Institute and Faculty of Actuaries

Records Retention and Disposal Policy

v1

May 2018

Authorised by: Anne Moore, Chief Operating Officer
First issued: May 2018
Last review date: May 2018
Next review date: May 2019

Update record:

Date	New version	Author	Description	Details
May 2018	v1	David Hood	Policy issued	New policy

Records Retention and Disposal Policy

1. Introduction

We must:

- implement effective records management;
- retain personal data for minimum periods of time to meet legal and regulatory obligations and for operational purposes;
- dispose of personal data when it is no longer required; and
- retain some records permanently to demonstrate our governance arrangements, evidence our decision making as a regulator or where it is in the public interest to do so.

2. Purpose

The purpose of this policy is to define our approach to retaining and disposing of information.

3. Scope

This Policy applies to all:

- employees, temporary employees, contractors, students, members, volunteers and third parties operating on behalf of the IFoA;
- facilities and information systems used to process information, whether hosted by or on behalf of the IFoA; and
- types of information, regardless of source, medium or format.

4. Policy Statements

We will

- include risks relating to retention and disposal of information on our risk registers;
- define our retention and disposal rules in a Records Retention Schedule (RRS);
- provide references for each retention rule that is based on legislation, regulation, or codes of practice;
- assign the longest retention period where there are multiple citations for retention periods; and
- review and update the RRS on an annual basis.

We:

- will dispose of or anonymise personal data as soon as is practical when the relevant retention period expires.

We will:

- ensure the level of security for disposal is related to the sensitivity of the information being disposed; and
- retain evidence of disposal to ensure we can prove how and when disposal occurred.

5. Roles and responsibilities

Role	Responsibility
Chief Executive Officer (CEO), Directors	Approval of this policy and the RRS.
Data Protection Officer (DPO)	Operational management of this policy and the RRS including oversight and audit of implementation across business areas
Head of Department(s) / Risk Owners	To direct implementation of this policy and the RRS within business areas.
Procurement / Supplier Manager(s)	Monitor suppliers' performance to ensure compliance with this policy and the RRS and report any concerns to the DPO
Suppliers / Service providers	Provide evidence of compliance with this policy and the RRS to the Procurement / Supplier Manager.
Executive staff	Be aware of this policy and the RRS and act upon instruction to affect disposal or archiving.
Volunteers and third parties processing information on behalf of the IFoA	Be aware of this policy and the RRS.

6. Policies and procedures

We will develop and implement organizational controls to ensure compliance with the policy including but not limited to embedding the policy requirements within our change processes and monitoring and logging system and user activity.

7. Compliance

We will measure compliance with these policies and procedures periodically. Failure to comply with these policies or procedures may result in:

- a risk event being documented and/or
- disciplinary action.

8. Review and approval

As defined in the roles and responsibilities, this policy and all related policies and procedures will be:

- reviewed by the DPO on an annual basis; and
- approved by the CEO whenever a material change has been made in order to comply with our Governance Manual.