**Records Disposal Policy**

**RMP009**



1. **POLICY STATEMENT**

This policy should be read in conjunction with the **sport**scotland Record Management Policy Statement which outlines its commitment to active management of the organisation’s records and associated responsibilities, and notes disposal of records as a key aspect of this.

Disposal is the process which determines the final fate of a record and can include physical destruction, transfer to another body such as the National Records of Scotland or permanent retention. All records are subject to disposal processes but not all records are destroyed (however it is estimated that less than 5% of **sport**scotland’s records will be permanently preserved).

The implications of the Data Protection Act 1998 (in particular principles 5 and 7),the General Data Protection Regulation and the Freedom of Information Scotland Act 2000 require the organisation to demonstrate consistency and transparency in the disposal of records.

This policy outlines the core principles of records disposal and is supported by a procedural note.

1. **PRINCIPLES**

The following principles will drive activities relating to the disposal of records:

* An agreed retention and destruction schedule is in place which demonstrates that the appropriate legislative and operational considerations have been taken into account.
* The retention and destruction schedule should be consulted to determine the appropriate retention period prior to disposal.
* The electronic disposal of records, aligned to the retention and destruction schedule, requires the authorisation of the document/record owner and, if applicable, the last person to have modified the document. (SharePoint contains audit trails)
* When paper records are being disposed of summary information should be noted in a disposal certificate which provides evidence that the disposal has actually been carried out. This disposal certificate to be retained by the Information Asset Manager.
* The retention of a document beyond its scheduled destruction timeline requires a clear rationale and the authorisation of two people, the document owner and the Information Asset Manager.

1. **OBJECTIVES**

The key objectives of this policy are to:

* ensure that records are managed and eventually disposed of in accordance with the **sport**scotland Records Management Policy and associated Retention and Destruction Schedule;
* ensure the disposal of time-expired records which are no longer required for legal or operational purposes and thus facilitate efficient access to information and economic use of storage spaces (physical and electronic); and
* provide methods for the appropriate/practical disposal of records.

1. **ROLES & RESPONSIBLITIES**

**sport**scotland is the only true and official owner of the records produced and/or received in the course of its business.

The various roles and responsibilities for record keeping relating to key business functions and activities are described in RMP001 – Statement of Records Management Responsibilities and individual record ownership within RMP006 – Retention and Destruction Schedule.

Heads of Service are responsible for records within their individual areas of responsibility and therefore responsible for record disposal and ensuring that final disposal is undertaken in accordance with **sport**scotland disposal policy and procedures, including authorising disposal certificates.

All destruction of confidential or protected paper records must be undertaken by a supplier approved and engaged by **sport**scotland for such a purpose. Details of current suppliers are available from the Information Asset Manager.

All disposals of ICT equipment is undertaken by **sport**scotland’s ICT Team through approved suppliers.

1. **MONITORING & REPORTING**

Compliance with this policy will be undertaken on an ongoing basis by the Information Asset Manager and incidences of non-compliance reported to the SMT through the Head of Office Support Services annually. Remedial actions will be put in place to ensure resolution.

Any breach of this policy should be reported immediately to the Information Asset Manager and ICT Manager.

Where any incidents of non-compliance lead to a significant or potential breach of information security, business continuity arrangements will be enacted as appropriate to the level of risk.

1. **REVIEW**

This policy will be reviewed annually by the Head of ICT.