Definitions are written in plain English and aligned, where possible, to internationally recognised standards. Provenance is shown in square brackets after each definition.

**Access:** Controlled availability of records to authorised users, balancing business need with privacy and confidentiality. [ISO 15489-1:2016 (concepts/principles)]

**Access Controls:** Mechanisms that restrict or allow users to view, edit, or otherwise use information, typically based on role, responsibility, and business need. [ISO/IEC 27001:2022 (ISMS overview)]

**Accountability:** The requirement to be able to explain and justify decisions and actions relating to records and information, including who is responsible for what. [ISO 15489-1:2016 (policies/responsibilities)]

**Activity (BCS):** Second level in a business classification scheme describing a set of actions that make up a business function. [ISO 15489-1:2016 (classification/controls)]

**Archival Transfer:** Moving records of enduring value to an authorised archive repository for long-term preservation (distinct from 'cold storage' within a live business system). [ISO 14721:2025 (OAIS archive responsibilities)]

**Archivist:** A specialist responsible for preserving, organising and providing access to records of long-term value.

**Asset Register (Information Asset Register, IAR):** A managed inventory describing an organisation's information assets (what they are, who owns them, where they are held, sensitivity, retention and key risks). [ISO 31000:2018 (risk context)]

**Audit Trail:** A documented history of actions on a record (creation, access, modification, movement and disposal) supporting accountability and evidence. [ISO 15489-1:2016 (controls/monitoring)]

**Authenticity:** A record is what it purports to be and its origin and context can be proven. [ISO 15489-1:2016 (characteristics)]

**Availability:** Information and systems are accessible and usable on demand by authorised users. [ISO/IEC 27001:2022 (CIA triad)]

**Backup (Offline):** A copy of data kept separately from live systems to enable recovery after loss, corruption or attack; offline backups reduce exposure to some threats. [ISO/IEC 27001:2022 (availability)]

**Bit Rot (Data Corruption):** Unintended deterioration or corruption of digital data over time, detectable through fixity checking. [ISO 14721:2025 (long-term preservation)]

**Business Classification Scheme (BCS):** A hierarchical structure that organises records by business function and activity (what the organisation does), supporting consistent filing and retention. [ISO 15489-1:2016 (records controls)]

**Caldicott Guardian:** A senior role in health and care settings responsible for protecting confidential patient/service-user information and enabling lawful, appropriate sharing.

**Capstone Approach (Email):** Managing email retention at account level (e.g., by role/seniority) rather than assessing each message by content.

**Certificate of Destruction:** Evidence provided by a disposal supplier confirming secure destruction has been completed in line with requirements.

**Checksum:** A calculated value used to detect whether a digital file has changed or become corrupted. [ISO 14721:2025 (integrity/fixity)]

**CIA Triad:** A core information security model focusing on Confidentiality, Integrity and Availability. [ISO/IEC 27001:2022 (CIA triad)]

**Classification:** Organising records using a consistent scheme (e.g., business classification) so they can be found, managed and disposed of consistently. [ISO 15489-1:2016 (records controls)]

**Cloud Governance:** Rules and responsibilities for how information is structured, stored, accessed and maintained within cloud platforms.

**Cold Storage:** Low-cost, less-accessible storage for inactive data; not equivalent to archival preservation unless preservation controls are in place.

**Compliance:** Meeting relevant legal, regulatory, contractual and policy requirements for managing records and information. [ISO 15489-1:2016 (governance/monitoring)]

**Confidentiality:** Ensuring information is not made available or disclosed to unauthorised individuals, entities or processes. [ISO/IEC 27001:2022 (CIA triad)]

**Covert Hold:** A legal hold applied without notifying all affected staff, typically to preserve evidence during sensitive investigations.

**Creator:** The person, team or system responsible for making a record; in many contexts this can be an individual or a corporate body.

**Data Controller:** The organisation (or person) that determines the purposes and means of processing personal data.

**Data Protection Officer (DPO):** A role responsible for advising on and monitoring compliance with data protection law, and acting as a point of contact with regulators and individuals.

**Data Rights (Information Rights):** Legal entitlements enabling individuals to access, correct, erase or otherwise control personal data about themselves, and (for public bodies) to request recorded information.

**Degaussing:** Erasing data on magnetic media by applying a strong magnetic field.

**Digital Continuity:** Ensuring digital information remains readable, accessible and usable for as long as it is required, despite changes in technology and formats.

**Digital Preservation:** Managed activities that ensure digital records remain authentic, accessible and usable over time despite technological change. [ISO 14721:2025 (OAIS long-term preservation)]

**Digital Records:** Records created, managed and stored in electronic form across systems and platforms. [ISO 15489-1:2016 (applies regardless of form)]

**Digital Sustainability:** Managing digital information to reduce unnecessary duplication and storage, supporting efficient working and lower environmental impact.

**Disaster Recovery:** Plans and capabilities to restore systems and access to records after disruption. [ISO/IEC 27001:2022 (availability/risk management)]

**Disposal:** Applying an authorised end-of-life outcome to a record (e.g., secure destruction, transfer, or permanent preservation) in line with retention rules.

**Disposal Outcome:** The defined fate for a record at end of retention (e.g., destruction, archival transfer, transfer of ownership, migration then deletion).

**Disposition:** The authorised end-of-life action for records (e.g., destroy, transfer, archive/preserve) following a retention trigger. [ISO 15489-1:2016 (controls)]

**Documented Information:** Information required to be controlled and maintained by a management system (including records) to support consistent operation and evidence. [ISO/IEC 27001:2022 (documented information concept); ISO 30301:2019 (MSR requirements)]

**Email as a Record:** An email that provides evidence of a decision, approval, action, agreement or obligation and must be managed as a record.

**Email Management:** Identifying emails that are records and saving them into appropriate business systems, rather than relying on personal inboxes as storage.

**Environmental Controls:** Managing temperature, humidity, light, dust and pests to reduce deterioration of physical records; stability is often more important than perfection.

**Evidence:** Recorded information that can be relied upon to demonstrate decisions, actions, compliance and what happened. [ISO 15489-1:2016 (records as evidence)]

**Fixity:** A method of confirming digital content has not changed unexpectedly, commonly using checksums. [ISO 14721:2025]

**FOI (Freedom of Information):** A right for the public to request recorded information held by public authorities, subject to lawful exemptions.

**FOISA:** The Scottish Freedom of Information regime for Scottish public authorities.

**Function (BCS):** Top level in a business classification scheme describing what the organisation does.

**Governance Framework:** The set of structures, roles, policies and processes used to direct and control how information is managed across the organisation. [ISO 30301:2019 (MSR governance)]

**Immutability:** A property supporting evidential value by ensuring records remain unchanged over time; any authorised change is controlled and auditable.

**Incident Management:** An organised approach to identify, report, contain, investigate and learn from information security incidents. [ISO/IEC 27001:2022 (risk management approach)]

**Incineration:** Controlled burning of records as a secure destruction method for highly sensitive information.

**Information Architecture:** Designing information structures, classifications and relationships so information is findable, understandable and governed across systems.

**Information Asset:** A collection or type of information held for a common purpose, with recognised value, risk and lifecycle, which may exist across multiple systems or formats.

**Information Asset Owner (IAO):** A senior role accountable for managing a specific information asset, including risk, access, and compliance within their remit.

**Information Governance:** The framework for managing information responsibly and lawfully so it supports organisational objectives, accountability and rights. [ISO 15489-1:2016 (policies/responsibilities)]

**Information Risk Register:** A log of information risks, their likelihood and impact, existing controls, residual risk, actions, owners and review dates. [ISO 31000:2018 (risk process)]

**Information Security Incident:** An event that compromises, or could compromise, the confidentiality, integrity or availability of information.

**Information Security Management System (ISMS):** A management system for establishing, implementing, maintaining and continually improving information security. [ISO/IEC 27001:2022 (ISMS overview)]

**Information Sustainability (Technological Sustainability):** Monitoring technology dependencies (formats, hardware, software) and planning migrations to reduce long-term access risks.

**Integrity:** The property of a record being complete and protected against unauthorised or accidental change. [ISO 15489-1:2016 (characteristics)]

**Least Privilege:** Ensuring users and systems have only the minimum access required to perform their role.

**Legal Hold:** A process that suspends normal disposal so relevant records are preserved for litigation, investigation or audit.

**Likelihood:** An assessment of how probable it is that a risk event will occur. [ISO 31000:2018 (risk assessment)]

**Long-term Preservation:** Preserving information for long enough to be concerned with technology change and the needs/knowledge of future users. [ISO 14721:2025 (OAIS long-term)]

**Metadata:** Information about records that provides context and supports identification, search, control, retention and evidential value. [ISO 23081-1:2017 (metadata principles)]

**Metadata Management:** Defining, capturing and maintaining metadata over time so records can be interpreted in business context and their integrity/authenticity supported. [ISO 23081 series (ISO TC46/SC11)]

**Migration (Preservation/Disposal):** Transferring digital records to a new system or format; once verified, the original may be deleted if no longer required. [ISO 14721:2025 (migration)]

**Monitoring and Review:** Ongoing checking of compliance and effectiveness, using evidence to improve policies, controls and behaviour over time. [ISO 30301:2019 (performance evaluation)]

**Off-site Storage:** Storage provided by a third-party facility, requiring clear inventories, access controls and lifecycle management.

**Organisational Context:** The internal and external environment (laws, sector expectations, business priorities and risks) shaping records management requirements. [ISO 31000:2018 (context)]

**Overwriting:** A secure deletion technique where storage locations are overwritten so previous data cannot be recovered.

**Physical Destruction:** Destroying physical records or media so information cannot be reconstructed.

**Physical Records:** Information recorded on paper or other tangible media, kept as evidence of decisions, actions or obligations.

**Preservation Planning:** Planning to maintain long-term access to records, including risk assessment, format strategies and migration schedules. [ISO 14721:2025 (preservation planning)]

**Protective Marking:** A label indicating the sensitivity of information (e.g., classification, caveat), used to guide handling and access decisions.

**Provenance:** Information describing the origin, context and custody of a record, supporting authenticity and evidence. [ISO 15489-1:2016 (provenance concepts)]

**Pulverising:** Industrial destruction that breaks media into fragments (commonly used for CDs/DVDs or hard drives).

**Record:** Information created or received and kept as evidence and as an organisational asset. [ISO 15489-1:2016 (concepts)]

**Records Lifecycle:** Stages a record passes through from creation/capture, active use, storage and management, review, and then disposal or long-term preservation. [ISO 15489-1:2016 (processes)]

**Records Management:** Systematic control of records through their lifecycle to support evidence, accountability and business needs. [ISO 15489-1:2016 (concepts/principles)]

**Records Manager:** Role responsible for implementing records management policies, guidance and controls, and supporting staff compliance.

**Records of Enduring Value:** Records with long-term historical, cultural or evidential significance that should be preserved rather than destroyed. [ISO 14721:2025 (long-term preservation)]

**Records of Processing Activities (ROPA):** A record of personal data processing activities describing purposes, categories, recipients and safeguards; used to demonstrate accountability.

**Reliability:** A record can be trusted as a full and accurate representation of the activity or decision it documents. [ISO 15489-1:2016 (characteristics)]

**Residual Risk:** Risk remaining after existing controls have been applied. [ISO 31000:2018 (risk treatment)]

**Retention Period:** How long a record must be kept after a trigger point before the authorised end-of-life action is applied.

**Retention Schedule:** A policy that links record types to retention triggers, retention periods, and authorised disposition actions.

**Risk Appetite:** The amount and type of risk an organisation is willing to accept in pursuit of objectives, informing risk treatment decisions. [ISO 31000:2018 (risk criteria)]

**Risk Assessment:** Identifying, analysing and evaluating risk to inform decisions about treatment. [ISO 31000:2018 (process)]

**Risk Escalation:** Raising risks that cannot be managed locally to higher governance levels (e.g., SIRO/organisational risk register) for decision and resourcing.

**Risk Treatment:** Selecting and implementing options to address risk, such as treating, tolerating, transferring or terminating. [ISO 31000:2018 (treatment)]

**Secure Disposal:** Destroying or permanently removing records so sensitive information cannot be reconstructed or retrieved.

**Secure Transfer:** Moving information between systems or parties using safeguards such as encryption and controlled access to protect it in transit.

**Security Classification:** A scheme that categorises information by sensitivity and required handling (e.g., OFFICIAL, OFFICIAL-SENSITIVE) to guide protection.

**Selection and Appraisal:** Deciding what should be kept, destroyed or preserved long-term based on value, risk, legal requirements and business need. [ISO 15489-1:2016 (analysis/appraisal)]

**Senior Information Risk Owner (SIRO):** A senior executive accountable for information risk strategy and oversight across the organisation.

**Sensitivity Review:** Reviewing records (especially prior to transfer or release) to manage confidentiality, personal data and other sensitivities.

**Shared Drive Governance:** Rules and ownership arrangements for structure, permissions and review of information stored on shared drives.

**Shredding (Cross-cut/Micro-cut):** A secure disposal method that cuts paper into small pieces to reduce the risk of reconstruction.

**Subject (Transaction):** A more detailed (optional) level within a classification scheme, sometimes called sub-activity, used where extra specificity is needed.

**Subject Access Request (SAR):** A request by an individual to access personal data held about them.

**Sustainable File Format:** A format suitable for long-term access because it is well-documented and widely supported. [ISO 14721:2025 (format/media change)]

**Technical Asset:** A system or application that stores or supports an information asset (e.g., M365, line-of-business system).

**Traceability:** The ability to reconstruct the history of a record (who did what, when, and under what authority). [ISO 23081 series (event history via metadata)]

**Transfer of Ownership:** Handing records to another organisation or department when the original owner no longer requires them, with secure handover and documentation.

**Trigger:** The event or point from which the retention period starts (e.g., case closed, financial year end).

**UK GDPR:** The UK legal framework governing processing of personal data, including principles, lawful bases, and individual rights.

**UK Government Security Classifications (GSC):** The UK public sector classification scheme defining levels such as OFFICIAL and OFFICIAL-SENSITIVE with handling expectations.

**Usability:** A record can be located, retrieved, presented and understood for as long as required. [ISO 15489-1:2016 (characteristics)]

**Version Control:** Managing document changes so the current, draft and superseded versions are clear and staff do not rely on outdated information.