**Statement of Responsibility for Records Management**

**RMP001**



The Chief Executive, as Accounting Officer, is responsible for the adequate protection of **sport**scotland assets which includes information which is collected, processed and stored within **sport**scotland. This includes the Information and Communications Systems required to support this responsibility. The Chief Executive has appointed a number of individuals to support this activity as outlined below.

**1.** **Senior Information Risk Owner**

The Senior Information Risk Owner (SIRO) is Forbes Dunlop as Chief Operating Officer, and as such is responsible for ensuring that appropriate policies and processes are in place to appropriately manage and safeguard the organisation’s information assets (including compliance with the Data Protection and Freedom of Information Acts).

The SIRO owns the information risk policy and associated risk assessment and act as an advocate for information risk at the Board and in internal discussions and provide written advice to the Chief Executive on the content of the Statement on Internal Control relating to information risk and associated systems.

**2. Data Protection Officer**

The DPO is responsible for ensuring that **sport**scotland and its staff are informed and given advice about how it can meet its obligations under the GDPR and other data protection laws. Responsibilities include monitoring compliance of the regulation in how it relates to the personal information **sport**scotland processes, reviewing internal data protection activities, providing advice on data protection impact assessments; training staff and conducting internal audits. The DPO is the first point of contact for the Information Commissioners Office and for data subject’s whose personal information is processed (employees, athletes etc.).

**3. Information Asset Owners/Heads of Service**

Heads of Service are responsible for all information processing activities within their remit therefore are the “Information Asset Owners”.

They have overall responsibility for ensuring records management principles are implemented and adopted by all staff and associated third parties relating to the business functions and activities within their service. They are also responsible for approving changes to the relevant retention and destruction schedules.

The IAO is responsible for the adequate protection of information which is collected, processed and stored within their service area including having an understanding of what information is held, what is added, what is removed, how information is moved and who has access and why.

**4. Information Technology Security Officer**

 The Information Technology Security Officer (ITSO) is the Head of ICT and Business Continuity, Mark Murphy.

The ITSO is responsible for the security of information in electronic form and for providing the infrastructure to support this objective. This is achieved through the delivery of a high-quality ICT support and development service to all users, the development and delivery of a comprehensive ICT Strategy set against the **sport**scotland corporate and business plans and the development of effective policies and procedures to maintain appropriate ICT systems, including a robust data disaster avoidance / recovery plan.

**5. Information Asset Manager**

The Information Asset Manager (IAM) is responsible for ensuring the sportscotland Records Management Plan is reviewed annually and updated to reflect current records management processes with **sport**scotland. This is a requirement under the Public Records Scotland Act (2011)

The IAM is the named contact for the National Records of Scotland who are responsible for ensuring Public Authorities have a robust records management plan in place.

The IAM will advise sportscotland staff on best practice for records management. The IAM’s role is to develop, maintain and support the delivery of the organisation’s Records Management Plan, processes and procedures and to ensure staff awareness of these.

**6. ICT Helpdesk**

 The primary role of the ICT Helpdesk is to provide an expert ICT response to any and all issues encountered through the operation of the **sport**scotland ICT equipment and systems. *The ICT Helpdesk is available from 0900 to 1700 hours Monday to Friday and an Out of Hours service is operated from 0800 to 0900 and 1700 to 2200 hours Monday to Friday, and from 0900 to 1700 hours on Saturdays, Sundays, and Bank Holidays (Excluding the festive period).* The Helpdesk can be contacted on 0141 534 6555 or on ithelpdesk@sportscotland.org.uk, and the Out of Hours service can be contacted on 07807 022 615.

 The ICT Helpdesk also has a role to play where there are breaches of any area of information security and will:

* Act as central point of contact for recording all breaches of information security, actual or suspected (this includes loss of ICT equipment or information regardless of form in which this)
* Report incident/s to the ICT Manager and agree immediate action.
* Support incident management and maintain action log.

**7. ICT Helpdesk Coordinator**

The ICT Helpdesk Coordinator is a specific role within **sport**scotland currently undertaken by Fiona Crumlish.

 The Coordinator role is to manage the Helpdesk functions and provide support, guidance and training to staff in the application of the various information governance policies and supporting operating systems.

**8. Legal Officer**

The Legal Officer is responsible for

* maintaining the Freedom of Information Policy and contributing towards the Data Protection Policies
* coordinating responses to Freedom of Information and Data Protection requests and queries with the DPO.
* providing legal advice in relation to any Freedom of Information or Data Protection requests.

**9. Web Manager**

 The Web Manager is responsible for managing and developing the web and intranet sites on behalf of **sport**scotland. The content of both these systems is managed by designated editors throughout the organisation.

.

**10. Line Managers / Contract Managers**

Ensure that staff/contractors understand their responsibilities for record keeping, are appropriately trained in managing records and implement the procedures as laid out. In addition to ensuring that record keeping procedures within their service areas comply with this policy and any related information security guidance. This includes the need to ensure team members/ partners/ contractors take immediate and appropriate steps to investigate and identify any risks to information security arising from the work situation and bring to the prompt attention of the ICT Manager and/or ICT Helpdesk any information security issue that requires attention (including risks and near misses)

Line/contract managers must inform ICT of any changes to staff/contractor’s employment status (e.g. going on Maternity leave, change of role, career break, resignation/end of contract) as soon as possible to ensure access rights are amended accordingly. The ICT New User Request form must be completed and submitted to HR within required ed timelines.

**11. All Staff/Information Asset Administrators**

All sportscotland staff have a responsibility to ensure they create, manage and dispose of records in accordance with the Records Management Policy and associated procedures and guidance and are therefore “Information Asset Administrators.

All staff are required to report any breaches or potential breaches of this policy immediately to the ICT Helpdesk and to their line manager (this includes loss of ICT equipment or information regardless of form in which this)

This reporting may, if circumstances deem appropriate, be done anonymously in writing to the ICT Manager, Head of Office Support Services or Director of Corporate Services.

**12. Third Parties**

The Records Management Policy must be adhered to by all third parties, contractors (including under contract for services arrangements) and any individual or organisation performing a function on behalf of **sport**scotland.

Third parties are required to report any breaches or potential breaches of the Records Management Policy immediately to the ICT Helpdesk or to their contract manager. This reporting may, if circumstances deem appropriate, be done anonymously in writing to the Head of ICT and Business Continuity, the Data Protection Officer or Chief Operating Officer.

**13. Audit Committee**

The Audit Committee’s role within the implementation of the Security Policy Framework isto provide independent appraisal through the application and review of internal audit activity and overview of management action plans. The Chief Executive will report on any significant breaches of information security to the Audit Committee in addition to the mitigating actions put in place to minimise any re-occurrence. This will inform the Audit Committee’s consideration of the requirement for any internal audit activity to provide additional assurance in this respect.

**14. Incident Management Team**

 In cases of significant breaches of information security, the Business Continuity Plan will be implemented, and an Incident Management Team assembled. The Team will comprise the Data Protection Officer (as IAO), the Head of ICT and Business Continuity (as ITSO), the Information Asset Manager, the Head of Communications and the Head of Service responsible for the information compromised. This Team will consider the risks to the organisation’s critical systems and services, to staff and to the organisation’s reputation and take action as appropriate. An investigation will be held into the incident and reported to the Chief Executive and through him to the Audit Committee as outlined above.