

**Data Retention Policy Template**

May 2018

Royal College of Surgeons in Ireland *Coláiste Ríoga na Máinleá in Éirinn*

# 1.0 Document Version Control

|  |  |
| --- | --- |
| Document Title | RCSI GDPR Data Retention Policy Template |
| **Version** | **Status** | **Author(s)** | **Reviewed By** | **Approved By** | **Draft Date**  |
| Draft | In Review | Veronica Carty | Dónall King  |  | 20/02/2018 |
| 1.0 | In Review | Veronica Carty | Ruth Meredith |  | 26/02/2018 |
| 1.1 | Updated & Approved | Veronica Carty | Dónall KingJustin RalphJennifer Cullinane | Dónall KingJustin RalphJennifer Cullinane | 01/03/2018 |
| 1.2 | Final | Veronica Carty  | Dónall King | Dónall King | 07/03/2018 |
| 1.3 | Updated Post Deloitte Review | Dónall King | Dónall King | Dónall King | 23/05/2018 |

# 2.0 Introduction

## 2.1 Overview

The RCSI (insert RCSI area/ department) Department retains personal data, which places an obligation on individuals regarding the safeguarding of this personal data, the lawful processing of this personal data and compliance with the safe destruction of data.

The General Data Protection Regulation (GDPR), effective 25th May 2018, governs the acquisition, processing, storage and erasure of personal data.

This document is written in the context of both the current Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such personal data and the GDPR.

## 2.2 Policy Purpose

The purpose of the (insert RCSI area/ department) Data Retention Policy is to:

* Ensure that necessary records and documents of the (insert RCSI area/ department) office are adequately protected and maintained.
* Identify any and all types of personal data stored in the (insert RCSI area/ department) department, both physically and electronically.
* Identify timelines for the management and deletion/destruction of personal data.
* Define how personal data should be deleted and destroyed in a secure and confidential manner.
* Aid employees of the (insert RCSI area/ department) department in understanding their obligations in retaining manual and electronic documents.

## 2.3 Policy Scope

This policy applies to all personal data stored in physical e.g. paper and electronic records generated in the course of the department’s operation, including both original documents and reproductions and is applicable to all (insert RCSI area/ department) data controllers and processors. These individuals are responsible to implement and comply with the requirements of the Policy.

## 2.4 Data Protection Definitions

Personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, (e.g. social security number), or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity, (e.g. name and first name, date of birth).

Sensitive personal data requires a higher degree of control and security and includes data relating to an individual's: racial or ethnic origin, political opinions, physical or mental health or condition, membership of a trade union, sexual life or orientation, commission or alleged commission of any offence, religious beliefs or similar and genetic or biometric information.

Personal data should be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’)
2. Collected for specified, explicit and legitimate purposes (‘purpose limitation’)
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)
4. Accurate and, where necessary, kept up to date (‘accuracy’)
5. Kept in a form which permits identification of data subjects for no longer than is necessary (‘storage limitations’)
6. Processed in a manner that ensures appropriate security of the personal data using appropriate technical or organisational measures.” (‘integrity and confidentiality’)

# 2.5 Policy Owner

The person responsible for updating this policy in the (insert relevant RCSI department) is (insert RCSI contact name/ area/ department).

# 2.6 Policy Review Cycle

This policy is to be reviewed (insert review cycle/ period, e.g. annually) at the (insert RCSI area/ department) team management meeting.

# 2.7 Roles & Responsibilities Within the Department

The following people are responsible for data retention/ deletion of personal data in the following categories:

(insert the personal data categories & RCSI contact name/ area/ department).

**2.8 Policy Implementation Monitoring**

The implementation of data retention schedules outlined in this policy will be monitored on a (insert review cycle/ period, e.g. bi-annual/ annual basis), the Head of the Department will be informed about the progress, with the next update due in (insert review date).

# 3.0 Data Retention

## 3.1 Data Retention Schedule

The (insert RCSI area/ department) Data Retention Schedule in Appendix A details the length of time that personal data is retained by the department. The period for which data is retained, is determined by the type of record in question and the rationale for its retention.

For example, there may be a legal requirement to retain records for a certain period of time e.g. 7 years.

In other instances, there may be a regulatory requirement imposed by the relevant authority for retention of records e.g. The Medical Council.

## 3.2 Record Destruction

The Data Retention Policy is intended to focus the mind as to what personal data is held and to set out in writing the rationale for its retention. If there is no compelling reason to retain the data, then there is no GDPR right to hold onto it.

It is important that RCSI departments achieve the right balance between personal data disposal and retaining historical documentation for business intelligence purposes.

A measured approach is essential so as to ensure that personal data which is retained is done for genuine business reasons.

The overriding criterion for document retention is a clearly demonstrated rationale. It is accepted that no *“one size fits all”* in RCSI.

When the retention duration has elapsed, destruction of restricted/ sensitive documents should be carried out in the appropriate manner, as highlighted below:

* Paper Files: Must be shredded in the locked official shredder bins or must be placed in the locked confidential disposal bins.
* Electronic Data: Destruction should include the removal from all sources/ locations, i.e. data may be held in applications, SANs, tape back-up etc. Ensure the physical media on which the data was distributed is destroyed, along with the derived copies of all data files – this may require destruction or secure erasure of the storage device(s) on which the derived files are stored.

There are multiple approaches that can be taken to make files inaccessible, including physical destruction of the device(s), (e.g., CDs, DVDs, tapes, diskettes), on which the files were stored, secure erasure of storage media followed by reformatting and/ or secure deletion of individual folders and/or files.

Please refer to the IT Security Policy, this can be found on the Policies and Procedures page on the IT portal. [IT Policies and Procedures](http://staff.rcsi.ie/administration-and-support/information-technology/policies-and-procedures)

* Third Parties: In the case of an external company destroying the data, a certificate confirming the date and contents of destruction should be retained as proof of destruction of records.

If you have any further queries please do not hesitate to contact, dataprotection@rcsi.ie.

## Appendix A

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of Data** | **Examples of Personal Data** | **Purpose of Data** | **Retention Period** | **Rationale** |
|  |  |  |  |  |
|   |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |