# RECORDS MANAGEMENT POLICY 2026

**Creating and managing records efficiently, making them accessible, protecting them and disposing of them safely at the right time**

## Records Management: Policy on a Page

### What is a record?

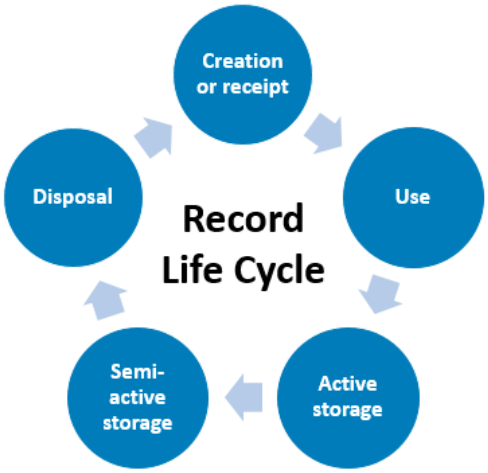
Recorded information, in any format, created or received by you or your department in the conduct or completion of business processes and activities, such as holding a meeting, agreeing a project plan, or appraising a member of staff. The value of a record is determined by its **content** and **context,** not its format – a record must contain enough information to provide reliable **evidence** of the activity that produced it.

### What is records management?

Records management is the framework of tools, policies and procedures that assist you in:

1. **Creating** and **managing** records efficiently,
2. Making them **accessible** to the right people,
3. **Protecting** and **storing** them securely and
4. **Disposing** of them safely at the right time.

This ensures that records are managed appropriately throughout their **life cycle** – from the point at which they are created to their eventual disposal:




### Why is records management important?

Managing our records effectively means that we have the right information at the right time in order to make and evidence the right decisions. It ensures that all of the College's records are created, received, used, stored and disposed of in a way that facilitates their most efficient use and fulfils our compliance requirements.

### How long are records kept for?

Records are kept only for as long as they are required and are disposed of when they are no longer of value. The length of time a record must be kept is subject to the organisational and legal requirements documented in the College **Retention Schedule.**

### What does it mean for me?

- **All employees, Trainees, members, Officers, Board of Trustees/Committee members, volunteers, College representatives and suppliers:**
  - Must **complete induction, refresher and specific training**, appropriate to their role
  - Must **follow all records management requirements in their respective role descriptions, contracts, terms and conditions and/or Code of Conduct**
  - Must ensure that all records they create or receive are **accurate, reliable and accessible**
  - Must **protect and secure all records containing personal data** in compliance with RCOG Data Protection Policies and Procedures
  - Must apply the RCOG Retention Schedule to all records, e.g. add the new Retention Labels to information held in SharePoint
  - Must maintain the departmental sections of the **Information Asset Register** and **Record of Processing Activity.**

The College will take appropriate action against employees, officers, trainees, members, College representatives or suppliers found breaching the Policy where appropriate to them.

## Introduction

This Records Management Policy is the Royal College of Obstetricians and Gynaecologists' (RCOG or the College) policy regarding the safekeeping of all our records from their creation to their disposal – this includes our procedures for sharing information externally.

The RCOG values its information and records as essential assets fundamental to the delivery of its strategic aims. The RCOG recognises that the effective management of records throughout their lifecycle is necessary to perform its core functions, to comply with legal and regulatory obligations, and support business efficiency, continuity and consistency.

## Purpose

The purpose of this Policy is to establish a framework for the creation, maintenance, storage, use and disposal of RCOG records, to support the College's strategic information governance framework, to provide evidence of corporate governance, and to facilitate compliance with statutory requirements.

This policy ensures member, service user, employee, volunteer and Officer records are:

- properly created,
- accessible and available for use,
- disposed of in a secure and timely fashion.

It provides employees, volunteers with RCOG accounts (i.e. email and network access), partners handling RCOG records and Officers with guidance regarding individual responsibility for accuracy and appropriate storage of records, covering:

1. Our Records Management Toolkit for employees, volunteers with RCOG accounts and Officers
2. Management of our merged Information Asset Register (IAR) and Record of Processing Activities (ROPA)
3. Our transparency and accountability procedures
4. Our information handling procedures, including:
    a. safely and legally sharing information externally,
    b. processing individual rights requests under UK GDPR,
    c. managing the withdrawal of consent.

The RCOG aims to be compliant with international and national standards and codes of practice for Records Management, e.g. BS 10025:2021 Records management – Code of Practice. The benefits of compliance are:

- RCOG business is conducted in an orderly, efficient and accountable manner, preserving accurate and authentic business records
- RCOG services are delivered in a consistent and equitable manner with understanding of previous completion of transactions
- A reliable knowledge base is preserved
- Business evidence of organisational activities is captured to provide consistency, continuity and productivity
- Vital records are identified to provide continuity in the event of a disaster
- Legislative and regulatory requirements are met with retention and provision of access to records
- RCOG maintains corporate memory through capturing evidence of business activity and identifying records of historical significance for permanent preservation
- Current and future research and development activities are supported through documentation

The RCOG is committed to the efficient and effective management of its records to maximise the benefit they bring to the College, as they are its corporate memory and ensure:

- good corporate governance,
- accountability,
- compliance with legal requirements,
- evidence of decisions and actions, and
- informed decision-making.

## Scope

This policy applies to:

- All records held by the RCOG in either paper or digital format, including records containing personal data
- All employees of the RCOG (permanent and temporary), volunteers with RCOG accounts, Officers and Committee members handling College records, contractors and consultants who have access to records, wherever these records may be located. The policy aims to ensure that all those handling College records are aware of what they must do to manage records in an effective and efficient way and in compliance with legal and regulatory requirements

## Related policies

This policy is part of the RCOG Information Governance and Security Framework that includes:

- Data Protection Policy and Procedures (internal only)
- Data Security and Protection Incident Handling Policy and Procedures (internal only)
- IT Security Policy (internal only)
- Privacy Policy
- Information Asset Register and Record of Processing Activity (held internally).

## Legal obligations

The management of records held by the College is regulated by and complies with the following legislation, principles and Codes of Practice:

- UK GDPR and Data Protection Act 2018
- Data (Use and Access) Act 2025
- Limitation Act 1980
- NHS Records Management Code of Practice 2021
- Caldicott Principles.

The College is not a public authority and is not subject to the Freedom of Information Act (FOIA) 2000. Official College records are not accessible under the FOIA, and requests are not routinely considered and responded to in accordance with internal procedures for Handling Requests for Information (RFIs). Where the RCOG performs work for a public authority under contract, the College may hold information 'on behalf of' this authority and information relating to these activities may be subject to the FOIA.

Records created by certain College functions have specific retention requirements set out in separate legislation such as those relating to employment, health and safety, finance and pensions, and environmental information. These are documented in the RCOG Retention Schedule.

Clinical and research data may have specific requirements in relation to management, storage, retention and disposal set out under the terms of funding contracts service agreements, or data sharing agreements that must be adhered to.

## Policy

A record is recorded information, in any form (it may be an electronic file or e-mail, or a paper document), created, received and maintained by the organisation or individual employees and Officers to support and show evidence of its activities. Also referred to as an "information asset".

Although not an exhaustive list, examples of items that can constitute records include:

- documents (including written and typed documents and annotated copies)
- computer files (including word processor files, databases, spreadsheets and presentations
- paper based files
- electronic mail messages
- reports
- The RCOG Hub and Internet Web pages
- MS Teams content, including Chat and meetings
- SharePoint Sites (SPS)
- Case files, such as Membership, trainee and staff records.

See Appendix A for more detailed definitions of a record and other related terms.

The RCOG recognises the importance of this essential resource and undertakes to:

- manage electronic and paper records effectively in line with this policy
- comply with legal obligations that apply to its records (see the RCOG Data Protection Policy and Procedures (internally only))
- exercise best practice in the management of records, as outlined in the Procedures below
- encourage effective access to and use of records as a corporate source of information, to support business efficiency and decision-making
- manage and store records in a suitable format to retain quality, relevance, accessibility, durability and reliability
- store records efficiently, utilising appropriate storage methods at all points in their lifecycle, and disposing of them securely when they are no longer required
- provide appropriate protection for records from unwanted environmental (fire, flood, infestation) or human impact (alteration, defacement, theft)
- safeguard vital records necessary for business continuity and regeneration in the event of a disastrous occurrence
- identify and make provision for the preservation of records of long term and historical value, which meet our Archive Collections Development Policy Criteria for Acquisition
- maintain high data quality standards in accordance with the UK Government Data Quality Framework
- review this policy and procedures annually to ensure they are adequate and that RCOG records continue to be kept to the highest standards.

This policy is implemented and supported by a set of procedures and ways of working, which have been designed according to the requirements of international standards of information, documentation and records management. These are included in Appendix B (internal only).

# Governance

## IGMG

The Information Governance Management Group (IGMG):

- Oversees the IG function of the College to ensure compliance is retained across the College
- Chaired by the SIRO
- Supported by Corporate Governance and RIGO

It is made-up of Directors from departments who process personal data and Subject Matter Experts (SME). The terms of reference are in Appendix B.

## IG Leads

The IG Leads are employees nominated by the departmental Information Asset Owners (SLT member) to assist them with their IG responsibilities. Please see Appendix D for their terms of reference.

## Performance Monitoring

- IG Dashboards – RCOG performance against key statutory compliance requirements are monitored at least quarterly, covering:
    - Individual Rights Requests – e.g. Data Subject Access Requests
    - Data Protection and Security Incidents – e.g. numbers logged as live, contained and closed with a severity rating and outstanding actions from lessons learned
    - Data Protection Impact Assessments – e.g. numbers logged with data protection risk rating
- Audit and Risk Committee (ARC) – quarterly compliance reports highlighting progress against regulatory (Data Security and Protection Toolkit) and statutory requirements using the IG Dashboards (see above), reviewed and approved by the Executive Committee ahead of submitting to the ARC.

# Roles and responsibilities

The RCOG has a responsibility to ensure that its records are managed well and in accordance with the regulatory environment. Different employees and Officers have different roles in relation to records management, and these responsibilities are defined below.

The **Executive Committee** has high level responsibility for ensuring compliance with this policy. Individual Executive Directors and Directors have responsibility for ensuring:

- their teams develop their own procedures and guidance which comply with the records management policy and procedures
- adequate records of their directorate's activities are maintained
- their employees and Officers comply with College-wide records management policy and procedures
- their employees and Officers attend the necessary records management training available via the Learning and Development Programme.

The **Senior Information Risk Officer (SIRO)** is delegated authority for information risk and mitigation by the Executive Committee, including responsibility for implementing and leading on IG risk assessment and management processes with the College. They:

- lead and foster a culture that values, protects and uses records and information for the success of the organisation and benefit of its members, trainees, staff and other stakeholders

- own the RCOG's overall information risk assessment processes and ensuring they are implemented consistently
- ensure the Board of Trustees, Officers and the Executive Committee are adequately briefed on IG issues and associated risks
- leads on the annual Data Security and Protection Toolkit submission to NHS Digital and the College's subsequent improvement plan
- develops and oversees the College's IG strategy and associated work programmes providing specialist advice and assistant to staff where required on areas of information governance legislation, ensuring specialist knowledge is kept up to date and changes in legislation or national and local policy are communicated effectively to staff at all levels of the organisation
- leads the College's work on information rights compliance, information asset and records management, and information risk assurance and management
- lead liaison with external regulators, such as the Information Commissioner's Office (ICO)
- lead on the of security incidents and data protection breaches
- own the College's Data Security and Protection Incident Handling policy and procedures
- provide the final point of resolution for any IG risk issues, and
- Chair the IGMG (IG Management Group).

The current SIRO is the Executive Director of Membership and Global, Kristen Morgan.
The **Caldicott Guardian** is primarily responsible for the protection of confidential, personal information and ensure it is used in line with the Caldicott Principles, with responsibility for the following:

- protecting the confidentiality of patient information
- enabling appropriate information-sharing
- ensuring the College satisfies the highest practical standards for handling patient identifiable information
- acting as the 'conscience' of the organisation
- actively supporting work to enable information sharing where it is appropriate to share, and
- advising on options for lawful and ethical processing of information.

The current Caldicott Guardian is the Director of Clinical Quality, Daniel Wolstenholme.

The **Information Governance Management Group (IGMG)** has responsibility for ensuring that the RCOG's record keeping supports Information Governance compliance.

The **Information Governance (IG)** function is delivered by the RIGO with additional subject expertise brought in, when necessary (see below), who are responsible for maintaining and implementing the Records Management Policy, including management of the off-site storage for semi-active and archive paper records.

The **Records and Information Governance Officer (RIGO** is responsible for the following:

- supports the SIRO and Caldicott Guardian
- manages the handling of requests for information (RFIs) according to information rights and copyright legislation
- coordinates, maintains and develops the information asset register (IAR), including information sharing protocols and agreements
- data security and protection incident reporting
- maintenance of the information risk register, ensuring remedial actions have been undertaken

- establish, develop and deliver both mandatory and discretionary staff training
- raising employees, volunteers and Officers awareness of records management
- establish, develop and deliver IG policies, procedures, guidance notes and ways of working
- preserving and providing access to the RCOG's Archives
- creation, analysis and presentation of performance indicators, such as a quarterly IG Dashboard
- provide a public frontline information rights handling and enquiries service
- deliver a functioning records management service the College's structured and unstructured records
- developing and maintaining retention and disposal schedules and documenting disposal activity, including management of the retention label framework with IM&T and process to ensure if reflects the approved RCOG Retention Schedule
- maintaining the Information Asset Register (IAR) and Record of Processing Activities (ROPA)
- providing advice and support to the IG Leads, Information Asset Owners and the wider organisation
- manage and respond to copyrights and permission request for the College's publications, ensuring compliance with copyright law and organisational policies.
- advising the SIRO and Executive Committee on potentially reportable data security and protection incidents/breaches, and
- deputising for the SIRO, as required.

The **Heritage Manager with the RIGO** manages the process transferring Semi-Active Records into the Permanent Archive using the RCOG Retention Schedule and new SharePoint retention labels.

The **Information Asset Owners (IAOs)** across the College have been delegated to Directors or Head of Service. They are responsible for enabling effective IG within their respective areas and teams, such as making decisions about how information is processed e.g. what is collected, how it is used, whom it is shared with, when it is deleted, and whether information risks are mitigated further or accepted by us. They:

- understand what information assets their team(s) process(es)
- understand its value to the College and the related approach, appetite and capacity for risks and opportunities in conjunction with the College's risk management standards
- make sure the information is managed according to this and all relevant IG, Data Security and Protection Policies
- are responsible for reviewing information where the retention label has expired, notification is automated and the information is held for up to 12 months before moving onto the Recycling Bin
- nominate a local Information Governance Lead (IG Lead) provide senior management support to IG Lead in discharging their role, and
- identify, oversee and support the work of information asset administrators within their areas of responsibility.

The **Information Asset Administrators (IAAs)** people nominated by IAO to assist with the operational responsibility for information asset management within their respective service areas. This involves the:

- application of IG rules
- identification of information assets to the IG Team, and
- updating RCOG records and information to ensure data integrity and quality.

In some departments, the IG Lead is also the IAA.

The **Information Governance (IG) Leads** are employees nominated by the departmental IAOs (SLT member) to assist them with their IG responsibilities. Please see Appendix D for their terms of reference.

The **Director of Information Management and Technology (IM&T)** is responsible for ensuring that adequate technical provision is in place to support record keeping across the organisation.

The **Director of Building and Guest Services** is responsible for providing adequate and appropriate storage and disposal facilities to support record keeping across the organisation.

The **Corporate Governance and Risk Team** are responsible for maintaining records of their committees and managing their disposition in line with the instructions provided in the Retention Schedule.

**All Employees, Volunteers with RCOG accounts and Officers** that create, receive, maintain or delete records are responsible for ensuring that they do so in accordance with the RCOG's Records Management Policy and procedures.

## Policy Waiver

The College has a risk-based approach to govern those situations that require the processing of personal data to deviate from this policy. In summary:

- The situation needs to be fully described
- The risks and mitigations captured
- The agreed waiver reviewed and signed off by the Information Asset Owner and Executive Director.

The Policy Waiver form in Appendix F must be completed and approved by senior management.

***For further advice concerning any aspect of this policy, please contact the Information Governance (IG) Team by email or call +44 20 7772 6309.***

# Appendices

## Appendix A: Glossary of Terms

An **Active Record** is one that is in "active" use or open, e.g. records created and used throughout an individual's membership with or employment at the College and stored on the following systems:

- Cascade
- iMIS
- Corporate file plan currently held as part of the College's legacy R: drives on a dedicated, local platform
- SharePoint sites (SPS) and associated document libraries.

An **Archive Record** is a record that has reached the end of its retention period (as per the College Retention Schedule) and is retained permanently because of its continuing business, evidential, historical or informational value to the College, e.g. minutes from Board of Trustees meetings.

**Business Information Systems** are databases, or other software, that create or capture information in relation to RCOG business. They are primarily used for reference but can be used for workflow or data sharing. Systems that hold information the RCOG would rely on as evidence should be able to manage their content as records and be Record Keeping Systems.

**Data** is the raw input from which information of value is derived.

A **Data Controller** is an individual or organisation who:

- decides to collect or process personal data
- decides what the purpose or outcome of processing is to be
- decides what personal data should be collected
- decides which individuals to collect personal data about
- obtains a commercial gain or other benefit from the processing, except for any payment for services from another controller
- processes personal data as a result of a contract between us and the data subject
- whose data subjects are the employees
- makes decisions about the individuals concerned as part of or as a result of the processing
- exercises professional judgement in the processing of the personal data
- has a direct relationship with the data subjects
- has complete autonomy as to how the personal data is processed
- has appointed processors to process the personal data on our behalf.

**Joint Data Controllers** are two or more individuals or organisations who:

- has a common objective with others regarding the processing
- processes the personal data for the same purpose as another controller
- use the same set of personal data (e.g. one database) for this processing as another controller
- designs the processing with another controller
- has common information management rules with another controller.

A **Data Processor** is an individual or organisation who:

- follows instructions from someone else regarding the processing of personal data
- is given the personal data by a customer or similar third party, or told what data to collect
- does not decide whether to collect personal data from individuals
- does not decide what personal data should be collected from individuals

- does not decide the lawful basis for the use of that data
- does not decide what purpose or purposes the data will be used for
- does not decide whether to disclose the data, or to whom
- does not decide how long to retain the data
- make some decisions on how data is processed, but implements these decisions under a contract with someone else
- is not interested in the end-result of the processing.

The **Data Protection Act 2018** is an Act of Parliament that enacted GDPR 2016 and established UK only derogations.

**Data quality** is a recognition that the accuracy, coverage, timeliness and completeness of data can significantly impact on the value of its use.

A **Data subject** is a living individual who can be identified from the personal data or from additional information held, or obtained, by the RCOG. For example, a CCTV image which can identify someone when linked to building access control codes.

The **Data (Use and Access) Act 2025** is a new Act of Parliament that updates some laws about digital information matters. It amends but does not replace: UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations.

A **File** is a collection of records stored in one unit, identified by a filename. It can be a document, picture, audio or video stream, data library, application, or other collection of data.

A **File Plan** is a governance tool that classifies RCOG records in terms of function and activity; it acts as the baseline to connect this policy, and its related guidance and procedures, to the business processes that create, manage, use and dispose of College records.

The **Freedom of Information Act 2000 (FOIA)** provides the public with a general right of access to all information held by, or on behalf of, public authorities. Any individual or organisation may request any information held by a public authority. The public authority must tell the applicant (normally within 20 working days) whether it holds the information. If it does, it must supply it, unless an exemption applies.

The **UK General Data Protection Regulation (UK GDPR):** sets out data protection and privacy rights of all individuals within the UK since exiting the European Union. It also applies to transfer (export) of personal data outside the UK. UK GDPR came into force on 01 January 2021.

An **Information Asset** is a body of information defined and managed as a single unit or aggregate so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

The **Information Asset Register** is a governance tool that lists the RCOG's key information assets and a mandatory requirement of the NHS Data Security and Protection Toolkit.

The I**nformation Commissioner or ICO** is responsible for the regulation of the Information Rights legislation across the UK, such as UK GDPR and DPA 2018. The Information Commissioner is appointed by the Queen and is independent of the UK Government.

**Information Governance**:

- encompasses the multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an organisation level,
- supports its immediate and future regulatory, legal, risk, environmental and operational requirements
- determines the balance point between two potentially divergent organisational goals: extracting value from information and reducing the potential risk of information
- defines the roles and responsibilities of all stakeholders involved in handling and managing College information.

**Information governance compliance** ensures compliance with all statutory requirements governing the management of information, including rights of access under Freedom of Information and Data Protection legislation.

**Information security** ensures that RCOG information is not compromised by unauthorised access, modification, disclosure or loss.

**Information sharing** ensures that RCOG information is shared in a compliant, controlled and transparent manner.

A **legal hold** is a restriction on a record that exists as a result of current or anticipated litigation, audit, government investigation or other such matter that suspends the normal retention and disposition of records

**Personal data** is all information that relates to an identifiable living person who can be identified from that information or from additional information held, or obtained, by the RCOG. Examples of personal data are contained in paper files, electronic records and visual and audio recordings.

**Processing** is all actions relating to personal data. Gathering, recording, analysing, amending, using, sharing, disclosing, storing and destroying personal data are all covered by this definition.

**RCOG Records** are defined as:

- recorded information in any format (including paper, microform, electronic and audio-visual formats) including records stored within SharePoint and other approved digital system.
- which are created, collected, processed, and/or used by RCOG employees and Officers, Trustees, Council, FMTs and other stakeholders when undertaking RCOG business, or contractors performing an RCOG function or service; and
- are then kept as evidence of that business.

A **RCOG record life cycle** covers the lifespan of a record throughout the following stages:

- Creation – e.g. the creation of new trainee/Member case file
- Usage = Active – e.g. a current Member case file
- Storage = Semi-Active – e.g. retained for 5 years following a member ending their membership and their case file closing
- Disposal – e.g. the destruction of the Member case file at the end of the retention period or permanent retention in the College Archives.

**Records management** is a set of processes and practices that ensure RCOG records are systematically controlled and maintained, covering the creation, storage, management, access, and disposal of records, in compliance with best practice, legal obligations and policy requirements.

A **Record Series** is a collection of records with a connection that are grouped together to be accessed and managed as a single item. The RCOG Record Series are defined in the Retention Schedule.

The RCOG Retention Schedule is in the process of being added to SharePoint and Microsoft 365 using an agree list **retention labels** made up of simplified 'retention buckets' that have been mapped from the Retention Schedule. Each bucket represents a group of records with the same retention period and disposal action, using the longer time period within the Retention Schedule to avoid premature disposal. These labels within SharePoint automatically apply retention rules and trigger review or disposal actions once the retention period has expired. The labels are:

- 1 year (includes information requiring immediate deletion) – e.g. personal data used for safeguarding purposes, such as DBS checks
- 4 years – e.g. internal communications, such as staff bulletins, and information without a retention period in the RCOG Retention Schedule
- 8 years – e.g. trainee files and Member registration forms
- 16 years – e.g. US building inspection records and complaints
- 24 years – e.g. AV content for RCOG projects and records of information destruction
- 40 years – e.g. asbestos testing/monitoring records and Exam candidate misconduct
- 100 years – e.g. staff pension enrolment and contribution records
- Permanent Archive – e.g. College working group/task force records and GMC approved curricula.

A **Retention Schedule** contains:

- the categories of records held by an organisation – the Record Series
- the start and end of the time-period that record is held for – the Retention Period
- a definition of the activity that triggers the beginning of the retention period – the closure of an active record
- the retention 'bucket' the Record Series has been mapped to in order to create the Retention Labels.

A **Semi-Active Record** is a record that is no longer in "active" use and has triggered the beginning of its retention period as per the RCOG Retention Schedule.

A **SharePoint Site** is the repository of a College departments unstructured information, documents and records. The were introduced in September 2025 and contain the College's Active and Semi-Active records migrated upon introduction and added since.

**Special Categories** of personal data: include data revealing:

- race or ethnicity
- religious or philosophical beliefs
- trade union membership
- a person's health
- sex life or sexual orientation
- genetic or biometric data.

A **Subject Access Request** is the right given, by Data Protection legislation, to an individual to ask for a copy of personal data processed by the College. The information must be supplied in an intelligible and permanent form unless this involves a disproportionate effort or the individual agrees otherwise. The RCOG may have to consider the Disability Discrimination Act requirements when providing personal data to an individual who may require the information to be provided in a certain

format to consider a special need.  Individuals have a right to correct inaccuracies in that information too – please see the RCOG Individual Rights Requests guidance for details.

**Weeding** is the process of removing and destroying redundant, obsolete or trivial information, including draft documents and duplicates.