary, use minimum necessary, access on need-to-know, everyone understands responsibilities, comply with law, duty to share for care.

NHS Code of Practice on Confidential Information	Guidance on protecting confidentiality in NHS and social care, information sharing protocols, and patient rights regarding their information.
Professional Standards (NMC, HCPC, etc.)	Professional codes require maintaining confidentiality, protecting patient information, and appropriate information sharing. Breaches are fitness to practise matters.

3. Definitions of Key Terms

The following information governance and data protection terminology applies:

Term	Definition
Personal Data	Information relating to identified or identifiable living individual. Includes names, addresses, identifiers, and any data that could identify someone when combined with other information.
Special Category Data	Sensitive personal data requiring extra protection including health information, racial or ethnic origin, religious beliefs, sexual orientation, genetic data, biometric data, and criminal convictions.
Data Controller	Organisation determining purposes and means of processing personal data. is data controller for service user and staff information we hold.
Data Processor	Organisation processing personal data on behalf of data controller. Examples include IT service providers, payroll companies, and cloud storage providers.
Data Subject	Individual to whom personal data relates. Service users and staff are data subjects with rights under UK GDPR.
Processing	Any operation on personal data including collection, recording, organisation, storage, alteration, consultation, use, disclosure, restriction, erasure, or destruction.
Lawful Basis	Legal ground permitting processing of personal data. Six bases: consent, contract, legal obligation, vital interests, public task, legitimate interests. Health data requires additional condition.
Consent	Freely given, specific, informed, and unambiguous indication of data subject's wishes. Must be clear affirmative action. Can be withdrawn at any time.
Data Breach	Security incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data. Must be reported to ICO within 72 hours if risk to individuals.
Pseudonymisation	Processing personal data so it cannot be attributed to specific data subject without additional information kept separately. Reduces privacy risks whilst maintaining utility.
Anonymisation	Permanently removing identifying information so individual cannot be identified by any means. Anonymised data is not personal data and GDPR does not apply.
Data Protection Impact Assessment (DPIA)	Process assessing privacy risks of new projects or systems processing personal data. Required for high-risk processing before implementation.

Information Asset	Body of information defined and managed as single unit. Examples include care records database, staff personnel files, and financial records.
Need to Know	Principle that access to information should be limited to those requiring it for legitimate purposes. Prevents unnecessary disclosure.
Summary Care Record (SCR)	Electronic record of important patient information from GP systems including medications, allergies, and adverse reactions. Accessible to authorised NHS staff.
Information Sharing Agreement	Formal agreement between organisations defining what information will be shared, for what purpose, legal basis, security arrangements, and responsibilities.

4. Policy Statement

4.1 Commitment to Data Protection

is committed to protecting the privacy, dignity, and confidentiality of service users, staff, and all individuals whose information we process. We will handle personal data lawfully, fairly, and transparently in accordance with UK GDPR, Data Protection Act 2018, and professional standards. Information governance is integral to providing safe, high-quality care and maintaining public trust.

4.2 Data Protection Principles

We commit to the UK GDPR data protection principles:

Lawfulness, Fairness, Transparency: Process personal data lawfully with transparency about how we use it

Purpose Limitation: Collect data for specified, explicit, legitimate purposes only

Data Minimisation: Process only data adequate, relevant, and necessary for purposes

Accuracy: Keep personal data accurate and up to date, correct or delete inaccurate data

Storage Limitation: Retain data only as long as necessary for purposes

Integrity and Confidentiality: Process data securely with protection against unauthorised access, loss, or damage

Accountability: Demonstrate compliance with principles through policies, training, and documentation

4.3 Balancing Privacy and Care

We balance protecting confidentiality with ensuring appropriate information sharing for safe, effective care. Information will be shared with consent where possible, or under appropriate legal basis where necessary for care delivery, safeguarding, or legal requirements. The Caldicott Principle ‘duty to share information can be as important as duty to protect patient confidentiality’ guides our approach.

4.4 Rights of Data Subjects

We respect and facilitate data subject rights under UK GDPR:

Right to be informed about data processing

Right of access to personal data

Right to rectification of inaccurate data

Right to erasure in specified circumstances

Right to restrict processing

Right to data portability

Right to object to processing

Rights regarding automated decision-making

5. Roles and Responsibilities

Effective information governance requires clear allocation of roles and collective responsibility:

Role	Information Governance Responsibilities
All Staff	Maintain confidentiality of personal information. Only access information needed for role. Follow data security procedures. Report data breaches immediately. Complete annual information governance training. Respect data subject rights. Never share passwords or leave systems unattended. Challenge inappropriate information access or sharing.
Registered Manager ()	Overall accountability for information governance and data protection compliance. Act as Senior Information Risk Owner (SIRO). Ensure adequate resources for data protection. Report data protection matters to board. Oversee Data Security and Protection Toolkit submission. Champion data protection culture. Approve information governance policies. Ensure legal compliance.
Duty Manager	Monitor daily compliance with information governance procedures. Ensure staff follow confidentiality protocols. Coordinate initial response to data breaches during shifts. Check secure storage of records. Verify staff access controls appropriate for roles. Report information governance concerns. Brief staff on data protection requirements. Support staff with information sharing decisions.
Data Protection Officer ()	Advise organisation on data protection obligations. Monitor compliance with UK GDPR and Data Protection Act. Conduct Data Protection Impact Assessments. Act as contact point for ICO and data subjects. Provide expert advice on information governance. Investigate data breaches. Deliver data protection training. Maintain data protection documentation. Review contracts with data processors.
Caldicott Guardian	Senior clinical professional responsible for confidential patient information. Advise on lawful and ethical information sharing. Review information sharing agreements. Champion confidentiality. Approve access to NHS care records. Oversee Summary Care Record usage. Investigate confidentiality breaches. Ensure Caldicott Principles embedded.
Information Asset Owners	Responsible for specific information assets (care records, HR files, etc.). Understand information flows and risks. Maintain asset registers. Ensure appropriate access controls. Review security measures. Report incidents affecting asset. Conduct regular reviews. Implement retention schedules.

IT Manager/System Administrator	Implement technical security measures. Manage user access rights. Monitor system security. Apply security patches and updates. Configure firewalls and encryption. Backup data regularly. Maintain audit logs. Respond to cyber security threats. Ensure secure disposal of IT equipment.
Records Manager	Oversee records management systems. Implement retention schedules. Coordinate secure storage and archiving. Manage records disposal. Respond to subject access requests. Maintain records inventory. Ensure compliance with records standards. Train staff on records management.
Safeguarding Lead ()	Advise on information sharing for safeguarding. Navigate confidentiality vs safeguarding tensions. Coordinate multi-agency information sharing. Ensure lawful processing of safeguarding information. Maintain safeguarding records securely. Report to safeguarding boards appropriately.
Training Lead	Deliver mandatory information governance training. Ensure all staff complete annual training. Provide role-specific training (SCR access, recording calls, etc.). Assess staff competency. Update training based on incidents and changes. Maintain training records.
Quality Assurance Lead	Audit information governance compliance. Monitor data quality and accuracy. Review data breaches for learning. Assess effectiveness of controls. Report compliance to governance meetings. Identify improvement opportunities. Benchmark against standards.

6. NHS Care Records

6.1 Summary Care Record (SCR)

The Summary Care Record provides authorised healthcare staff with access to key patient information from GP records:

Access Authorisation:

Only clinically qualified staff with NHS Smartcard or Care Identity Service access

Role-Based Access Control ensuring appropriate permissions

Named individual registration with NHS Digital

Legitimate relationship with patient required

Training on SCR usage before access granted

When to Access SCR:

Emergency situations requiring urgent clinical information

Unplanned care delivery when GP records unavailable

Medication reconciliation to prevent errors

Checking allergies and adverse reactions

Never access for curiosity or non-clinical purposes

Patient Consent:

Express consent preferred – inform patient you need to access their SCR and why

Implied consent acceptable in emergency when express consent not possible

Respect if patient opts out or requests restricted access

Document SCR access and consent in care records

Audit Trail:

Every SCR access is automatically logged

Audits review appropriateness of access

Inappropriate access may result in disciplinary action and ICO referral

Patients can request access logs through GP

6.2 GP Connect and Shared Care Records

Where we have access to GP Connect or local shared care records:

Access limited to authorised staff with clinical need

Information Sharing Agreements in place with GP practices and local systems

Clear processes for contributing information to shared records

Data quality responsibilities understood

Patient consent obtained where required by local agreements

Regular reviews of access appropriateness

6.3 Transferring NHS Records

When service users transfer between services:

Share relevant clinical information with receiving service

Use secure NHS email (nhs.net) or secure file transfer

Obtain consent for sharing or rely on lawful basis

Share minimum necessary information for continuity of care

Document information sharing in records

Retain copy in accordance with retention schedule

7. Recording of Telephone Calls

7.1 Purpose and Legal Basis

may record telephone calls for the following purposes:

Quality assurance and training for customer service improvement

Evidence in complaints, disputes, or safeguarding investigations

Compliance monitoring and regulatory requirements

Protection of staff from abuse or threats

Clinical documentation where telephone is sole contact method

Legal basis: Legitimate interests (quality assurance, compliance, protection) or consent depending on context. Call recording is subject to GDPR and Regulation of Investigatory Powers Act 2000.

7.2 Consent and Notification Requirements

Informing Callers:

Automated message at start of call: ‘This call may be recorded for quality and training purposes’

Verbal notification by staff member if no automated system

Caller continuing after notification implies consent

If caller objects, stop recording and note objection

Staff Making Outbound Calls:

Inform recipient at start: ‘I’m calling from [company], this call is being recorded for quality and training purposes’

Obtain verbal consent to proceed with recording

If consent refused, do not record

Document consent or refusal in records

7.3 Recording Systems and Security

Call recordings must be:

Stored on secure systems with encryption

Access restricted to authorised staff only

Protected by robust passwords and authentication

Backed up regularly to prevent loss

Retained according to retention schedule (typically 2-6 years)

Securely deleted after retention period expires

Never stored on personal devices

7.4 Access to Recordings

Who Can Access:

Quality assurance staff for monitoring purposes

Managers investigating complaints or incidents

Safeguarding investigators where recording is evidence

Legal team if litigation arises

Regulators (CQC, ICO) upon lawful request

Data subjects exercising right of access

Access Procedures:

Request access through Data Protection Officer

Justify legitimate need for access

Document access in audit log

Never share recordings via insecure methods

7.5 Subject Access Requests

Individuals have right to request copies of recordings:

Respond within one month of valid request

Verify identity before releasing recordings

Redact third-party voices to protect their privacy

Provide recordings in accessible format

Free of charge unless request manifestly unfounded or excessive

7.6 Calls NOT to Record

Never record:

Personal calls on company phones

Calls after caller explicitly refuses consent

Calls to helplines, counselling services, or support organisations

Calls involving highly sensitive disclosures unless essential and consented

8. Recording of Telehealth Consultations

8.1 Telehealth Definition and Scope

Telehealth consultations include remote clinical assessments, reviews, and interventions delivered via:

Video consultations (Zoom, MS Teams, Attend Anywhere, etc.)

Telephone consultations with clinical content

Remote monitoring reviews

Virtual ward rounds

8.2 Purpose and Clinical Justification

Telehealth consultations may be recorded for:

Clinical record-keeping and documentation

Second opinion or specialist review

Training and clinical supervision

Safeguarding evidence

Quality assurance and clinical governance

Research with appropriate ethical approval

Recording should be exception not routine. Clinical benefit must justify privacy intrusion.

8.3 Consent Requirements

Explicit Informed Consent Required:

Explain to service user that consultation will be recorded

State purpose of recording clearly

Explain who will have access to recording

Inform of retention period

Clarify right to refuse recording (consultation can still proceed)

Obtain verbal consent at start of consultation

Document consent in clinical records

If refused, proceed without recording

Consent Script Example:

‘Good morning. Before we begin, I’d like your permission to record this consultation. The recording will be saved to your clinical record and may be reviewed by [purpose]. It will be stored securely for [time period]. You’re free to decline – we can still have our consultation without recording. Do I have your consent to record?’

8.4 Technical Requirements

Recording systems must:

Use approved, secure platforms (NHS-approved where available)

Encrypt recordings in transit and at rest

Store within UK or ensure GDPR-compliant international transfers

Provide clear visual/audio indicators when recording active

Allow participants to pause/stop recording

Integrate with or link to electronic care records

Meet cyber security standards (DSP Toolkit compliance)

8.5 Storage and Access

Storage Requirements:

Save recording to service user’s electronic care record

Tag/label with consultation date, clinician, and purpose

Protect with access controls – clinical team only

Delete local copies after transfer to care record

Retain as per clinical records retention schedule (typically 8 years)

Access Controls:

Clinically qualified staff with legitimate relationship only

Audit all access to recordings

Patients can access own recordings via subject access request

Never share via social media, messaging apps, or insecure email

8.6 Patient Rights

Service users have right to:

Decline recording without affecting care provision

Request recording be paused during sensitive discussion

Withdraw consent and request deletion (if no legal basis to retain)

Access copy of recording via subject access request

Complaint if recording used inappropriately

9. Confidentiality

9.1 Duty of Confidentiality

All staff have legal, ethical, and professional duty to maintain confidentiality:

Information shared in healthcare relationship is confidential

Implied duty of confidence exists without need for explicit agreement

Applies to all information learned about service users

Continues after care relationship ends

Extends beyond death (confidentiality survives deceased)

Breaching confidentiality may constitute professional misconduct, civil wrong, or criminal offence

9.2 When Information Can Be Shared

Confidential information may be shared:

With Consent: Service user gives explicit permission to share. Preferred route for information sharing.

Without Consent – Legal Basis:

Direct care: Within care team for treatment, diagnosis, care planning

Safeguarding: To protect vulnerable adult or child from harm

Public interest: Prevention, detection, or prosecution of serious crime

Legal obligation: Court order, statutory requirement, coroner request

Vital interests: Life-threatening emergency when consent cannot be obtained

Decision to share without consent must be justified, documented, and proportionate. Share minimum necessary information.

9.3 Information Sharing Principles

Apply these principles when sharing information:

Seek consent where possible before sharing

Share only what is necessary for purpose

Share only with those who need to know

Use secure methods (NHS mail, encrypted systems)

Document what was shared, with whom, when, and why

Consider whether anonymisation/pseudonymisation sufficient

Inform service user of sharing unless contraindicated

9.4 Common Confidentiality Scenarios

Family Members Requesting Information:

Cannot share without service user's consent unless best interests decision for person lacking capacity. Family relationship does not automatically grant information rights.

Other Healthcare Professionals:

Can share relevant clinical information for direct care purposes. Ensure recipient has legitimate need and secure systems.

Social Services/Local Authority:

Share for safeguarding, care planning, or statutory assessments. Document lawful basis and information shared.

Police Requests:

Share without consent if serious crime prevention/investigation. Otherwise require consent, court order, or legal advice. Document decision carefully.

Insurance Companies/Solicitors:

Require explicit written consent from service user. Verify identity and authenticity of request. Share only information specified in consent.

9.5 Maintaining Confidentiality in Practice

Staff must:

Never discuss service users in public places

Avoid using names in corridors or public areas

Dispose of confidential waste securely (shredding)

Lock paper files when not in use

Log out of systems when leaving desk

Position screens away from public view

Use private spaces for confidential phone calls

Challenge others who breach confidentiality

10. Handling Personal Data

10.1 Lawful Bases for Processing

processes personal data under the following lawful bases:

For Care Delivery:

Contract: Processing necessary to fulfil care contract

Vital interests: Protecting life in emergencies

Special category condition: Health and social care purposes (Article 9(2)(h))

For Staff Management:

Contract: Employment relationship

Legal obligation: Tax, pensions, employment law compliance

Legitimate interests: Business administration, HR management

For Marketing:

Consent: Explicit opt-in for marketing communications

10.2 Data Minimisation

Only collect and process personal data that is:

Adequate: Sufficient for the purpose

Relevant: Directly related to purpose

Necessary: Cannot achieve purpose without it

Do not collect ‘just in case’ or for unclear future purposes. Regularly review data holdings and delete unnecessary information.

10.3 Data Accuracy

Ensure personal data is accurate and up to date:

Verify information at point of collection

Review and update records regularly

Correct errors promptly when identified

Respond to data subject rectification requests

Document corrections in audit trail

Inform third parties of corrections where data shared

10.4 Data Retention

Personal data retained only as long as necessary:

Service user clinical records: 8 years from last contact (adults), longer for children

Staff employment records: 6 years after employment ends

Financial records: 6 years for tax purposes

Safeguarding records: Until case closed plus retention period as per local policy

CCTV footage: 30 days unless incident requires retention

Email: Delete after business purpose complete unless record-keeping needed

Full retention schedule available from Records Manager. Data must be securely destroyed after retention period expires.

10.5 Secure Processing

Protect personal data through:

Technical Measures:

Encryption of data at rest and in transit

Firewalls and anti-virus protection

Regular security patches and updates

Secure password policies

Multi-factor authentication where available

Backup and disaster recovery

Access controls and authentication

Organisational Measures:

Clear desk and clear screen policies

Secure storage of paper records

Confidential waste disposal procedures

Staff training on data security

Incident response procedures

Regular security audits

Visitor access controls

11. Data Subject Rights

11.1 Right of Access (Subject Access Request)

Data subjects can request copies of their personal data:

Respond within one month of valid request

Verify identity before releasing information

Provide information in accessible format

Include supplementary information (purposes, recipients, retention)

Redact third-party information requiring protection

Free of charge unless manifestly unfounded or excessive

Log request and response in data protection register

11.2 Right to Rectification

Data subjects can request correction of inaccurate data:

Respond within one month

Correct inaccurate data promptly

If disputed, note disagreement in record

Inform third parties of corrections where data shared

Cannot alter clinical opinion, only factual errors

11.3 Right to Erasure

Limited right to deletion in specific circumstances:

Where consent was basis and withdrawn

Where processing unlawful

Where no longer necessary for original purpose

Exemptions apply: Legal obligation to retain, public interest, establishment of legal claims. Clinical records rarely eligible for erasure due to professional and legal retention requirements.

11.4 Other Rights

Right to Restriction: Limit processing in specific circumstances while accuracy or lawfulness determined.

Right to Portability: Receive personal data in structured, machine-readable format for transfer to another controller.

Right to Object: Object to processing based on legitimate interests or direct marketing. Must stop unless compelling legitimate grounds override.

12. Data Breaches

12.1 What Constitutes a Data Breach

A breach of security leading to accidental or unlawful:

Loss of personal data

Theft or unauthorised access

Alteration, destruction, or corruption

Disclosure to unauthorised recipients

Examples: Lost laptop, misdirected email, unauthorised system access, ransomware attack, records left in public place.

12.2 Reporting Data Breaches

All staff must report suspected breaches immediately:

Contact Data Protection Officer or Duty Manager immediately

Complete incident report form

Preserve evidence (do not delete)

Do not attempt to investigate alone

12.3 Breach Response Process

DPO coordinates response following this process:

1. Containment (within hours):

Stop the breach if ongoing

Recover compromised data where possible

Prevent further access or disclosure

2. Assessment (within 24 hours):

Determine type and volume of data affected

Assess risk to individuals

Identify cause and contributing factors

Decide if ICO notification required

3. Notification (within 72 hours):

Report to ICO if likely risk to individuals

Notify affected individuals if high risk

Inform other regulators/parties as required

Document decision not to notify if below threshold

4. Remediation and Learning:

Implement preventive measures

Review and strengthen controls

Deliver targeted training

Update policies where needed

Share learning across organisation

13. Training and Development

13.1 Mandatory Training

All staff complete annual information governance training covering:

UK GDPR and Data Protection Act 2018 principles

Confidentiality and information sharing

Data subject rights

Data security and breach prevention

Recognising and reporting data breaches

Cyber security awareness

Records management

13.2 Role-Specific Training

Additional training provided for:

NHS Smartcard holders: Summary Care Record access training

Staff recording calls/consultations: Consent and recording procedures

Managers: Information governance responsibilities, breach management

New starters: Induction covering policy and procedures

13.3 Competency Assessment

Staff competency assessed through:

E-learning completion tests

Scenario-based assessments

Supervision observations

Audit of record-keeping practice

14. Monitoring and Review

14.1 Compliance Monitoring

Information governance compliance monitored through:

Quarterly audits of data protection practices

Annual Data Security and Protection Toolkit submission

Review of data breaches and incidents

Subject access request response times

Training completion rates

System access audits

Records quality reviews

14.2 Key Performance Indicators

100% staff complete annual IG training

Zero significant data breaches

95% subject access requests responded within one month

Data Security and Protection Toolkit standards met

Zero ICO enforcement actions

14.3 Policy Review

This policy reviewed annually and following:

Changes to data protection legislation

Significant data breaches

ICO guidance updates

CQC inspection feedback

Organisational changes affecting data processing

15. Reporting Concerns

15.1 Internal Reporting

Report information governance concerns through:

Data Protection Officer:

Duty Manager for immediate issues

Caldicott Guardian for confidentiality concerns

Incident reporting system

Whistleblowing procedures for serious breaches

15.2 External Reporting

Data subjects or staff may report concerns to:

Information Commissioner's Office (ICO): 0303 123 1113 / casework@ico.org.uk

Care Quality Commission: 03000 616161

Local Authority commissioning team

16. Related Policies and Procedures

This policy should be read alongside:

Consent Policy

Mental Capacity Act Policy

Safeguarding Adults Policy

Records Management Policy

Information Security Policy

Cyber Security Policy

Social Media Policy

Photography and Video Recording Policy

Subject Access Request Procedure

Data Breach Response Procedure

This document is confidential. It must be stored securely and only accessed by authorised personnel. Unauthorised disclosure may constitute a data breach.

Policy Approval & Review

APPROVED BY	SIGNATURE
Not Specified	*No signature on file*
REVIEW DATE	NEXT REVIEW DATE
1 January 1970	**17 February 2027**