New

Confidentiality Policy + Templates

PRO

Version Control

Date	Version	Change
12 March 25	1.0	Publication

Template Customisation and Usage Guide [DELETE WHEN READY]

Customising Your Policy Template

This template is a guideline and must be customised to reflect your organisation's operations, regulatory obligations, and internal controls. Replace all placeholder text with business-specific information to align with your processes, risk framework, and compliance structure.

*****This guidance and footer graphic should be removed from the final saved version*****

Using This Template

This template provides a comprehensive framework to help your organisation develop a policy that meets regulatory requirements and industry best practices. While structured to align with FCA expectations, you must review and adjust the content to reflect your organisation's compliance framework, sector-specific risks, and operational procedures.

If your organisation has policies related to this document, ensure that relevant cross-references are included. Some of the policies referenced are available separately or as part of bundled compliance toolkits.

Licence and Usage Terms

Disclaimer

This template supports regulatory compliance and governance, but does not constitute legal or professional advice. While designed for accuracy and relevance, your organisation ensures compliance with FCA regulations, industry standards, and legal requirements.

Customise this document to reflect your business model, risk exposure, and internal policies. If unsure of your regulatory or legal obligations, seek professional advice before finalising.

Use of this template assumes no liability for loss, damage, or regulatory action.

1. Introduction

This Confidentiality Policy establishes the framework for managing and protecting confidential information within [The Organisation] (hereinafter referred to as "the Organisation"). It draws upon best practices from sectors such as healthcare, charitable organisations, and regulated financial services, ensuring alignment with contemporary legal standards and ethical obligations. The policy integrates insights from key reference materials, including NHS England's Confidentiality Policy, Age UK Carlisle and Eden's Confidentiality Policy, and comprehensive confidentiality manuals for regulated entities. As of August 2025, this policy reflects the latest developments in UK data protection law, including the Data (Use and Access) Act 2025 (DUAA), which updates aspects of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 to facilitate innovation while upholding robust safeguards.

The policy emphasises a proactive approach to confidentiality, fostering a culture of accountability and transparency. It is designed to mitigate risks associated with data breaches, unauthorised disclosures, and non-compliance, thereby protecting individuals' privacy rights and maintaining the Organisation's reputation.

1.1 Purpose of the Policy

The primary purpose of this policy is to outline the principles, procedures, and responsibilities that must be observed by all individuals associated with the Organisation when handling confidential information. This includes personal data, sensitive business information, and any other data that could cause harm if disclosed inappropriately. By establishing clear guidelines, the policy aims to:

- Ensure compliance with applicable UK and international laws, including the UK GDPR, Data Protection Act 2018, and the newly enacted Data (Use and Access) Act 2025, which introduces reforms to streamline data processing while preserving essential protections.
- Safeguard the confidentiality, integrity, and availability of information, preventing unauthorised access, use, or disclosure that could lead to harm, discrimination, or financial loss.
- Promote ethical handling of information in line with principles such as the Caldicott Principles (updated to eight principles in 2021, with no further changes noted as of 2025), which guide the use of patient-identifiable information in health and social care contexts.
- Support the Organisation's operational objectives by enabling secure information sharing where necessary, such as in collaborative partnerships or regulatory reporting, while minimising risks.
- Provide a mechanism for identifying, reporting, and responding to breaches, ensuring swift remediation and continuous improvement.

This policy serves as a foundational document for all related procedures, training programmes, and audits, ensuring that confidentiality is embedded in the Organisation's daily operations.

1.2 Scope and Applicability

This policy applies to all individuals who have access to confidential information through their association with the Organisation, regardless of their role or location. It encompasses:

- Permanent and temporary employees, including senior management, line managers, and administrative staff.
- Trustees, board members, volunteers, and interns.
- Contractors, consultants, third-party service providers, and external partners (e.g., IT vendors or collaborative organisations).
- Any other individuals or entities handling information on behalf of the Organisation, such as in joint ventures or data-sharing agreements.

The policy covers all forms of confidential information, whether held in physical, digital, or verbal formats, including but not limited to:

- Personal data (e.g., names, addresses, health records) and special category data (e.g., ethnic origin, religious beliefs, biometric data).
- Organisational data (e.g., financial reports, trade secrets, procurement details).
- Information is processed in various environments, such as office settings, remote working, mobile devices, or cloud storage.

Exclusions: This policy does not apply to anonymised data where individuals cannot be identified, nor does it override statutory obligations for disclosure (e.g., under court orders). It must be read in conjunction with related policies, such as the Data Protection Policy and Information Security Policy. The policy is applicable across all UK operations and extends to international activities where cross-border data transfers occur, subject to adequacy decisions and safeguards as per the UK GDPR.

Geographical scope includes all UK jurisdictions, with considerations for devolved administrations (e.g., Scotland, Wales, Northern Ireland) where additional regulations may apply.

1.3 Key Definitions

To ensure clarity and consistent application, the following key terms are defined as per relevant legislation and best practices:

- Confidential Information: Any data that is not publicly available and whose disclosure could cause harm, including personal data, business-sensitive information, or trade secrets. This encompasses information identifiable to an individual (e.g., name, NHS number, postcode) or organisation (e.g., contracts, financial strategies).
- Personal Data: Information relating to an identified or identifiable living individual, as defined under the UK GDPR and Data Protection Act 2018 (e.g., contact details, IP addresses, genetic data).
- Special Category Data: Sensitive personal data requiring higher protection, including health information, racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, and data concerning sexual orientation.

- Breach of Confidentiality: Any unauthorised access, use, disclosure, alteration, or destruction of confidential information, whether intentional or accidental, leading to potential harm or non-compliance.
- Data Controller: The Organisation, as the entity determining the purposes and means of processing personal data.
- Data Processor: Any third party processing data on behalf of the Organisation, bound by contractual confidentiality obligations.
- Caldicott Guardian: A senior role (where applicable, e.g., in health-related organisations) responsible for protecting patient confidentiality and enabling appropriate information sharing.
- Common Law Duty of Confidence: A legal obligation to protect information shared in confidence, enforceable through courts, unless overridden by public interest or legal requirements.

A full glossary is provided in Appendix E for additional terms.

1.4 Policy Objectives and Principles

The objectives of this policy are to:

- Protect the rights and freedoms of individuals by ensuring confidential information is handled lawfully, fairly, and transparently.
- Minimise risks of data breaches through robust controls, training, and monitoring.
- Facilitate secure information sharing where it benefits service delivery, research, or public interest, while obtaining necessary consents.
- Achieve and maintain compliance with evolving regulations, including the integrity and confidentiality principle under the UK GDPR (Article 5(1)(f)), which requires appropriate security measures against unauthorised processing.
- Promote a culture of confidentiality, where breaches are reported promptly and lessons are learned to prevent recurrence.

Core principles underpinning this policy, aligned with the UK GDPR and Caldicott Principles, include:

- Lawfulness, Fairness, and Transparency: Process information only with a valid legal basis and inform individuals about its use.
- Purpose Limitation: Use data only for specified, explicit purposes.
- Data Minimisation: Collect and retain only necessary information.
- Accuracy: Keep data up-to-date and rectify inaccuracies promptly.
- Storage Limitation: Retain data only as long as necessary.
- Integrity and Confidentiality: Implement security measures to protect against risks.
- Accountability: Demonstrate compliance through records, audits, and impact assessments.
- Caldicott-Specific (if applicable): Justify uses, minimise identifiable data, and ensure access on a strict need-to-know basis.

These principles guide all decision-making and are embedded in training and procedures.

2. Legal and Regulatory Framework

This chapter outlines the legal and regulatory obligations governing confidentiality within the Organisation as of August 2025. It incorporates key developments, such as the Data (Use and Access) Act 2025 (DUAA), which amends existing data protection frameworks to promote innovation while upholding stringent safeguards. The framework draws from statutory legislation, common law, and sector-specific guidance, ensuring the Organisation's practices align with requirements from healthcare, charitable, and financial sectors as reflected in reference materials like NHS England's policy, Age UK Carlisle and Eden's guidelines, and regulated confidentiality manuals. Compliance with these obligations is mandatory to protect individuals' rights, prevent breaches, and avoid severe penalties.

The DUAA, receiving Royal Assent on 19 June 2025, introduces targeted reforms to the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018), and Privacy and Electronic Communications Regulations 2003 (PECR), without replacing them. These changes, phased in between June 2025 and June 2026, aim to simplify processes, clarify research provisions (e.g., allowing broad consent for scientific research), and facilitate responsible data sharing for purposes like crime prevention and innovation. The Organisation must monitor implementation guidance from the Information Commissioner's Office (ICO) to adapt accordingly.

2.1 Overview of Applicable UK and EU Legislation

The UK's data protection regime, post-Brexit, is primarily governed by the UK GDPR and DPA 2018, as amended by the DUAA 2025. These laws regulate the processing of personal data, including collection, use, storage, and disclosure, with a focus on protecting individuals' privacy rights.

Key UK legislation includes:

- UK General Data Protection Regulation (UK GDPR): Retained EU law post-Brexit, it sets out principles for lawful processing (e.g., lawfulness, fairness, transparency), data subject rights (e.g., access, erasure), and obligations for controllers and processors. Amendments under the DUAA clarify provisions for scientific research, broad consent, and automated decision-making to foster innovation.
- Data Protection Act 2018 (DPA 2018): Complements the UK GDPR by providing UK-specific rules, such as exemptions for national security, law enforcement processing, and the appointment of a Data Protection Officer (DPO). Section 170 criminalises the unlawful obtaining or disclosure of personal data, with penalties including fines or imprisonment.
- Human Rights Act 1998: Incorporates Article 8 of the European Convention on Human Rights, protecting the right to respect for private and family life. Disclosures must be proportionate and necessary to avoid breaching this right.
- Privacy and Electronic Communications Regulations 2003 (PECR): Regulates electronic marketing, cookies, and communications confidentiality, amended by the DUAA to align with modern digital practices.
- Sector-Specific Laws: For health and care contexts, the Care Act 2014 and Children Acts 1989/2004 impose duties to safeguard vulnerable individuals' information. The Health Service

(Control of Patient Information) Regulations 2002 enable sharing for public health purposes under Section 251 approvals.

EU legislation remains relevant for cross-border activities or EU data subjects, primarily through the EU GDPR (Regulation (EU) 2016/679). The UK's adequacy decision with the EU, renewed in 2021, is under scrutiny in 2025, which could impact data transfers if compatibility issues arise. The Organisation must ensure equivalence in standards to maintain seamless EU-UK data flows.

Additional guidance includes the Caldicott Principles (updated to eight in 2021), NHS Confidentiality Code of Practice 2003, and NHS Care Record Guarantee, which emphasise justifying uses, minimising identifiable data, and enabling patient choice.

2.2 Key Regulatory Requirements from Relevant Authorities

Regulatory oversight is provided by bodies such as the Information Commissioner's Office (ICO), Financial Conduct Authority (FCA) for regulated firms, and Health Research Authority (HRA) for health data.

Key requirements include:

- ICO Requirements: As the UK's data protection authority, the ICO enforces the UK GDPR and DPA 2018. Organisations must register if processing personal data (unless exempt), conduct Data Protection Impact Assessments (DPIAs) for high-risk processing, and report breaches within 72 hours if they risk rights and freedoms. The DUAA enhances ICO powers for innovation-friendly enforcement, such as guidance on Smart Data schemes.
- FCA Requirements (if applicable): Under the Financial Services and Markets Act 2000 (FSMA), firms must protect client data per SYSC (Senior Management Arrangements, Systems and Controls) and COBS (Conduct of Business Sourcebook). This includes robust controls against unauthorised disclosures and compliance with the Market Abuse Regulation (MAR) for insider information.
- Health and Care Regulators: The Care Quality Commission (CQC) and HRA require adherence to Caldicott Principles and Section 251 approvals for non-consensual sharing. The Confidentiality Advisory Group (CAG) advises on approvals for research or public interest disclosures.
- Other Authorities: For charities, the Charity Commission mandates secure handling under governance standards. The DUAA introduces provisions for digital verification services, requiring compliance in emerging areas like Open Banking.

Organisations must demonstrate accountability through records of processing activities (ROPAs), staff training, and audits.

2.3 Common Law Duty of Confidence

The common law duty of confidence, derived from case law (e.g., Coco v A N Clark (Engineers) Ltd [1969]), imposes a legal obligation to protect information shared in circumstances implying confidentiality. This duty applies alongside statutory laws and persists even without a contract.

Key elements include:

- Information must have the necessary quality of confidence (not public knowledge).
- It must be imparted in circumstances importing an obligation of confidence (e.g., doctor-patient relationship).
- There must be unauthorised use or disclosure causing detriment.

Exceptions allow disclosure if:

- Consented to by the confider.
- Required by law (e.g., court order).
- Justified in the public interest (e.g., preventing serious harm, as per W v Egdell [1990]).

In health contexts, this duty aligns with NHS codes, requiring breaches to be escalated to a Caldicott Guardian or DPO. Breaches can lead to civil claims for damages or injunctions, reinforcing the need for secure handling.

2.4 International Considerations and Cross-Border Data Transfers

For operations involving international data, the UK GDPR Chapter V governs transfers to ensure equivalent protection levels.

Key considerations:

- Adequacy Decisions: Transfers to countries with ICO-recognised adequacy (e.g., EU/EEA under the 2021 decision, subject to 2025 review) require no further safeguards.
- Safeguards for Non-Adequate Countries: Use Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other mechanisms. The DUAA may introduce new tools for digital verification in cross-border contexts.
- Derogations: Limited use for specific cases, e.g., explicit consent or contractual necessity.
- Risk Assessments: Conduct Transfer Risk Assessments (TRAs) to evaluate recipient country risks, such as government access laws.

The Organisation must document transfers, ensure processors comply via contracts, and monitor global developments, including EU-UK adequacy renewal in 2025.

2.5 Consequences of Non-Compliance

Non-compliance with confidentiality obligations can result in severe repercussions, emphasising the need for robust adherence.

Potential consequences include:

- Financial Penalties: Under the UK GDPR, fines up to £17.5 million or 4% of global annual turnover (whichever is higher) for serious breaches. The ICO can also issue enforcement notices or bans on processing.

- Criminal Sanctions: DPA 2018 offences (e.g., Section 170) carry unlimited fines and up to two years' imprisonment.
- Civil Liabilities: Claims for compensation under the UK GDPR for material/non-material damage (e.g., distress), plus common law damages.
- Reputational Damage: Loss of trust, leading to client attrition or partnership terminations.
- Regulatory Actions: FCA sanctions (if applicable) include licence revocation; health regulators may impose conditions or closures.
- Other Impacts: Mandatory breach notifications, increased scrutiny, and costs from remediation or litigation.

The Organisation mitigates these through proactive compliance, as non-compliance under the DUAA could hinder innovation benefits like expanded research provisions.

3. Principles of Confidentiality

This chapter delineates the foundational principles that govern the handling of confidential information within the Organisation. These principles are derived from the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and sector-specific guidelines such as the Caldicott Principles, which remain unchanged at eight principles as of August 2025. The Data (Use and Access) Act 2025 (DUAA) introduces refinements to the application of these principles, particularly in areas like purpose limitation and lawful bases for processing, to facilitate innovation while maintaining high standards of protection. By adhering to these principles, the Organisation ensures ethical, lawful, and secure management of information, minimising risks and promoting trust. These principles apply universally across all data processing activities and are integrated into policies, training, and audits to foster a culture of responsibility.

3.1 Core Principles Underpinning Confidentiality

The core principles of confidentiality are enshrined in Article 5 of the UK GDPR and form the bedrock of data protection practices. These principles ensure that confidential information is processed in a manner that respects individuals' rights and freedoms. The DUAA 2025 does not alter these fundamental principles but enhances their practical application, such as by clarifying compatibility in purpose limitation.

The seven UK GDPR principles are:

- Lawfulness, Fairness, and Transparency: All processing must have a valid legal basis, be conducted fairly without misleading individuals, and involve clear communication about how data is used.
- Purpose Limitation: Data must be collected for specified, explicit, and legitimate purposes and not further processed in incompatible ways. Under the DUAA, re-use is permitted if it is compatible with the original purposes, supporting innovation in areas like research.
- Data Minimisation: Only data that is adequate, relevant, and limited to what is necessary for the purposes should be processed.
- Accuracy: Data must be accurate and kept up-to-date, with steps taken to rectify or erase inaccuracies without delay.
- Storage Limitation: Data should be retained only as long as necessary for the purposes, with secure disposal thereafter.
- Integrity and Confidentiality (Security): Appropriate technical and organisational measures must protect data against unauthorised or unlawful processing, accidental loss, destruction, or damage.
- Accountability: The Organisation must demonstrate compliance through measures like records, audits, and impact assessments.

In health and social care contexts, these are complemented by the eight Caldicott Principles, which provide additional guidance for handling patient-identifiable information:

- Justify the purpose(s) for using confidential information.
- Don't use patient-identifiable information unless necessary.

- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need-to-know basis.
- Everyone with access must be aware of their responsibilities.
- Comply with the law.
- The duty to share information for individual care is as essential as the duty to protect confidentiality.
- Inform patients and service users about how their confidential information is used.

These principles are mandatory where applicable and guide decision-making to balance confidentiality with necessary sharing.

3.2 Justification for Handling Confidential Information

Every instance of handling confidential information must be justified to ensure it aligns with legitimate organisational needs and legal requirements. Justification involves assessing the necessity, proportionality, and benefits of processing against potential risks to individuals' privacy.

Key considerations for justification include:

- Legitimate Purpose: Processing must serve a clear, defined objective, such as service delivery, research, or compliance. Under the Caldicott Principles, each use or transfer must be scrutinised and reviewed regularly.
- Necessity Test: Determine if the information is essential; anonymised or pseudonymised data should be used where possible to avoid identifiable details.
- Proportionality: Weigh the benefits (e.g., improved care or innovation) against risks (e.g., breach potential). The DUAA supports justification for recognised legitimate interests like crime prevention without a full balancing test, streamlining processes.
- Documentation: Maintain records of justifications, including DPIAs for high-risk activities, to demonstrate accountability.
- Review Mechanisms: Regularly evaluate ongoing uses, involving the DPO or Caldicott Guardian, to ensure continued relevance.

In charitable or health settings, justification extends to safeguarding vulnerable individuals, where sharing may be warranted in the public interest or for child protection, as per the Children Act.

3.3 Minimising Risks in Data Processing

Risk minimisation is integral to confidentiality, requiring proactive measures to reduce the likelihood and impact of breaches. This principle aligns with data minimisation and security under the UK GDPR, emphasising prevention over reaction.

Strategies for minimising risks include:

- Data Minimisation Practices: Collect only essential data and limit its scope. For example, avoid unnecessary special category data unless justified.

- Security Controls: Implement encryption, access restrictions (e.g., role-based access), and secure storage. Physical measures, such as locked cabinets for paper records, and digital tools like multi-factor authentication, are essential.
- Risk Assessments: Conduct regular DPIAs and Transfer Risk Assessments for cross-border activities to identify and mitigate vulnerabilities.
- Anonymisation and Pseudonymisation: Use these techniques to reduce identifiability, especially in research or sharing scenarios, as encouraged by Caldicott Principle 2.
- Incident Preparedness: Develop response plans for breaches, including containment and notification, to limit damage.
- Vendor Management: Ensure third parties adhere to equivalent standards via contracts and audits.

The DUAA's focus on innovation necessitates balancing risks with benefits, such as in expanded research processing, while upholding minimisation.

3.4 Consent and Lawful Bases for Processing

Processing confidential information requires a lawful basis under Article 6 of the UK GDPR, with additional conditions for special category data under Article 9. Consent is one basis but not always the most appropriate, especially where imbalances exist.

Lawful bases under Article 6 include:

- Consent: Freely given, specific, informed, and unambiguous; withdrawable at any time.
- Contract: Necessary for performing or entering a contract.
- Legal Obligation: Required by UK/EU law.
- Vital Interests: To protect someone's life.
- Public Task: For official functions or tasks in the public interest.
- Legitimate Interests: Pursued by the Organisation or third party, subject to a balancing test (simplified under DUAA for recognised interests like emergencies or national security).

For special category data, explicit consent or other conditions (e.g., employment, health provision) apply. The DUAA introduces "recognised legitimate interests" as a basis without full assessment for specified purposes.

Best practices:

- Prioritise non-consent bases where power imbalances exist (e.g., employee data).
- Document bases in ROPAs.
- For health data, use Section 251 approvals if consent is impracticable.
- Ensure consent is granular and recorded.

3.5 Transparency and Accountability

Transparency requires clear communication about data handling, while accountability demands demonstrable compliance.

Transparency measures:

- Privacy Notices: Provide accessible information on purposes, bases, recipients, and rights at collection points.
- Informing Individuals: Explain uses, especially for secondary purposes, aligning with Caldicott Principle 8.
- Updates: Notify changes via notices or direct communication.

Accountability involves:

- Records and Documentation: Maintain ROPAs, DPIAs, and consent logs.
- DPO Role: Appoint a DPO for oversight and ICO liaison.
- Audits and Reviews: Conduct internal audits to verify adherence.
- Training and Culture: Ensure staff understand obligations, with breaches escalated.

The DUAA enhances accountability in innovation contexts, requiring robust documentation for new processes, such as broad research consent.

4. Roles and Responsibilities

This chapter outlines the specific roles and responsibilities assigned to various individuals and teams within the Organisation to ensure effective implementation and oversight of confidentiality practices. Clear delineation of duties promotes accountability, facilitates compliance with legal and regulatory requirements, and embeds confidentiality into the Organisation's culture. These roles are informed by best practices from healthcare, charitable, and regulated sectors, ensuring a comprehensive governance framework. All parties must understand and fulfil their obligations, with breaches subject to disciplinary procedures. Responsibilities are scalable based on the Organisation's size and sector, with mandatory training provided to support role execution.

4.1 Board of Directors and Senior Management

The Board of Directors and Senior Management hold ultimate accountability for confidentiality governance, setting the strategic direction and ensuring alignment with organisational objectives and legal standards. They champion a culture of confidentiality, allocating resources and overseeing high-level risks.

Key responsibilities include:

- Approving and reviewing the Confidentiality Policy annually or following significant changes, such as legislative updates under the Data (Use and Access) Act 2025.
- Ensuring adequate resources, including budget and personnel, are allocated to information governance, training, and security measures.
- Overseeing risk management, including signing off on high-risk decisions related to data sharing or processing, and chairing relevant committees (e.g., Information Governance Steering Group).
- Monitoring compliance through regular reports on breaches, audits, and key performance indicators, taking corrective actions as needed.
- Promoting ethical practices by modelling confidentiality behaviours and integrating them into strategic planning.
- Appointing key roles such as the Senior Information Risk Owner (SIRO) or equivalent, who assumes accountability for information risks.

In health-related organisations, the Board ensures alignment with Caldicott Principles, appointing a Caldicott Guardian where required.

4.2 Data Protection Officer (DPO) and Caldicott Guardian (where applicable)

The Data Protection Officer (DPO) provides independent advice and oversight on data protection matters, reporting directly to the highest management level. In health or social care contexts, the Caldicott Guardian fulfils a similar role focused on patient confidentiality, often collaborating with the DPO.

Responsibilities of the DPO include:

- Advising on compliance with the UK GDPR, Data Protection Act 2018, and Data (Use and Access) Act 2025, including conducting Data Protection Impact Assessments (DPIAs).
- Monitoring internal audits, training effectiveness, and policy adherence, reporting findings to the Board.
- Acting as the primary contact for the Information Commissioner's Office (ICO) and handling data subject requests (e.g., access, erasure).
- Investigating breaches, advising on notifications, and recommending remedial actions.
- Promoting awareness through guidance, training sessions, and updates on regulatory changes.

For the Caldicott Guardian (mandatory in NHS-equivalent settings):

- Protecting patient confidentiality by reviewing and approving uses of identifiable health data.
- Enabling appropriate information sharing, such as under Section 251 approvals, while ensuring minimal identifiable data is used.
- Chairing or participating in governance groups to balance confidentiality with care delivery needs.
- Providing expert advice on ethical dilemmas, such as public interest disclosures.

Where roles overlap, a single individual may hold both positions if conflicts are managed.

4.3 Line Managers and Supervisors

Line Managers and Supervisors are responsible for day-to-day enforcement of confidentiality practices within their teams, ensuring operational compliance and supporting staff development.

Their duties encompass:

- Implementing the Confidentiality Policy at the team level, including risk assessments and secure handling procedures.
- Supervising staff to prevent breaches, such as monitoring access to confidential information and enforcing need-to-know principles.
- Conducting induction and ongoing training, ensuring team members complete mandatory sessions and understand their obligations.
- Reporting incidents promptly via the Organisation's incident portal and supporting investigations.
- Reviewing team processes for vulnerabilities, such as remote working setups, and implementing controls like access logs.
- Addressing concerns raised by staff, escalating complex issues to the DPO or Information Governance Team.

In supervisory roles, they must lead by example, fostering an environment where confidentiality is prioritised and breaches are not tolerated.

4.4 All Employees, Contractors, Volunteers, and Third Parties

All individuals associated with the Organisation, including employees, contractors, volunteers, and third parties, share a personal duty to uphold confidentiality. This is reinforced through contracts, non-disclosure agreements (NDAs), and mandatory training.

Common responsibilities include:

- Adhering to the Confidentiality Policy, including secure handling, storage, and disposal of information in all formats (e.g., paper, digital, verbal).
- Accessing confidential information only on a need-to-know basis and for authorised purposes.
- Reporting any suspected or actual breaches immediately to their line manager or via designated channels, without fear of reprisal.
- Participating in induction, annual training, and awareness sessions to stay informed on best practices and legal updates.
- Avoid careless disclosures, such as discussing sensitive matters in public or leaving devices unattended.
- Complying with specific clauses in employment contracts or agreements that outline confidentiality obligations, with breaches potentially leading to disciplinary action or contract termination.

Contractors and volunteers must sign NDAs, and third parties are bound by data processing agreements ensuring equivalent protections.

4.5 Information Governance Team

The Information Governance Team supports the Organisation by providing operational expertise, coordinating activities, and ensuring consistent application of confidentiality standards.

Key functions include:

- Developing and maintaining policies, procedures, and tools related to confidentiality, such as privacy notices and breach response plans.
- Conducting audits and assessments to evaluate compliance, identifying gaps and recommending improvements.
- Delivering training programmes, awareness campaigns, and guidance materials tailored to different roles.
- Managing incident responses in collaboration with the DPO, including root cause analysis and lessons learned.
- Liaising with external regulators and partners on confidentiality matters, such as data sharing agreements.
- Monitoring emerging risks and legislative changes, updating the Organisation accordingly.

The team acts as a central resource, offering advice on complex queries and promoting best practices across departments.

4.6 External Partners and Service Providers

External Partners and Service Providers, including suppliers, collaborators, and data processors, must align with the Organisation's confidentiality standards to prevent risks in shared environments.

Their responsibilities, enforced through contracts, include:

- Complying with the UK GDPR as data processors, implementing security measures and reporting sub-processors.
- Signing NDAs or data processing agreements that specify confidentiality obligations, breach notification timelines (e.g., within 24 hours), and audit rights.
- Ensuring their staff are trained and vetted, with access limited to necessary information.
- Providing assurances on data handling, such as encryption for transfers and secure disposal.
- Cooperating in audits, incident investigations, and compliance reviews conducted by the Organisation.
- Notifying the Organisation of any breaches affecting shared data and assisting in remediation.

The Organisation conducts due diligence before engagement and monitors performance through regular reviews to maintain chain-of-trust integrity.

5. Handling Confidential Information

This chapter provides detailed guidance on the practical aspects of managing confidential information throughout its lifecycle, from identification to disposal. It ensures that all handling practices comply with legal requirements, such as those under the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, and the Data (Use and Access) Act 2025, while minimising risks of unauthorised access or breaches. Drawing from best practices in healthcare, charitable, and regulated environments, these procedures emphasise security, necessity, and accountability. All individuals must follow these guidelines to protect sensitive data, with deviations treated as potential breaches subject to investigation. Handling must always align with the principles of data minimisation, purpose limitation, and integrity, incorporating tools like encryption and audits to maintain robust protection.

5.1 Identification and Classification of Confidential Information

Identifying and classifying confidential information is the first step in effective management, enabling appropriate safeguards based on sensitivity levels. Confidential information includes any data that, if disclosed, could cause harm to individuals, the Organisation, or third parties. This encompasses personal data, special category data, and business-sensitive information.

Key steps for identification include:

- Assessing whether the information relates to an identifiable individual (e.g., name, address, health records) or organisation (e.g., financial strategies, contracts).
- Determining if it falls under special protections, such as special category data (e.g., health, ethnic origin, biometric details) or commercially sensitive material.
- Evaluating potential harm from disclosure, including financial loss, reputational damage, or privacy invasion.

Classification should use a tiered system to guide handling:

Classification Level	Description	Examples	Handling Requirements
Public	Information is freely available without restrictions.	Marketing brochures, public reports.	No special controls; can be shared openly.
Internal	Data for internal use only, not sensitive.	General staff memos, non-confidential policies.	Limit to authorised personnel; basic access controls.
Confidential	Sensitive data that could cause moderate harm if disclosed.	Employee records, client contact details.	Encrypt, restrict access on a need-to-know basis; log access.

Restricted	Highly sensitive data with high risk of harm.	Special category data, trade secrets, legal documents.	Advanced encryption, multi-factor authentication, regular audits, and minimal sharing.

All information must be labelled accordingly upon creation or receipt, with reviews conducted periodically to reclassify if risks change. Unclassified data defaults to 'Confidential' until assessed.

5.2 Collection and Acquisition of Information

Collection and acquisition must be justified, minimal, and conducted lawfully to avoid unnecessary risks. Data should only be gathered for explicit purposes, with individuals informed via privacy notices at the point of collection.

Procedures for collection include:

- Justification and Minimisation: Collect only essential data, using anonymised formats where possible. Conduct a necessity assessment before acquisition, aligning with purpose limitation principles.
- Lawful Bases: Ensure a valid basis (e.g., consent, contract, legal obligation) is established and documented. For special category data, obtain explicit consent or rely on appropriate conditions.
- Consent Processes: Where consent is used, it must be informed, specific, and granular. Provide clear options for withdrawal and record consents in a verifiable manner.
- Sources and Methods: Acquire data from reliable sources, such as direct from individuals or authorised third parties. Use secure forms, encrypted channels, and avoid unsolicited collection.
- Quality Checks: Verify accuracy and relevance upon acquisition, rectifying errors promptly to maintain data integrity.

In health or charitable contexts, collection should prioritise vulnerability safeguards, such as obtaining proxy consent for those lacking capacity. All collection activities must be logged for accountability.

5.3 Secure Storage and Access Controls

Secure storage and access controls are critical to preventing unauthorised access, ensuring the integrity and confidentiality of information. Storage must incorporate physical, technical, and organisational measures tailored to the data's classification.

Key storage guidelines:

- Physical Storage: Store paper records in locked cabinets or secure rooms with restricted entry (e.g., keypads, swipe cards). In shared spaces, prevent oversight by unauthorised parties.
- Digital Storage: Use encrypted servers, cloud services with UK GDPR-compliant providers, and databases with access logging. Avoid storing sensitive data on removable media unless encrypted.

- Access Controls: Implement role-based access control (RBAC), where permissions are granted on a need-to-know basis. Review and revoke access regularly, primarily upon role changes or terminations.
- Technical Safeguards: Employ encryption (e.g., AES-256), firewalls, and intrusion detection systems. Use multi-factor authentication for all systems holding confidential data.
- Monitoring: Log all access attempts, with alerts for suspicious activity. Conduct regular vulnerability scans and penetration testing.

Storage locations must comply with retention schedules, with off-site backups encrypted and tested for recovery. In mixed environments, segregate confidential data to prevent cross-contamination.

5.4 Sharing, Disclosure, and Transfer of Information

Sharing, disclosure, and transfer must be authorised, secure, and limited to necessary instances, balancing confidentiality with operational needs. Unauthorised sharing constitutes a breach and may trigger legal obligations.

Protocols for sharing include:

- Authorisation: Obtain explicit consent or rely on a lawful basis (e.g., public interest). For health data, seek Caldicott Guardian approval or Section 251 exemptions if consent is impracticable.
- Secure Methods: Use encrypted email, secure portals, or file transfer protocols (e.g., SFTP). Avoid unencrypted channels or public platforms.
- Data Sharing Agreements: Formalise arrangements with recipients via contracts specifying purposes, security measures, and breach reporting.
- Disclosure Exceptions: Permit sharing without consent in cases like child protection, court orders, or public interest (e.g., preventing harm). Document rationale and escalate to the DPO.
- Transfers: For cross-border transfers, ensure adequacy or use safeguards like Standard Contractual Clauses. Conduct Transfer Risk Assessments to evaluate recipient protections.

All sharing must be logged, with minimal data transferred. Recipients are responsible for equivalent protections, with the Organisation retaining oversight.

5.5 Use in Remote or Mobile Working Environments

Remote or mobile working introduces additional risks, requiring enhanced controls to maintain confidentiality outside traditional office settings. All remote access must be approved and monitored.

Guidelines for remote use:

- Device Security: Use Organisation-issued devices with full-disk encryption, antivirus software, and remote wipe capabilities. Prohibit the use of personal devices for confidential information.
- Network Protections: Mandate VPN usage for all remote connections; avoid public Wi-Fi. Implement endpoint detection and response tools.
- Physical Safeguards: Ensure information is not visible or audible to unauthorised persons (e.g., family members). Lock screens when unattended and store devices securely.

- Data Handling: Limit downloads of confidential data; use secure cloud access instead. Prohibit printing unless necessary, with immediate secure storage or disposal.
- Incident Reporting: Report lost or stolen devices immediately. Conduct risk assessments for remote setups, including home office audits.
- Training: Provide specific training on remote risks, such as phishing and secure communication.

Remote workers must sign agreements acknowledging personal responsibility, with breaches potentially leading to access revocation.

5.6 Disposal and Destruction of Information

Disposal and destruction must ensure confidential information is irrecoverable, aligning with storage limitation principles and retention schedules. Retain data only as long as necessary, then dispose securely to prevent unauthorised recovery.

Destruction procedures:

- Retention Schedules: Develop schedules based on legal requirements (e.g., 6 years for financial records). Review annually to identify data for disposal.
- Physical Destruction: Shred paper documents using cross-cut shredders (DIN level P-4 or higher). Destroy CDs/DVDs via specialist equipment.
- Digital Destruction: Use secure deletion tools (e.g., overwriting with DoD 5220.22-M standards) for files. Wipe or degauss hard drives; physically destroy if necessary.
- Verification: Confirm destruction through certificates or logs, with witnesses for high-sensitivity data.
- Third-Party Disposal: Engage certified providers with contracts ensuring compliance; audit their processes.
- Archiving: For data requiring long-term retention, archive securely with access restrictions.

All disposal must be documented, with breaches (e.g., improper dumping) reported as incidents. Post-disposal reviews ensure no residual risks remain.

6. Specific Guidelines for High-Risk Scenarios

This chapter addresses high-risk scenarios where confidentiality risks are elevated due to the sensitivity of the information, potential for harm, or complex legal considerations. These guidelines build on the core principles and handling procedures outlined earlier, providing tailored controls to mitigate threats in contexts such as sensitive data processing, client interactions, and external engagements. As of August 2025, these align with enhanced provisions under the Data (Use and Access) Act 2025, which facilitates responsible sharing in high-risk areas like research while upholding stringent safeguards. All scenarios require documentation, escalation to the Data Protection Officer (DPO) or Caldicott Guardian where applicable, and post-event reviews to ensure compliance and continuous improvement. Breaches in these areas may attract heightened regulatory scrutiny, emphasising the need for vigilance and proportionality.

6.1 Dealing with Special Category Data (e.g., Health, Ethnic Origin)

Special category data, as defined under Article 9 of the UK GDPR, includes highly sensitive personal information such as health details, ethnic or racial origin, religious or philosophical beliefs, political opinions, trade union membership, genetic or biometric data, and data concerning sexual orientation or sex life. Processing this data requires explicit justification and additional conditions beyond standard lawful bases, with risks amplified due to the potential for discrimination or harm if mishandled.

Key guidelines for dealing with special category data include:

- Lawful Conditions for Processing: In addition to an Article 6 basis, satisfy an Article 9 condition, such as explicit consent, employment obligations, vital interests, or substantial public interest (e.g., equality monitoring). The Data (Use and Access) Act 2025 expands options for scientific research, allowing broad consent where appropriate.
- Enhanced Risk Assessments: Conduct mandatory Data Protection Impact Assessments (DPIAs) before processing, evaluate risks like stigmatisation, and implement mitigations such as pseudonymisation.
- Minimised Use: Limit collection to absolute necessities, using anonymised aggregates for analysis where feasible. In health contexts, adhere to the Caldicott Principles by justifying each use and accessing on a strict need-to-know basis.
- Security Measures: Apply advanced protections, including end-to-end encryption, segregated storage, and audit trails. Access must be logged and restricted to authorised personnel with specific training.
- Consent and Rights: Obtain explicit, granular consent when relying on it, ensuring it is informed and withdrawable. Inform individuals of processing via detailed privacy notices, and handle rights requests (e.g., erasure) with priority due to sensitivity.
- Sharing Restrictions: Prohibit sharing without explicit authorisation; for health data, seek Section 251 approvals if consent is impracticable. Document all decisions, escalating to the Caldicott Guardian for review.

Regular audits of special category data processing are required, with breaches reported to the ICO within 72 hours if rights are at risk.

6.2 Confidentiality in Client/Patient Interactions

Client or patient interactions often involve real-time handling of confidential information, heightening risks of accidental disclosure or misuse. Maintaining confidentiality builds trust, supports service delivery, and complies with ethical duties, particularly in health, charitable, or financial sectors.

Guidelines for these interactions include:

- Secure Communication: Use encrypted channels (e.g., secure portals, video calls with end-to-end encryption) for discussions. Avoid insecure methods like standard email unless risks are explained and consented to.
- Verification and Consent: Verify client identity before sharing information. Obtain consent for recording interactions or involving third parties, and document it.
- Need-to-Know Access: Limit disclosures to essential details; for example, in patient care, share only pertinent health data with involved professionals.
- Environmental Controls: Conduct interactions in private settings to prevent overhearing. In virtual scenarios, ensure backgrounds and screens are not visible to unauthorised viewers.
- Documentation: Record interactions accurately in secure systems, noting any disclosures and rationales. Inform clients of how their data is used, aligning with transparency principles.
- Vulnerable Individuals: For clients lacking capacity, seek proxy consent from legal representatives. In safeguarding cases, prioritise protection while minimising breaches.

Training must cover scenario-based examples, with breaches in interactions treated as serious incidents requiring immediate reporting.

6.3 Handling Requests for Information (e.g., Subject Access Requests)

Information requests, such as Subject Access Requests (SARs) under Article 15 of the UK GDPR, enable individuals to exercise their rights but pose risks if mishandled, such as inadvertent disclosure of third-party data. Timely, accurate responses are essential to compliance.

Procedures for handling requests include:

- Verification: Confirm the requester's identity using secure methods (e.g., two-factor checks) to prevent unauthorised access.
- Scope and Response: For SARs, provide copies of personal data, processing details, and rights information within one month (extendable to three for complex cases). Redact third-party data to avoid breaches.
- Exemptions: Apply limited exemptions where disclosure would harm others (e.g., child protection) or if manifestly unfounded, documenting reasons.
- Other Requests: Handle rectification (Article 16), erasure ('right to be forgotten', Article 17), or restriction (Article 18) promptly, notifying recipients of changes.
- Logging and Tracking: Use a central system to log requests, track deadlines, and record responses. Escalate complex cases to the DPO.
- Fees and Support: Responses are free unless excessive; provide accessible formats (e.g., large print) upon request.

Annual reviews of request handling ensure efficiency, with training focusing on balancing rights with confidentiality.

6.4 Whistleblowing and Public Interest Disclosures

Whistleblowing and public interest disclosures allow confidential information to be shared to expose wrongdoing or risks, but must be managed to avoid unnecessary breaches. These are protected under the Public Interest Disclosure Act 1998 and align with Caldicott Principle 7, emphasising the duty to share for care or safety.

Guidelines include:

- Protected Disclosures: Encourage reporting concerns (e.g., malpractice, harm risks) via internal channels without fear of retaliation. Disclosures to regulators or prescribed persons are protected if made in good faith.
- Public Interest Justification: Disclose without consent if necessary to prevent serious harm (e.g., crime, child abuse), weighing proportionality. Document the balancing test, consulting the DPO or legal advisors.
- Secure Channels: Use anonymous whistleblowing hotlines or encrypted platforms to protect the discloser's identity.
- Investigation: Handle reports confidentially, limiting access to investigators. Provide feedback to whistleblowers where possible without compromising others.
- Training and Policy: Integrate into training, with a dedicated Whistleblowing Policy cross-referenced. Monitor for patterns indicating systemic issues.
- Legal Protections: Ensure compliance with employment laws; unauthorised disclosures outside protected routes may breach confidentiality.

All disclosures must be recorded, with lessons applied to prevent future risks.

6.5 Managing Conflicts of Interest and Insider Information

Conflicts of interest and insider information pose risks of misuse or unfair advantage, particularly in financial or corporate contexts. Managing these maintains integrity and complies with regulations like the Market Abuse Regulation.

Strategies include:

- Identification: Declare potential conflicts (e.g., personal relationships, financial interests) via a register, reviewed annually.
- Insider Information Controls: Classify and restrict access to non-public information that could influence decisions (e.g., merger details). Use 'Chinese walls' to segregate teams.
- Mitigation Measures: Recuse individuals from decisions where conflicts exist; implement monitoring to detect misuse.
- Disclosure Policies: Require NDAs for those handling insider data; report suspicions of abuse immediately.

- Training: Provide scenario-based training on recognising and managing conflicts, with emphasis on ethical decision-making.
- Audits: Conduct regular reviews of declarations and accesses, escalating breaches to senior management.

In regulated settings, align with FCA requirements for robust controls against market abuse.

6.6 Confidentiality in Mergers, Acquisitions, or Third-Party Engagements

Mergers, acquisitions, or third-party engagements involve extensive data sharing, heightening breach risks. These must be governed by contracts and due diligence to protect confidentiality.

Guidelines encompass:

- Due Diligence: Assess third-party security practices pre-engagement, including audits and compliance checks.
- Contracts and NDAs: Mandate data processing agreements specifying protections, breach notifications, and return/destruction clauses.
- Controlled Sharing: Use secure data rooms with access logs; share minimal data in phases, redacting sensitive elements.
- Risk Assessments: Perform DPIAs for large-scale sharing, identifying integration risks post-merger.
- Post-Engagement: Ensure data is returned or destroyed; monitor for residual risks during transitions.
- Oversight: Assign a project lead (e.g., DPO) to oversee confidentiality, with escalation protocols for issues.

These processes safeguard assets and comply with competition laws, with breaches potentially derailing deals.

7. Training, Awareness, and Culture

This chapter outlines the Organisation's commitment to equipping all individuals with the knowledge and skills necessary to handle confidential information effectively. Training, awareness, and cultural initiatives are essential for embedding confidentiality principles into daily practices, reducing breach risks, and ensuring compliance with legal standards such as the UK General Data Protection Regulation (UK GDPR) and the Data (Use and Access) Act 2025. By fostering a proactive culture, the Organisation promotes vigilance, accountability, and ethical behaviour. These efforts are mandatory, tailored to roles, and regularly evaluated to address evolving threats and regulatory changes. Participation is tracked, with non-compliance treated as a disciplinary matter. The Information Governance Team coordinates these activities, drawing on best practices from healthcare, charitable, and regulated sectors to deliver engaging, practical content.

7.1 Mandatory Training Programmes

Mandatory training programmes form the cornerstone of the Organisation's confidentiality education, ensuring all personnel understand their obligations and how to apply them. Training is role-specific, delivered through a combination of e-learning modules, workshops, and assessments, and must be completed annually or more frequently for high-risk roles.

Key elements of the programmes include:

- Core Content: Coverage of legal frameworks (e.g., UK GDPR principles, common law duty of confidence), identification of confidential information, secure handling procedures, breach reporting, and high-risk scenarios like special category data.
- Delivery Methods: Interactive online modules with quizzes, in-person sessions for practical exercises (e.g., role-playing disclosures), and sector-specific modules (e.g., Caldicott Principles for health roles).
- Frequency and Duration: Annual refresher training (at least 2 hours) for all staff; additional sessions following policy updates or incidents. New risks, such as those introduced by the Data (Use and Access) Act 2025, are incorporated promptly.
- Tracking and Compliance: Use a learning management system to record completion, with automated reminders and escalations for non-compliance. Certificates are issued upon passing assessments (minimum 80% score).
- Tailoring: Customise for audiences—e.g., advanced modules for managers on oversight, basic overviews for volunteers.

Training materials are updated annually, with input from the Data Protection Officer (DPO) to reflect current best practices and lessons from audits.

7.2 Awareness-Raising Initiatives

Awareness-raising initiatives complement formal training by keeping confidentiality top-of-mind through ongoing, engaging activities. These initiatives aim to reinforce behaviours, highlight emerging risks, and encourage proactive reporting.

Initiatives include:

- Campaigns and Communications: Regular emails, newsletters, and intranet posts on topics like phishing risks, secure remote working, or breach examples. Annual awareness weeks feature posters, videos, and quizzes with incentives for participation.
- Scenario-Based Learning: Share anonymised case studies of real breaches or near-misses, discussing lessons learned in team meetings or webinars.
- Resources and Tools: Provide quick-reference guides (e.g., Do's and Don'ts checklists), infographics on principles, and access to an online confidentiality hub with FAQs and self-assessment tools.
- Events and Workshops: Host guest speakers from regulators (e.g., ICO) or organise interactive sessions on topics like data sharing ethics.
- Targeted Efforts: Focus on high-risk groups, such as remote workers with tips on device security, or client-facing staff with reminders on interaction protocols.

Feedback from participants is solicited to refine initiatives, ensuring they remain relevant and impactful.

7.3 Fostering a Culture of Confidentiality

Fostering a culture of confidentiality involves leadership commitment and organisational-wide efforts to make the protection of information a shared value. This culture reduces complacency, encourages reporting, and integrates confidentiality into decision-making.

Strategies for building this culture include:

- Leadership Role Modelling: Senior management demonstrates commitment by prioritising confidentiality in communications, participating in training, and recognising exemplary behaviours (e.g., through awards).
- Open Dialogue: Create forums for discussing concerns, such as anonymous suggestion boxes or regular governance meetings, to normalise conversations about risks.
- Integration into Operations: Embed confidentiality checks into processes like project planning or performance reviews, ensuring it's not viewed as an add-on.
- Positive Reinforcement: Celebrate successes, such as zero-breach quarters, and use motivational messaging to link confidentiality to the Organisation's mission (e.g., protecting vulnerable clients).
- Accountability Measures: Link compliance to appraisals, with clear consequences for breaches balanced by support for honest mistakes.
- Collaboration: Partner with external bodies for benchmarking, sharing best practices to evolve the culture dynamically.

Cultural assessments, via surveys or focus groups, are conducted biannually to measure progress and identify areas for improvement.

7.4 Induction and Ongoing Education for New Starters

Induction and ongoing education ensure new starters quickly align with confidentiality standards, while providing continuous learning for all to adapt to changes. This phased approach builds foundational knowledge and sustains competence.

Induction processes include:

- Initial Orientation: Within the first week, deliver a dedicated session covering policy overview, key principles, and personal responsibilities. Include signing a confidentiality statement or NDA.
- Role-Specific Modules: Tailor content to the starter's duties—e.g., access controls for IT roles, client interaction guidelines for front-line staff.
- Practical Components: Hands-on activities like system demos for secure storage or quizzes on breach scenarios.

Ongoing education encompasses:

- Refresher Courses: Mandatory annual updates, plus ad-hoc sessions on new legislation (e.g., Data (Use and Access) Act 2025 implications).
- Continuous Learning Paths: Offer optional advanced courses, webinars, or certifications (e.g., in data protection) for career development.
- Support Mechanisms: Provide mentors for new starters and access to resources like e-learning libraries for self-paced education.
- Monitoring Integration: Track progress through probation reviews, ensuring full compliance before granting unrestricted access.

This approach minimises early risks and supports long-term adherence.

7.5 Evaluation and Feedback on Training Effectiveness

Evaluation and feedback mechanisms are crucial to assess the impact of training and awareness efforts, identifying strengths and gaps for continuous improvement. This ensures programmes remain adequate, relevant, and value-adding.

Evaluation methods include:

- Metrics and KPIs: Track completion rates, assessment scores, breach incidents pre/post-training, and survey responses on knowledge retention.
- Feedback Collection: Use post-training questionnaires, focus groups, and anonymous surveys to gauge satisfaction, relevance, and suggested improvements.
- Impact Assessments: Conduct pre- and post-training tests to measure knowledge gains; analyse incident reports for correlations with training gaps.
- Audits and Reviews: Include training effectiveness in annual audits, with the Information Governance Team leading reviews and reporting to the Board.

- Adjustments: Based on feedback, update content (e.g., add modules on emerging threats like AI in data processing) and delivery formats to enhance engagement.
- Benchmarking: Compare against industry standards or peer organisations to ensure best-in-class practices.

Results are documented in annual reports, with actions tracked to closure, fostering a cycle of enhancement.

8. Incident Management and Breach Response

This chapter details the Organisation's structured approach to managing incidents and responding to breaches of confidentiality, ensuring swift containment, thorough investigation, and effective remediation. A breach is defined as any unauthorised access, disclosure, alteration, loss, or destruction of confidential information, whether accidental or intentional, that compromises its security or leads to potential harm. As of August 2025, these processes align with requirements under the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, and the Data (Use and Access) Act 2025, which emphasise timely reporting and enhanced accountability in data incidents. The framework promotes a no-blame culture for honest mistakes while holding individuals accountable for negligence or malice. All incidents must be managed through a centralised system, with the Information Governance Team and Data Protection Officer (DPO) overseeing responses. This proactive strategy minimises damage, complies with notification obligations, and drives continuous improvement through lessons learned. Regular drills and audits ensure readiness, with all personnel trained to recognise and report incidents promptly.

8.1 Identifying and Reporting Breaches

Identifying and reporting breaches early is crucial to limiting impact and fulfilling legal duties. All individuals must be vigilant for signs of breaches, such as unauthorised access logs, missing documents, suspicious emails, or accidental disclosures (e.g., sending data to the wrong recipient).

Key steps for identification and reporting include:

- Recognition Criteria: Classify incidents as breaches if they involve confidential information and pose risks to rights and freedoms (e.g., identity theft, discrimination). Examples include lost devices containing personal data, phishing successes, or verbal leaks in public spaces.
- Reporting Obligations: Report all suspected or confirmed breaches immediately—within 2 hours if possible—to the line manager, DPO, or via the Organisation's dedicated Incident Reporting Portal. Anonymous reporting options are available to encourage disclosures.
- Initial Assessment: Upon report receipt, the DPO or designated responder conducts a triage to determine severity (low: no harm; medium: potential harm; high: significant harm or regulatory reportable).
- Documentation at Reporting Stage: Use a standardised form (see Appendix D: Breach Reporting Form) to capture details like date, time, nature of the incident, involved data, and potential impacts.
- Training Integration: Annual training includes breach identification scenarios, with reminders that failure to report is a disciplinary offence.
- Monitoring Tools: Employ automated systems (e.g., access logs, intrusion detection) to flag anomalies, triggering automatic alerts for proactive identification.

Reports are confidential, with protections against retaliation to foster a reporting culture.

8.2 Incident Response Procedures

Incident response procedures provide a step-by-step framework to contain and manage breaches efficiently, minimising escalation. The Organisation maintains an Incident Response Plan, reviewed annually, with a cross-functional Response Team (including DPO, IT, legal, and communications leads) activated upon confirmation of a breach.

Core procedures include:

- Activation and Containment: Upon triage confirming a breach, activate the Response Team within 1 hour. Immediate actions: isolate affected systems (e.g., disconnect networks), revoke compromised access, and secure remaining data (e.g., change passwords, encrypt at-risk files).
- Response Phases:
    - Phase 1: Containment (0-4 hours): Stop the breach spread; for digital incidents, deploy backups if data is corrupted.
    - Phase 2: Eradication (4-24 hours): Remove root causes, such as malware or vulnerabilities, through scans and patches.
    - Phase 3: Recovery (24-72 hours): Restore operations securely, testing systems before reactivation.
- Communication Protocols: Internal updates to affected teams; external if necessary, coordinated by the communications lead to avoid misinformation.
- Resource Allocation: Pre-identify external experts (e.g., forensic investigators) for complex incidents, with escalation to senior management for high-severity cases.
- Drills and Testing: Conduct quarterly simulated breaches to test procedures, refining based on outcomes.
- Documentation Throughout: Maintain a real-time incident log detailing actions, decisions, and timelines for accountability.

These procedures ensure a coordinated, timely response, aligned with ICO guidelines for breach management.

8.3 Investigation and Root Cause Analysis

Thorough investigation and root cause analysis (RCA) follow containment to understand the breach's origins, assess impacts, and prevent recurrence. Led by the DPO or an independent investigator, this phase is impartial and evidence-based.

Investigation steps include:

- Evidence Gathering: Collect logs, witness statements, device forensics, and affected data samples without compromising further security. Use chain-of-custody protocols for physical evidence.
- Impact Assessment: Evaluate harm to individuals (e.g., financial loss, distress), the Organisation (e.g., reputational damage), and compliance (e.g., regulatory fines). Quantify where possible, such as the number of records exposed.

- Root Cause Analysis Techniques: Employ methods like the '5 Whys' or fishbone diagrams to identify underlying factors (e.g., human error, system flaws, policy gaps).
- Timeline Reconstruction: Map the incident chronologically to pinpoint failures, involving interviews with involved parties.
- Independent Review: For serious breaches, engage external experts to ensure objectivity; in health contexts, involve the Caldicott Guardian.
- Interim Reporting: Provide updates to the Board and Response Team, with a preliminary report within 48 hours.

Findings inform remediation, with all investigations documented confidentially and retained for at least 6 years.

8.4 Notification to Affected Parties and Regulators

Notifications to affected parties and regulators are mandatory for breaches risking rights and freedoms, promoting transparency and enabling mitigation. Timelines comply with UK GDPR requirements (72 hours to regulators; without undue delay to individuals).

Notification protocols include:

- Regulatory Notification: Report to the ICO within 72 hours for notifiable breaches, including details on nature, consequences, and measures taken. Use the ICO's online portal; for cross-border incidents, coordinate with lead authorities.
- Individual Notification: Inform affected persons if high risk (e.g., via email or letter) with clear details on the breach, potential harms, protective steps (e.g., credit monitoring), and contact points. Exemptions apply if the data is disproportionate or encrypted.
- Content Requirements: Notifications must be concise, transparent, and actionable, avoiding jargon. Include Organisation contact details and advice on rights.
- Third-Party Involvement: Notify data processors or partners if their data is affected; for joint controllers, agree on lead notifier.
- Public Communication: For widespread breaches, use press releases or website notices if individual notifications are impractical, and coordinate with the communications team.
- Documentation: Log all notifications, including rationale for non-notifications, for audit purposes.

Decisions on notification are made by the DPO, with legal review for complex cases.

8.5 Remediation, Lessons Learned, and Disciplinary Actions

Remediation addresses immediate harms, while lessons learned drive systemic improvements. Disciplinary actions ensure accountability, balanced with support for unintentional errors.

Remediation and learning processes include:

- Immediate Remediation: Offer support to affected individuals (e.g., counselling for distress); implement technical fixes (e.g., software patches) and policy updates.

- Lessons Learned Review: Post-incident, convene a debrief within 7 days to analyse findings, identify preventives (e.g., enhanced training), and update the Incident Response Plan.
- Action Planning: Develop a timed remediation plan with assigned owners, tracked via governance meetings until closure.
- Disciplinary Measures: Assess intent; for negligence, apply progressive discipline (e.g., warnings, retraining); for malice, escalate to dismissal or legal action under Data Protection Act 2018 Section 170.
- Compensation Considerations: Evaluate claims for damages, handling through insurance or settlements.
- Follow-Up Audits: Conduct targeted audits 3-6 months post-breach to verify fixes.

This phase emphasises learning over punishment, fostering resilience.

8.6 Reporting and Record-Keeping of Incidents

Comprehensive reporting and record-keeping enable oversight, trend analysis, and regulatory compliance. All incidents are documented centrally for traceability and improvement.

Reporting and record-keeping include:

- Internal Reporting: Submit quarterly summaries to the Board and Information Governance Steering Group, covering incident volumes, types, impacts, and trends.
- Record Maintenance: Use a secure database to store incident details, investigations, notifications, and outcomes, retained for at least 3 years (or longer if litigated).
- Key Metrics: Track indicators like breach frequency, response times, and remediation completion rates in dashboards for proactive management.
- External Reporting: Beyond ICO notifications, report to other regulators (e.g., FCA for financial breaches) or authorities (e.g., police for criminal acts).
- Annual Review: Include incident data in the Organisation's annual report, anonymised where necessary, to demonstrate accountability.
- Access Controls: Limit records to authorised personnel, with audit trails to prevent unauthorised views.

These practices support transparency and inform policy enhancements, ensuring the Organisation evolves in response to threats.

9. Monitoring, Auditing, and Continuous Improvement

This chapter describes the Organisation's systematic approach to monitoring, auditing, and enhancing confidentiality practices. These activities ensure ongoing compliance with legal frameworks, such as the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, and the Data (Use and Access) Act 2025, while identifying opportunities for improvement. By August 2025, these processes incorporate emerging requirements for innovation accountability, fostering a dynamic environment where risks are proactively managed. Monitoring and auditing are conducted regularly, with results informing policy updates and training. The Information Governance Team leads these efforts, supported by the Data Protection Officer (DPO) and senior management, to promote transparency, accountability, and a culture of excellence. All findings are documented, with corrective actions tracked to closure, ensuring the Organisation remains resilient against evolving threats and regulatory changes.

9.1 Internal Monitoring Mechanisms

Internal monitoring mechanisms provide real-time oversight of confidentiality practices, enabling early detection of issues and compliance verification. These mechanisms are embedded in daily operations, using a combination of automated tools and manual checks to track adherence across the Organisation.

Key monitoring mechanisms include:

- Access and Activity Logging: Implement automated logging for all systems handling confidential information, capturing details such as user access, modifications, and transfers. Review logs weekly for anomalies, with alerts for suspicious patterns (e.g., unusual download volumes).
- Compliance Checks: Conduct spot checks on processes like data sharing or remote access, using checklists aligned with policy requirements. Line managers perform monthly reviews within teams, escalating findings to the Information Governance Team.
- Technology Tools: Utilise data loss prevention (DLP) software to monitor outbound communications for sensitive data, and endpoint monitoring to track device usage. Integrate with vulnerability scanners to identify security gaps.
- Self-Assessment Surveys: Distribute quarterly surveys to staff assessing their understanding and application of confidentiality practices, with aggregated results analysed for trends.
- Incident Trend Analysis: Monitor reported incidents for patterns (e.g., recurring remote working breaches), using dashboards to visualise data and inform targeted interventions.
- Reporting Structure: Feed monitoring results into monthly governance reports, with thresholds for escalation (e.g., high-risk anomalies to the Board).

These mechanisms are reviewed annually to incorporate new technologies or regulatory guidance, ensuring proactive rather than reactive oversight.

9.2 Conducting Confidentiality Audits

Confidentiality audits are formal, independent evaluations to assess the effectiveness of controls, identify weaknesses, and verify compliance. Audits are scheduled regularly and may be triggered by incidents or changes, such as new legislation under the Data (Use and Access) Act 2025.

Audit processes include:

- Planning and Scope: Define audit scope based on risk (e.g., focusing on special category data or third-party engagements), with objectives aligned to policy principles. Engage internal auditors or external experts for objectivity.
- Methodology: Use a mix of techniques, including document reviews, interviews, system testing, and site visits. Sample high-risk activities, such as data transfers or client interactions, for in-depth examination.
- Execution Phases:
    - Preparation: Gather policies, logs, and records; notify auditees.
    - Fieldwork: Test controls (e.g., attempt unauthorised access simulations) and evaluate adherence.
    - Reporting: Produce a detailed report with findings, risks, and recommendations, rated by severity (e.g., critical, high, medium, low).
- Frequency: Annual comprehensive audits, plus bi-annual thematic audits (e.g., on remote working). Ad-hoc audits follow breaches or policy updates.
- Follow-Up: Track implementation of recommendations via action plans, with re-audits within 6 months for critical issues.
- Documentation: Maintain audit trails and reports securely, available for regulatory inspections.

Audits promote accountability, with results shared organisation-wide to reinforce best practices.

9.3 Key Performance Indicators (KPIs) and Metrics

Key Performance Indicators (KPIs) and metrics quantify the effectiveness of confidentiality practices, enabling data-driven improvements. These are monitored through dashboards and reported quarterly to senior management.

Selected KPIs and metrics include:

- Breach-Related Metrics: Number of breaches per quarter, categorised by type (e.g., accidental disclosure, cyber-attack); average response time (target: under 4 hours for containment); percentage of breaches notified within 72 hours.
- Training and Awareness Metrics: Completion rates (target: 100%); average assessment scores (target: 90%); participation in awareness initiatives (e.g., survey response rates).
- Compliance Metrics: Percentage of Data Protection Impact Assessments (DPIAs) completed for high-risk activities (target: 100%); audit finding closure rate (target: 95% within timelines).
- Access and Security Metrics: Number of unauthorised access attempts detected; percentage of data encrypted (target: 100% for confidential information); system uptime and vulnerability patch compliance (target: 99%).

- Request Handling Metrics: Average response time for Subject Access Requests (target: under 1 month); percentage of requests upheld (tracked for trends).
- Cultural Metrics: Staff survey scores on confidentiality awareness (target: above 85%); whistleblowing reports volume (indicating reporting culture).

Metrics are benchmarked against industry standards, with thresholds triggering reviews (e.g., rising breaches prompt targeted training). Annual targets are set and reviewed to align with organisational goals.

9.4 Policy Review and Update Process

The policy review and update process ensures the Confidentiality Policy remains current, effective, and responsive to changes in legislation, technology, or risks. Reviews are systematic, involving stakeholder input to maintain relevance.

Process steps include:

- Scheduled Reviews: Conduct annual full reviews, plus interim checks following significant events (e.g., Data (Use and Access) Act 2025 implementations or major breaches).
- Trigger Events: Initiate updates for new laws, audit findings, incident lessons, or organisational changes (e.g., new data processing activities).
- Review Methodology: Form a review team (including DPO, Information Governance Team, and representatives from key departments) to assess content against current requirements. Gather input via consultations or surveys.
- Update Procedures: Draft revisions, incorporating feedback; test changes (e.g., pilot new procedures). Obtain approvals from senior management and the Board.
- Version Control: Use a tracker (see Appendix F) to document changes, with previous versions archived. Communicate updates via training and notifications.
- Impact Assessment: Evaluate updates for equality and data protection impacts, ensuring no unintended risks.

This process guarantees the policy evolves, with all updates disseminated within 30 days of approval.

9.5 Feedback Loops and Stakeholder Engagement

Feedback loops and stakeholder engagement facilitate ongoing dialogue, capturing insights from internal and external parties to refine confidentiality practices. This inclusive approach enhances buy-in and identifies blind spots.

Engagement strategies include:

- Internal Feedback Mechanisms: Use anonymous surveys, suggestion portals, and focus groups post-training or audits to gather staff views on policy effectiveness and challenges.
- Stakeholder Consultations: Engage clients, patients, or partners through privacy notices feedback sections or advisory panels, particularly for high-risk areas like data sharing.

- External Input: Collaborate with regulators (e.g., ICO consultations), industry forums, or peers for benchmarking and best practice sharing.
- Feedback Integration: Analyse input quarterly, prioritising actions (e.g., policy tweaks from common queries) and tracking via action logs. Report back to contributors on how feedback was used.
- Engagement Activities: Host town halls or webinars on confidentiality topics, encouraging questions and discussions.
- Measurement: Track engagement metrics, such as response rates and action implementation percentages, to assess effectiveness.

These loops ensure the Organisation remains adaptive, with stakeholder views integral to continuous improvement.

10. Related Policies and Supporting Documents

This chapter outlines the interconnections between this Confidentiality Policy and other organisational documents, ensuring a cohesive governance framework. It also addresses the policy's impact on equality and references external resources that inform its development and application. As of August 2025, these linkages reflect the Organisation's integrated approach to information management, aligning with evolving regulations such as the Data (Use and Access) Act 2025. Related policies and documents provide supplementary guidance, procedures, and tools to support implementation, avoiding duplication while reinforcing confidentiality standards. All referenced materials are accessible via the Organisation's intranet or governance repository, with cross-references reviewed during policy updates to maintain consistency. This holistic structure promotes comprehensive compliance, ethical practices, and effective risk management across the Organisation.

10.1 Cross-References to Other Organisational Policies

The Confidentiality Policy does not operate in isolation but intersects with several other organisational policies that collectively form the information governance ecosystem. These cross-references ensure alignment, with each policy addressing specific aspects while supporting confidentiality objectives. Where conflicts arise, the most stringent requirements prevail, and the Data Protection Officer (DPO) provides resolution.

Key cross-referenced policies include:

- Data Protection Policy: Outlines detailed procedures for personal data processing under the UK GDPR and Data Protection Act 2018, including lawful bases, rights management, and impact assessments. It complements this policy by providing operational guidance on consent and data minimisation.
- Information Security Policy: Focuses on technical and physical safeguards, such as encryption standards, access controls, and cyber threat responses. It directly supports secure storage, remote working, and breach containment sections of this policy.
- Information Sharing Policy: Guides lawful data exchanges with third parties, including agreements and risk assessments. It expands on sharing protocols here, ensuring consistency in high-risk scenarios like mergers or public interest disclosures.
- Retention, Destruction, and Disposal Policy: Specifies schedules for data lifecycle management, aligning with storage limitations and disposal guidelines in this policy to prevent unnecessary retention risks.
- Whistleblowing Policy: Details protected disclosure processes, intersecting with public interest exceptions and reporting mechanisms to encourage ethical reporting without breaching confidentiality unduly.
- Recruitment and Selection Policy: Incorporates confidentiality clauses in contracts and NDAs for new starters, linking to induction training and third-party obligations.
- Disciplinary Policy and Procedure: Defines consequences for breaches, providing the framework for actions outlined in incident management sections.
- Equality and Diversity Policy: Ensures non-discriminatory practices in data handling, with cross-links to the equality impact assessment in this chapter.

These policies are hyperlinked in digital versions for easy navigation, with annual joint reviews to synchronise updates and avoid gaps.

10.2 Equality Impact Assessment

An Equality Impact Assessment (EIA) has been conducted to evaluate this policy's potential effects on protected characteristics under the Equality Act 2010, including age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation. The assessment ensures the policy promotes equality, eliminates discrimination, and fosters good relations, while identifying any indirect impacts on diverse groups. As part of its development, the EIA considered accessibility, vulnerability in data handling, and inclusive training. No significant adverse impacts were identified, but mitigations were implemented to enhance positive outcomes.

Summary of the EIA findings and actions:

Protected Characteristic	Potential Impact	Mitigation Measures	Responsible Party	Timeline
Age	Older individuals may face digital access barriers in remote training or notifications.	Provide alternative formats (e.g., printed materials, in-person sessions) and simplified digital tools.	Information Governance Team	Ongoing, reviewed annually
Disability	Policy procedures may not accommodate needs like screen readers for audits or large print for notices.	Ensure all documents are accessible (e.g., WCAG-compliant PDFs); offer reasonable adjustments in training.	DPO and HR	Immediate implementation
Gender Reassignment	Sensitive data handling could risk outing or discrimination if breached.	Strengthen controls for special category data; include diversity training in confidentiality modules.	Training Lead	Within 6 months of the policy update
Marriage and Civil Partnership	Minimal direct impact; potential in family-related data sharing.	Emphasise need-to-know access in family or dependency scenarios.	Line Managers	As part of the induction
Pregnancy and Maternity	Health data risks in maternity contexts require extra care.	Align with Caldicott Principles for health data; prioritise consent in related interactions.	Caldicott Guardian (if applicable)	Ongoing

Race	Ethnic origin data as a special category could lead to bias if mishandled.	Conduct bias checks in audits; promote cultural awareness in awareness initiatives.	Equality Officer	Bi-annual reviews
Religion or Belief	Religious data sensitivity demands minimal processing.	Limit collection and ensure anonymisation where possible.	DPO	Policy review cycle
Sex	Gender-specific data risks in equality monitoring.	Use aggregated, anonymised data for reporting; secure storage protocols.	Information Governance Team	Continuous
Sexual Orientation	High sensitivity; breaches could cause distress.	Explicit consent for processing; enhanced encryption for records.	DPO	Immediate for high-risk data

The full EIA report is appended or available upon request, with ongoing monitoring to address emerging issues. Updates to the policy incorporate EIA revisions, ensuring equality remains integral.

10.3 References to External Guidance and Best Practices

This policy draws on a range of external guidance and best practices to ensure alignment with industry standards and regulatory expectations. These references provide foundational principles, practical tools, and benchmarks for effective confidentiality management. The Organisation encourages personnel to consult these resources for deeper insights, with key documents linked in the governance repository.

Key external references include:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018: Core legal texts governing data processing, principles, and rights, as amended by the Data (Use and Access) Act 2025 for innovation-focused reforms.
- Information Commissioner's Office (ICO) Guidance: Comprehensive resources on breach reporting, DPIAs, and accountability, including codes of practice for data sharing and security.
- Caldicott Principles (2021 Update): Eight principles for handling patient-identifiable information in health and social care, emphasising justification, minimisation, and the duty to share.
- NHS Confidentiality Code of Practice (2003): Ethical guidelines for NHS staff on protecting patient data, with supplements on care record guarantees and information governance.
- Equality Act 2010 and Public Sector Equality Duty: Frameworks for assessing impacts on protected characteristics, informing the EIA process.
- ISO 27001: Information Security Management: International standard for security controls, referenced in auditing and risk management practices.
- Health Research Authority (HRA) Guidance: Advice on Section 251 approvals for non-consensual data use in research, applicable to health-related activities.

- Charity Commission Governance Standards: Best practices for charities on data handling and trustee responsibilities, ensuring ethical compliance in the voluntary sector.
- Financial Conduct Authority (FCA) Handbook (SYSC and COBS): Rules on systems, controls, and client data protection for regulated firms, including insider information management.

Additional best practice sources include reports from the National Data Guardian and sector-specific toolkits from bodies like Age UK or NHS England. These are reviewed annually for updates, with policy amendments as needed to incorporate new insights.

11. Appendices

The appendices provide supplementary resources to support the implementation and understanding of this Confidentiality Policy. They include practical tools, summaries, templates, and references that staff, managers, and stakeholders can use for quick reference and application. These materials are designed to enhance compliance, facilitate training, and ensure consistent practices across the Organisation. As of August 2025, the appendices incorporate updates from the Data (Use and Access) Act 2025 and other relevant developments. They should be reviewed alongside the main policy and updated as needed during policy reviews. Digital versions may include hyperlinks to external resources or editable templates for ease of use.

11.1 Appendix A: Confidentiality Do's and Don'ts

This appendix offers a concise guide to best practices and common pitfalls in handling confidential information. It serves as a quick reference for all personnel and is incorporated into training materials and awareness campaigns.

Do's:

- Safeguard the confidentiality of all person-identifiable or confidential information you come into contact with; this is a statutory obligation for everyone associated with the Organisation.
- Clear your desk at the end of each day, securing all non-digital records containing confidential information in recognised filing and storage places that are locked at times when offices are closed.
- Lock your computer sessions when not at your desk.
- Challenge any person in your area who does not have an identity card or is not a known member of staff.
- Ensure that technology such as laptops and USB sticks is locked with a password or PIN and encrypted, particularly when taken outside the Organisation's premises.
- Change passwords regularly and do not share them; use strong passwords with a mix of letters, numbers, and symbols.
- Ensure that you check the name of the recipient several times before sending an e-mail or post to make sure it is the correct address. If sending a sensitive or confidential e-mail, ask a colleague to check before you send it.
- Encrypt and password-protect attachments containing person-identifiable or confidential information.
- Where possible, avoid printing confidential information; if you have to print, collect the printed matter immediately, preferably in person.
- Follow guidance and procedures at all times.
- Discuss any concerns or queries about confidentiality with your Line Manager or the Corporate Information Governance Team.
- Ensure that person-identifiable or confidential information is kept physically secure when in transit by using locked boxes or zipped folders, and do not leave it unattended at any time (e.g., ensure it is locked in the boot of a car overnight if necessary).

- When sending confidential information by post/parcel, use recorded/signed for/special delivery services.
- Ensure that any confidential information sent by e-mail is sent securely.
- Seek advice if you need to share patient/person-identifiable information without the identifiable person's consent, and record the decision and any action taken.
- Report any actual or suspected breaches of confidentiality.
- Participate in induction, training, and awareness-raising sessions on confidentiality issues.

Don’ts:

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to whom it relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless necessary; anonymise the information where possible.
- Don't collect, hold, or process more information than you need, and do not keep it for longer than necessary.
- Don't divulge personal information or send confidential messages by e-mail unless encrypted or to a secure NHS e-mail address.
- Don't gossip about patients/persons or disclose person-identifiable or confidential information to an unauthorised person.
- Don't make personal or insensitive comments about a patient/person's condition or circumstance on social networking sites such as Facebook or X (formerly Twitter).
- Don't leave person-identifiable or confidential information lying around unattended, including telephone messages containing such information.
- Don't leave a computer terminal logged on to a system where person-identifiable or confidential information may be accessed unattended.
- Don't leave a portable computer containing person-identifiable or confidential information unattended or in view when in transit, and do not allow your computer screen to be viewed by unauthorised persons.
- Don't forward person-identifiable or confidential information via e-mail to your home computer.
- Don't leave confidential information in your home office unattended or in a place where other members of your family, friends, or visitors can view it.

11.2 Appendix B: Summary of Key Legislation and Codes of Practice

This appendix summarises the primary legal and guidance frameworks relevant to confidentiality. It is not exhaustive but highlights obligations applicable to the Organisation as of August 2025. Personnel should consult full texts or the DPO for detailed advice.

Legislation/Code	Key Provisions	Relevance to Confidentiality
UK General Data Protection Regulation (UK GDPR)	Principles for lawful processing (e.g., lawfulness, purpose limitation, security); data subject rights; breach notification within 72 hours.	Requires secure handling of personal data; mandates accountability through records and assessments.
Data Protection Act 2018 (DPA 2018)	UK-specific rules on processing, including criminal offences for unlawful disclosure (Section 170); exemptions for law enforcement.	Criminalises misuse of personal data; complements UK GDPR with national security provisions.
Data (Use and Access) Act 2025 (DUAA)	Reforms to UK GDPR/DPA for innovation, including broad consent for research and recognised legitimate interests.	Facilitates responsible sharing while upholding safeguards; enhances accountability in digital verification.
Human Rights Act 1998	Article 8: Right to respect for private and family life; disclosures must be proportionate.	Protects against unjustified intrusions; balances with public interest needs.
Privacy and Electronic Communications Regulations 2003 (PECR)	Rules on electronic marketing, cookies, and communications security.	Ensures confidential electronic transmissions; amended by DUAA for modern digital practices.

Common Law Duty of Confidence	Obligation to protect information shared in confidence; exceptions for consent, law, or public interest.	Enforceable through courts; applies to all confidential data beyond personal information.
Caldicott Principles (2021 Update)	Eight principles for health/social care data: justify use, minimise identifiability, need-to-know access, etc.	Guides ethical handling in patient contexts; emphasises duty to share for care.
NHS Confidentiality Code of Practice (2003)	Ethical guidelines for protecting patient data include care record guarantees.	Promotes patient choice and secure practices; relevant for health-related operations.
Equality Act 2010	Protects against discrimination; requires impact assessments.	Ensures confidentiality practices do not disadvantage protected groups.
Public Interest Disclosure Act 1998	Protects whistleblowers; allows disclosures in good faith.	Enables reporting of concerns without breaching confidentiality unduly.

For full details, refer to official sources like the ICO website or government publications.

11.3 Appendix C: Template for Confidentiality Agreement/Non-Disclosure Agreement (NDA)

This template provides a standard form for confidentiality agreements or NDAs, to be customised and signed by employees, contractors, volunteers, or third parties. It ensures explicit commitment to policy obligations.

Confidentiality Agreement/Non-Disclosure Agreement

Parties:

[The Organisation] (the "Disclosing Party") and [Name of Individual/Entity] (the "Receiving Party").

Date: [Insert Date]

Purpose: This Agreement protects confidential information disclosed during [e.g., employment, contract, partnership].

Definition of Confidential Information: Includes personal data, special category data, business secrets, and any information marked as confidential or reasonably considered so.

Obligations of the Receiving Party:

- Use information solely for authorised purposes.
- Not disclose without prior written consent, except as required by law.
- Implement security measures (e.g., encryption, access controls).
- Report breaches immediately.
- Return or destroy information upon request or termination.

Exceptions: Does not apply to information that is public, independently developed, or legally required to disclose (with notice to Disclosing Party).

Duration: Obligations survive [e.g., 5 years] post-termination.

Consequences of Breach: Disciplinary action, termination, legal remedies, including damages.

Governing Law: Laws of England and Wales.

Signatures:

Disclosing Party: _____ Date: _____

Receiving Party: _____ Date: _____

Consult legal advisors before use; attach to contracts as needed.

11.4 Appendix D: Breach Reporting Form

This form standardises incident reporting, ensuring comprehensive details for investigation. Submit electronically via the Incident Portal or to the DPO.

Breach Reporting Form

Reporter Details:

Name: _____ Role: _____ Contact: _____

Date/Time of Report: _____ Anonymous? [Yes/No]

Incident Details:

Date/Time Discovered: _____ Location: _____

Description: [Detail what happened, e.g., unauthorised access, lost device]

Type of Information Involved: [e.g., personal data, special category]

Number of Records/Affected Individuals: _____

Potential Causes: [e.g., human error, cyber-attack]

Immediate Actions Taken: [e.g., contained access, notified manager]

Impact Assessment:

Potential Harm: [e.g., financial loss, distress]

Affected Parties: [e.g., clients, staff]

Regulatory Reportable? [Yes/No – Explain]

Additional Information: [Attach evidence if available]

Signature: _____ Date: _____

The DPO will acknowledge receipt within 24 hours and initiate response procedures.

11.5 Appendix E: Glossary of Terms

This glossary defines key terms used in the policy for clarity and consistent application.

- Breach of Confidentiality: Unauthorised access, use, disclosure, alteration, or destruction of confidential information, leading to potential harm or non-compliance.
- Confidential Information: Data not publicly available whose disclosure could cause harm, including personal data and business secrets.
- Data Controller: The Organisation determining purposes and means of personal data processing.
- Data Processor: Third-party processing data on behalf of the controller, bound by agreements.
- Data Protection Impact Assessment (DPIA): Evaluation of risks in high-risk processing activities.
- Data Protection Officer (DPO): Independent advisor on data protection compliance.
- Personal Data: Information relating to an identified or identifiable living individual.
- Special Category Data: Sensitive personal data (e.g., health, ethnic origin) requiring extra protections.
- Subject Access Request (SAR): Individual's request for their personal data held by the Organisation.
- UK GDPR: Retained EU GDPR law in the UK, governing data protection principles and rights.

Additional terms are defined in the main policy or external legislation.