RECORDS MANAGEMENT POLICY AND PROCEDURES 2023

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?

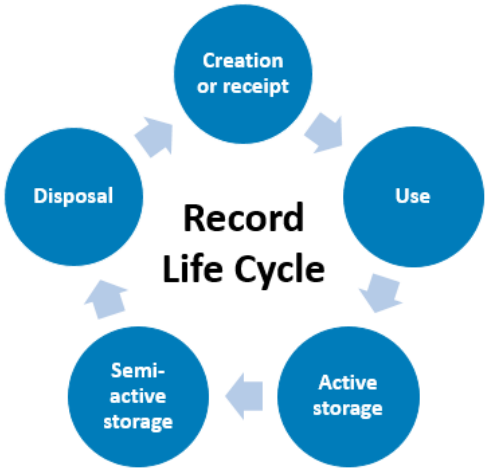
Recorded information, in any format, created or received by you or your department in the conduct or completion of business processes and activities, such as holding a meeting, agreeing a project plan, or appraising a member of staff. The value of a record is determined by its **content** and **context,** 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/to the College's standards

- 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
- 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 Gynaecologist's (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.

These are working documents for staff so some of the hyperlinks are not accessible via the RCOG website.

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 and Officer records are:

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

It provides employees and Officers with guidance regarding individual responsibility for accuracy and appropriate storage of records. It covers:

1. Our Records Management Toolkit for employees 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, temporary and voluntary), 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 employees and Officers 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
- Data Security and Protection Incident Handling Policy and Procedures
- IT Security Policy
- Privacy Policy
- Information Asset Register and Record of Processing Activity.

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
- 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, but requests are 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 College 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 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
- Intranet and Internet Web pages.

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)
- 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.

To support the RCOG's recognition of the importance of Records Management, all people handling RCOG records must comply with this policy by following the procedures listed below.

Procedures

This policy is implemented and supported by the following procedures and ways of working, which have been designed according to the requirements of international standards of information,

documentation and records management. All RCOG employees and Officers must adhere to the following procedures:

1. Creating, locating and retrieving records

1.1 Understand what constitutes a record (see Policy definition above) and its life cycle and be familiar with the definitions contained in this policy (see Appendix A)

1.2 Follow guidance and complete training on the creation and use of records, and understand their legal responsibilities to share and safeguard personal and confidential information, e.g. all staff creating and using member records held in our CRM must not share their username or password

1.3 Capture and organise records according to RCOG standards to ensure that records are accessible, retrievable and readable:

1.3.1 Use the Corporate File Plan as a standardised structure and layout for the contents of records with local file plans informed by the RCOG Retention Schedule's Record Series classification and listed in the Information Asset Register

1.3.2 Use Naming Conventions to consistently name documents and folders with appropriate and version control to ensure ease of access and the application of the Retention Schedule

1.3.3 Use RCOG templates to ensure electronic records are created in a consistent format with appropriate document properties

1.4 Complete a records transfer form when preparing semi-active paper records for transfer to our offsite storage provider, and ensure records are inventoried and boxed appropriately to enable accurate retrieval and subsequent tracking

1.5 Ensure records are accessible to enable individuals to exercise their rights under UK GDPR where their personal data is held within College records, following our RCOG Individual Rights Request guidance and Handling Requests for Information procedure and covering:

a. The right to be Informed - e.g. fair processing/privacy notices and information
b. The right of Access - e.g. subject access requests (SARs)
c. The right to Rectification - e.g. correcting your data
d. The right to Erasure – e.g. deleting or removing your data
e. The right to Restrict Processing – e.g. stopping your data being used
f. The right to Data Portability – e.g. transferring your data easily
g. The right to Object – e.g. challenging what we're doing with your data
h. Rights in Relation to Automated Decision Making and Profiling – e.g. ensuring safeguards are in place so we don't make potentially damaging decisions about you without any human involvement

1.6 Identify the appropriate lawful basis before processing records and information containing personal data and ensure the lawful basis is accurately recorded in the Information Asset Register (IAR) and Record of Processing Activities (ROPA) - see section 7 below

1.7 Ensure that all records containing personal data are created and managed in line with RCOG transparency and data protection procedures:

1.7.1 Ensure our privacy notice outlines to people why we hold their data, the lawful basis for doing so, and their rights in terms of how we process their data

1.7.2 Ensure our privacy notice is freely available to all people whose data we process and is part of our commitment to transparency and accountability to satisfy the individual's right to be informed under GDPR

1.7.3 Ensure our privacy notice is available on the footer of every page of the RCOG website: https://www.rcog.org.uk/

1.7.4 Ensure all service users, or their legal representative if necessary, will be informed of their rights regarding their personal data when they sign-up to be an employee, member/trainee, or other service user of the College

1.7.5 Review and update the privacy notice at least annually and obtain Executive Committee sign-off

1.7.6 Provide people with the RCOG Privacy Policy, and any supplementary notices developed for specific processing, at the moment we ask them to give us their personal data

1.7.7 Ensure that when we receive an individual's personal data from a source other than that individual, we provide them with the RCOG Privacy Policy without undue delay and at least within one month.

2 Information transfers

2.1 Ensure that RCOG records and information containing personal data are protected and not disclosed inappropriately, either by accident or design, whilst in use or when they are being transferred, e.g. by using Mimecast to encrypt all personal data sent via email

2.2 Ensure the processing and sharing of RCOG records and information containing personal data with external, third parties must follow one and/or other of the following processes to ensure it is safe and legal:

2.2.1 Client (Data Controller) and Contractor (Data Processor) personal data sharing must be governed by a written and signed contract or service agreement that meets RCOG data protection standards, e.g. the RCOG Contract/Service Agreement plus Data Protection Schedule. Where the contract proposed is different to the RCOG contractual templates, you and the IG Team are to complete a "risk assessment" as part of "due diligence" and assess if the differences/gaps pose a risk to the College

2.2.2 Equal partner (Data Controller to Data Controller) personal data sharing must be governed by a written and signed Information Sharing Agreement (ISA) that meets RCOG data protection standards, e.g. the RCOG Information Sharing Agreement template

2.2.3 Joint or separate Data Controllers where both data processing and control is shared between the RCOG and another organisation, then both a contract and ISA is to be used.

2.3 Refer to the following policies regarding the secure handling and transfer of RCOG records and information containing personal data:

a. Data Protection Policy and Procedures
b. IT Security policy

2.4 Implement procedures to enable withdrawal of consent to share personal data:

2.4.1 Ensure all people have the right to withdraw their consent to have their personal data shared at any time

2.4.2 Guarantee it is as easy to withdraw consent as it is to give consent – the processes will vary dependent on the nature of consent obtained for data processing

2.4.3 If an individual withdraws their consent to share their personal data, to discuss it in full and explain how this decision may impact the service outcome for which their data is being processed

2.4.4 In certain instances, where legislation or public good outweighs the individual's right to not consent to information sharing, we may not be able to honour any withdrawal of consent. This needs to be discussed in detail with the IG Team and will only occur if we can demonstrate compelling legitimate grounds where the processing overrides the interests, rights and freedoms of the individual.

2.4.5 The Senior Responsible Officer to keep a log of consent not given or withdrawn, adding a note to the individual's records.

3 Data quality

3.1 Maintain all records according to RCOG standards of data quality, including:

3.1.1 Accuracy – ensuring all data is sufficiently accurate for its intended purposes

3.1.2 Completeness - ensuring you have all the data required for a particular purpose

3.1.3 Consistency - ensuring data formats do not conflict with each other within a record or across records and datasets, e.g. all address data held in our CRM must follow the same format

3.1.4 Timeliness – all data must be captured as quickly as possible, be available for use when needed and disposed of without delay once no longer required, in line with retention requirements in the College's Retention Schedule

3.1.5 Uniqueness – the authoritative and definitive version of a record must be clearly identified to prevent the creation of duplicate versions containing conflicting data

3.1.6 Validity – all data must be recorded and used in compliance with College requirements

3.2 Conduct regular data quality reviews to make sure that records containing personal data are accurate, adequate and not excessive, e.g. all data sets shared by partner organisations must be reviewed on receipt to ensure that they do not contain personal data beyond that which is directly relevant and necessary to accomplish the specified purpose.

3.3 Perform regular reviews and periodic 'weeding' of records containing personal data to reduce the risks of inaccuracies and excessive retention.

5. Access control

4.1 Ensure both paper and digital records are held in accessible but protected central locations, controlled by up-to-date security permissions to prevent unauthorised access to and disclosure of information, in compliance with the IT Security Policy and Data Protection Policy and Procedures, e.g. restrict folder access to the necessary members of staff, and apply password protection to files containing confidential information

4.2 Store all records essential for business use in the central corporate file plan in the R: drive, so that departments can operate efficiently when individual employees are absent or leave the College. The P:drive is only to be used for personal purposes

4.3 Use links to electronic records and folders instead of attachments when sharing information internally, to control access and avoid storing duplicate data unnecessarily

4.4 Store any paper records containing personal or confidential information in locked cabinets or secured rooms when not in use.

5. Retention

5.1 Apply all organisational, statutory and regulatory retention periods set out in the College Retention Schedule to ensure that records are kept only for as long as they are required to meet business and legal requirements

5.2 Regularly review records containing personal data to identify opportunities for minimisation, pseudonymisation or anonymization, and ensure personal data is retained only for as long as is strictly necessary, e.g. review external stakeholder contact lists on an annual basis and remove any outdated or unnecessary information

5.3 Notify the Information Governance (IG) Team of any new records created during the course of RCOG functions that are not already included in the classification scheme, to ensure that the Retention Schedule is accurate and up to date

5.4 Assist the IG Team where it is necessary to retain specifically identified individual records, or group of records (clinical or otherwise), for longer than the stated retention period, such as Public Inquiries and ongoing subject access requests.

6. Disposal

6.1 Implement and record disposal decisions, in partnership with the IG Team and Information Asset Owner (IAO), to ensure that records are fully and correctly managed throughout their lifespan

6.2 Ensure that all records containing confidential information are destroyed in line with the Disposal of confidential material guidance and any contractual obligations, e.g. using approved data erasure software to securely destroy sensitive personal data supplied by NHS Digital or another Data Controller where the RCOG is the Data Processor

6.3 Information Asset Owners must ensure that records are destroyed in a timely and secure manner, and that all copies, including duplicates and where possible backup copies, held in any format are destroyed at the same time

6.4 Ensure all contracts with third parties include the standard data protection clauses mandating the secure and timely disposal of personal data and the provision of destruction certificates by the supplier to the RCOG

6.5 In partnership with the IG Team, ensure semi-active paper records held offsite are reviewed at the end of their retention period and any records eligible for permanent preservation are retrieved and referred to the Archivist for appraisal

6.6 Return any IT equipment for disposal to Information Management and Technology (IM&T) to ensure that it is completed securely and that any information remaining on any storage device is securely wiped.

7. Information asset register

7.1 Information Asset Owners (IAO) must ensure their department's section of the IAR and ROPA is kept accurate and up-to-date by following the Maintaining the IAR and ROPA procedure and by participating in the College-wide annual review of the IAR and ROPA

7.2 Information Asset Administrators must support the IAOs in maintaining their department's section of the IAR and ROPA, e.g. by conducting regular reviews to ensure that the list of assets is up to date and the ROPA accurately reflects the department's current processing activity, and by notifying the IG Team of any significant changes.

8. Business continuity, disaster recovery and back-ups

8.1 Corporate Governance, in partnership with Buildings and Guest Services, must maintain a risk-based Business Continuity Plan to manage disruption and a Disaster Recovery Plan to manage technical and environmental disasters, which identify and make provisions for vital records that are critical to the continued functioning of the College

8.2 Information Management and Technology (IM&T) must conduct regular backups of all relevant systems for recovery purposes and replicated data to a secure offsite location on a daily basis, as per the IT Security Policy.

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 the IG Team.

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 – quarterly compliance reports highlighting progress against regulatory (Data Security and Protection Toolkit) and statutory requirements using the IG Dashboards (see above)
- Executive Committee – quarterly Data Security and Protection Toolkit (DSPT) project reports focusing on progress made against the DSPT for that year.

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
- 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 **Deputy SIRO** is the Head of Information and Governance and is responsible for the strategic improvement, day-to-day operation and delivery of IG within the RCOG. This includes, but is not limited to:

- supports the SIRO and Caldicott Guardian

- leads on the following IG areas – information rights compliance, information asset and records management, and information risk assurance and management
- manages the handling of requests for information (RFIs) under according to information rights and copyright legislation
- co-ordinating, maintaining and developing the information asset register (IAR), including information sharing protocols and agreements
- data security and protection incident reporting and
- maintenance of the information risk register, ensuring remedial actions have been undertaken
- 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
- establish, develop and deliver both mandatory and discretionary staff training
- establish, develop and deliver IG policies, procedures, guidance notes and ways of working
- preserving and providing access to the RCOG's Archives
- lead liaison with external regulators, such as the Information Commissioner's Office (ICO)
- 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
- maintain the RCOG Retention Schedule
- advising the SIRO and Executive Committee on potentially reportable data security and protection incidents/breaches, and
- deputising for the SIRO, as required.

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) team** is made up of the Head of Information and Governance, who is the RCOG Deputy SIRO, and the Records and IG Officer 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:

- ensuring that the records management policy and procedures, guidance and training are kept up to date and relevant
- raising employees and Officers awareness of records management
- providing advice and guidance to all employees and Officers
- developing and maintaining retention and disposal schedules and documenting disposal activity
- 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
- investigating security incidents and breaches
- coordinating IG Team managed Requests for Information (RFIs) such as Individual Rights requests, e.g. Subject Access Requests (SARs).

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
- 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 Information Asset Owners 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 Information Asset Owners (SLT member) to assist them with their IG responsibilities. Please see Appendix D for their terms of reference.

The **Director of 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 Team and Personal Administrators** are responsible for maintaining records of their committees and managing their disposition in line with the instructions provided in the Retention Schedule.

All Employees 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 E 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
- Open Engage
- Corporate file plan.

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.

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** 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);
- 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.

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.

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 College Retention Schedule.

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.

Appendix B: IGMG Terms of Reference

- To provide strategic leadership for information governance and information risk management throughout the College, reporting into the Executive Committee, Officers (as appropriate) and Audit and Risk Committee with Director representation from key departments, namely those handling large volumes or high risk personal data, such as Clinical Quality, Membership, Education, Exams and People.
- To support, monitor and authorise the development of the Information Governance Framework and its implementation, including all accompanying policies, guidance and tools.
- To support the College's Information Governance network of IG Leads.
- To oversee the College's annual Data Security and Protection Toolkit Submission (formerly known as the IG Toolkit).
- To agree, support and monitor the annual Data Security and Protection Improvement plan to drive change, including plan revision and realignment to mitigate risk.
- To take ownership of information risk management, including monitoring compliance with the Information Governance Framework, reporting and escalating information risks as appropriate, taking corrective actions where necessary, and maintaining the IG Risk Register.
- To receive and consider reports into breaches of confidentiality and security and, where appropriate, undertake or recommend remedial action.
- To develop solutions and implementation programmes (including training and raising awareness) to ensure that the RCOG complies with developing information governance requirements.
- To ensure that each directorate fulfil their responsibilities and apply relevant information governance policies and controls.

- To support directors and managers with the implementation of information governance standards and policies, the management of information risks, and in promoting awareness throughout their areas.
- To support audit and assessment arrangements for information governance (internal and external).
- To ensure that the College's approach to information governance and information risk is effective in terms of resource, commitment and execution, and that it is communicated to all staff.
- To liaise with boards, committees and other working groups to ensure compliance with the College's Information Governance Framework.
- To provide a focal point for the resolution and/or discussion of information governance and risk issue.

Appendix C: IGMG Forward Plan

The remit of the IGMG is broad and requires detailed monitoring of information risk. As such, the following forward plan is in place to ensure there is sufficient time to complete this work and to assist with the IGMG meeting agenda.

The following "standing items" are included in the agenda for every meeting:

- Data Security and Protection (DSP) Submission and Improvement Plan – quarterly progress report
- IG Dashboards
- DSP Incident Register – review and escalation

The following "standing items" are only included in the agendas of these quarterly meetings:

- **January**
  - Review and sign-off the revised DSP policy and procedures framework
- **March**
  - Review and sign-off the revised DSP ways of working, staff training and communications framework
  - Review the Information Risk Register
- **June**
  - Review and sign-off updates to the Information Asset Register
- **October**
  - Review and approve the proposed DSP Toolkit Submission Plan for the next year.

Appendix D: IG Leads Terms of Reference

- To represent the IG needs of their department and be either a Head of Service or Team Lead role, supporting and deputising for the SLT Information Asset Owner
- To champion IG within their departments, including data protection and records management
- To be the first point of contact on all IG related matters, including data protection and records management, within their departments
- To develop a good knowledge and understanding of relevant IG, including familiarity with the policies and ways of working
- To complete all relevant IG training over and above the College's mandatory requirements, including Advanced Data Protection and relevant modules
- To raise and monitor awareness of good IG practice within their departments, especially the processing of personal data

- To attend IG Team organised meetings and events
- To actively engage with and contribute to the internal IG consultations, including the annual DSPT submission and DSP policy reviews to act as a contact point with the IG Team concerning the retention, disposal and transfer of records within the department
- To assess the records management procedures as they relate to each business function within their departments
- To assist employees and Officers on team records management procedures.

Appendix E: Policy Waiver Form

[Insert policy title here] POLICY WAIVER AUTHORISATION FORM - REF. [insert policy initials here]-000

Working together to handle personal data safely, respectfully and lawfully

Directorate:	**Information Asset Owner:**
Department:	**Information Asset Administrator/IG Lead:**
Proposed by departmental SLT member:	
Approved by Executive Director:	
Responsible member of staff name and job title:	**Email:** **Tel:**
Date of request:	
Information types – please list all the types and categories of information to be handled, e.g. paper copy examination forms**:** • …	
Description of information handling – please summarise the processes required that deviate from the cited policy, e.g. taking College information home or using personal webmail accounts**:** • …	
Duration of information handling: **START DATE:** **END or REVIEW DATE:**	
Insert here the policy controls that you require exempting from: • …	
What alternative measures have been considered? Please also explain why they have been rejected.	
Does the information contain personal data? Y/N – please delete as appropriate. **If yes, what?** • …	
Does the information contain any high risk, special category (aka sensitive) personal data or monitoring activities? Y/N – please delete as appropriate. **If yes, what?** …	

List the information risks of the above handling – e.g. accidental loss of information, and unlawful access by 3rd parties at home. • …	
List your proposed mitigations of the above risks: • …	
INTERNAL USE ONLY BY IG TEAM OR IM&T	
Severity: LOW/MEDIUM/HIGH	
Mitigations accepted by IG Team/IM&T: Y/N – please delete as appropriate.	
Further measures recommended: **1. …** **2. …** **3. …**	
Authorisation **SIRO:**	
Waiver logged in Information Risk Register: Y/N – please delete as appropriate.	
Does the President / CEO need to be informed(Y/N):	**External/internal communication required:** **Y/N –** please delete as appropriate. **Details if applicable:**
Date waiver reviewed or closed :	