Records Management Policy (DP-Pol-089)

Document Title	Records Management Policy
Document Number	DP-Pol-089
Version	1.0
Department	Quality Assurance and Corporate Risk
Owner/Responsible for Implementation	Manager, Quality Assurance and Corporate Risk
Approving Body	Executive Board
Effective date:	June 2019
Next Review date:	June 2021
Related Documents	DP-Pol-090 – Data Protection Policy ISMS-Pol-101 – Information Security Policy ED-Pol-088 – Programme Information & Data Management Policy DP-Pol-133 – Data Breach Management Policy and Procedure DP-SOP-081 – Subject Access Procedure DP-GL-170 – RCPI Retention Schedule

1. Purpose and Aims of this Policy

The Royal College of Physicians of Ireland (RCPI) is committed to ensuring that it creates and maintains records that are full and accurate.

The purpose of this policy is to provide a clear statement of the RCPI's commitment to effective records management as part of its overall commitment to good governance, efficiency, accountability and compliance. In supporting this commitment, this policy provides the basis for good records management practice to:

- support business functions in meeting legal and professional obligations and to reflect the activities of RCPI.
- mandate the establishment of suitable structures, set out the major elements of the RCPI's records management programme and to facilitate the development and implementation of these elements.
- identify the roles and responsibilities of RCPI's staff and management regarding records management.

The aims of this policy are to ensure that:

- adequate records of business activities are being created and maintained, and that these records are authentic and reliable
- appropriate access controls are in place to safeguard confidential or sensitive records
- records are arranged effectively to facilitate efficient retrieval
- records required for legal, administrative and fiscal purposes are retained for as long as they are needed
- records no longer required are destroyed in a controlled manner according to the agreed retention policy
- vital records essential for the operations of RCPI, in the context of business continuity and disaster planning, are identified as such and protected
- adequate storage is provided for the records in a safe and secure environment
- records of archival value are appropriately identified and managed

Effective implementation of this policy will ensure that:

- business is conducted in an orderly and efficient manner
- policy formation and managerial decision-making is properly supported and documented
- management and administration are consistent in the management of corporate information
- corporate knowledge is maintained and accessible
- business continuity is assured in the event of a disaster
- legislative and regulatory requirements are met
- the rights and interests of all RCPI stakeholders are protected

- current, future and historical research are facilitated
- RCPI achievements and heritage are preserved

2. Scope of this policy

All records, regardless of format, created or received in the course of RCPI business, constitute the official records of the Royal College of Physicians of Ireland. They are the property of RCPI and subject to its control.

This policy applies to all information, regardless of format, that is created, received or maintained by or on behalf of RCPI, in the pursuance of its legal obligations or in the transaction of its business.[1]

This policy applies to all offices, units, departments and areas of work under the governance of RCPI.

This policy does not apply to non-records, working copies or duplicates that are created for temporary or convenience purposes only.

3. Roles and responsibilities

The Records Management Policy is a formal policy of RCPI, approved by the Executive Board and must be observed and implemented by all staff, contractors, consultants and other agents in accordance with the various procedures deriving from it.

The Senior Management Team is responsible for ensuring appropriate resourcing for the successful implementation of this policy and for the security and integrity of RCPI records.

Department Managers are responsible for ensuring that their staff are familiar with this policy and all associated procedures and guidelines.

The Data Protection Officer is responsible for monitoring and improving compliance with this policy.

Each manager with temporary staff, contract staff, consultants, auditors or any other non-staff visitors to RCPI under their supervision is responsible for the compliance of their activities with RCPI records.

Employees leaving RCPI or changing positions within the RCPI must leave all records available for use and accessible by their successors, in line with relevant policies and procedures developed by RCPI.

[1] Reference ISO15489

4. Distinguishing Records from Approval and Review

The ISO 15489-1:2016 defines records as "information created, received, and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business".

NB - Whether or not a document is formally declared a record, or a non-record, can become irrelevant, as all information in your possession can be subject to any legal discovery process including and Data Protection legislation and subpoena.

Non-records are items or documents of a transitory nature which are no longer required for a business purpose.

Sample List of Non-Records

- Duplicates of documents produced by other departments e.g. POs
- Externally produced documents such as publications
- Personal research / reference files
- Requests for stock information such as maps, plans or advertising material
- Rough drafts of documents
- Routine administrative documents (e.g. room bookings, arrangements for meetings)
- ~~Trivial~~ Inconsequential email messages (as opposed to emails that meet the ISO definition above)
- Printed copies or photocopies of statutes (bound or unbound)
- RCPI event advertising / flyers / brochures (once a single copy has been provided to the Keeper of Collections)

5. Security Classification of Documents

While RCPI is committed to transparency, accountability and facilitation of appropriate sharing and distribution of information, it is necessary to ensure that appropriate steps are taken to identify information which requires protection and safeguarding in order to avoid inappropriate access or sharing.

Responsibility for assigning a security classification rests with the creator of the document when the document is created. The Security Classification Guide is provided to ensure consistent approach to assigning security classifications to information.

NB - Designating an information asset as Internal or Confidential does not automatically prevent it from being released to outside parties under relevant legislative provisions.

Security Classification	Explanation
Confidential	Unauthorised release of the information would have significant negative consequences for the College, for identifiable individuals or other stakeholders. Access to the information is restricted internally and circulation outside the College is strictly limited on a need-to-know basis. Appropriate access controls are in place to ensure confidentiality is maintained.
Internal	Release of the information would have little or no negative consequences. There is general access to the information within the College amongst staff, volunteers, contractors and other stakeholders.
Public	There are no adverse consequences to the release of the information. The information is published or is made available upon request without any restrictions.

Where items are stored as part of a folder or aggregation (paper or digital), the folder should be assigned a classification level consistent with protecting the most sensitive item in that folder. For example, if most items in a folder are classified “Internal” but a small number of items are classified “Confidential”, then the entire folder should carry a “Confidential” designation and access should be controlled accordingly.

6. Annual Records Review

The Data Protection Officer must ensure that there is an annual review of the records of each department. The review will include an audit of the departmental record keeping as well as controlled archiving, off-site storage or destruction of records in accordance with the Records Retention Schedule.