|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 2.2**  **Contents** |

**1. INTRODUCTION / EXECUTIVE SUMMARY**

**2. POLICY STATEMENT**

**3. LEGISLATION**

**3.1 Security Policy Framework & Information Risk**

**3.2 Data Protection**

**3.3 Freedom of Information**

**3.4 Other Legislation**

**4. ROLES AND RESPONSIBLITIES**

**5. UNDERPINNING PROCEDURES & GUIDELINES**

* 1. **System Security (inc Passwords)**
  2. **Information Governance**
  3. **Use of E-Mail, the Internet and Intranet**
  4. **Mobile Communication**
  5. **ICT Purchasing**

**6. TRAINING & COMMUNICATION**

**7. MONITORING & REVIEW**

**8. APPENDICES**

* 1. **Acceptable Use Document**
  2. **Service Level Agreement**
  3. **SharePoint User Guide**
  4. **Retention and Destruction Schedule**

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit**  **Section 1 : Introduction / Executive Summary** |

1. **sport**scotland, as a public body, is required to manage its information effectively and efficiently within Scottish Government guidelines and associated legislation (as detailed fully in Section 3). To support and enable this we have developed this Information and Computer User Toolkit.

2. The Toolkit is designed to provide guidelines for all employees, contractors and selected partners in respect of the use, integrity, storage and security of information – whether this held and used in hard/paper format or by electronic means through the use of computer systems (including laptops, mobile telephones, blackberries, USB keys and servers).

3. The policy statement in Section 2 describes the expectations of the Board of **sport**scotland and the remainder of the Toolkit provides detailed guidance to support this. All users are expected to familiarise themselves with the policy statement and associated requirements and to ensure their full understanding. The Acceptable Use Document and Service Level Agreement appended seek to provide both the Board and management team with a level of assurance in this respect and you are required to complete this.

4. The organisation has in place an ICT Strategy (and associated implementation plan) which provides a strategic framework within which major ICT developments are delivered. This Strategy supports the delivery of the policy statement and is available on both the **sport**scotland internet and intranet.

5. As a **sport**scotland information and computer user you are expected to take appropriate measures to protect information (paper and electronic) as outlined in Section 5 and to report any potential breaches and/or risks as outlined in Section 5.2. This action is necessary to meet both legislative requirements, such as maintaining personal information under the Data Protection Act, and to ensure the reputation of **sport**scotland is maintained. We are all too aware of recent media coverage and consequential loss of public confidence in public sector bodies following incidents such as the loss of a laptop or ability to view information from papers not protected from public view. As a risk averse organisation, we ask that all potential risks in this respect are reported as outlined in Section 5.2.

6. You are expected to develop and store information in an electronic format in line with the guidance for SharePoint, which is the organisation’s document management system of choice. A reference guide has been developed and is available electronically.

7. The retention and destruction schedule in Appendix 4 outlines the method by which information should be stored (i.e. hard copy or electronic), the location, the length of retention, any archive arrangements, the nominated owners of the information, the destruction methods employed and any relevant associated contextual policy arrangements. Adherence to this document is core to the organisation’s ability to respond to the requirements of the Freedom of Information (Scotland) Act 2002, which is referenced in more detail in Section 3, and to ensuring efficiency of managing information by holding only that which is either essential or useful to the organisation. It should be noted that information contained in e-mails should be treated the same as any other information and e-mails saved to SharePoint as appropriate.

8. To support and aid your understanding of the contents of this Toolkit, a series of mandatory induction and awareness raising sessions will take place for all users. You will be informed of the details of these and all efforts will be made to ensure that they take place at a convenient time and location to ease attendance.

9. **REDACTED**

10. This document includes some of sportscotland’s security information which has been redacted as it is exempt as per section 30(1)(c) (prejudice to effective conduct of public affairs) of the Freedom of Information (Scotland) Act 2002. Disclosure would prejudice substantially the effective conduct of public affairs. This information is not something which is of serious concern and benefit to the public and therefore the public interest is best served in withholding the information.

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit**  **Section 2 : Policy Statement** |

1. **sport**scotland (including the National Centres, HQ, Caledonia House, Stirling Institute and Area Institutes and any other **sport**scotland facilities) recognises that communication plays an essential role in the conduct of its business. To support efficient and effective communication, **sport**scotland has invested significantly in its information and communications systems and provides access to these to its employees, contractors and selected partners. **sport**scotland expects that these systems and the information contained therein will be used in a professional and appropriate manner at all times.

2. Only authorised individuals are allowed access to **sport**scotland information and information systems and the confidentiality of corporate, customer and partner information will be assured and information protected against unauthorised access. To support and enable this, appropriately protected/lockable filing systems are made available to all users to ensure the security of both electronic and hard copy documentation.

3. Electronic accounts are accessible through an individual, confidential password which must not be disclosed to any other person. This account provides access to the **sport**scotland ICT systems including e-mail and the internet for work-related purposes. Separate terminals may be made available at the discretion of management for personal usage outwith working hours.

4.How you communicate with people not only reflects on you as an individual but on **sport**scotland as an organisation. Therefore, although we will respect your personal autonomy and privacy in line with current legislation, we outline in the Information and Computer User Toolkit what we expect from you and in turn what you can expect from **sport**scotland in respect of your use of e-mail, the internet and other means of communication such as fax, fixed line or mobile phones. Compliance with current information security legislation is regarded as the minimum standard acceptable and various sections of the Toolkit seek to reflect this.

5. **sport**scotland monitors e-mail and internet usage, subject to the rule of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, for the purposes of:

* Record keeping
* Checking compliance with regulations/legislation
* Quality control
* Staff training
* Preventing and/or detecting criminal activity
* Investigating and/or detecting unauthorised, inappropriate or excessive use
* Checking for viruses or other threats to the integrity of the ICT systems

6. We all have responsibility for implementing the specific arrangements made within the Toolkit with a description of specific roles and responsibilities provided in Section 4. All breaches of this policy (and associated guidance), actual or suspected, will be investigated, issues and risks identified and mitigating actions put in place as appropriate, including enacting disciplinary procedures. Any illegal activities identified will be reported to the appropriate authorities and full co-operation given by **sport**scotland.

7. Business continuity and data disaster recovery plans for business critical systems are in place, maintained and tested on a regular basis.

8. **sport**scotland will provide appropriate training as part of the induction process and ongoing training and development programme. You are expected to be aware of the contents of the Toolkit, familiarise yourself with its provisions and carry out define responsibilities. The Toolkit will be available electronically to all users and reference hard copies held at each of the **sport**scotland offices.

9. This policy will be audited for its effectiveness and it will be reviewed as described in Section 7 of this Toolkit.

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 3 : Legislation** |

**1. SECURITY POLICY FRAMEWORK & INFORMATION RISK**

1.1 As a Non Departmental Public Body (“NDPB”), **sport**scotland falls within the requirements of the Scottish Government Security Policy Framework and Information Risk and its associated mandatory requirements.

**2. DATA PROTECTION ACT 1998 (“the Act”)**

2.1 Through your employment with **sport**scotland personal data may come into your knowledge, possession or control. In relation to such personal data (excluding personal data contained in personal communications) whether you are working at **sport**scotland’s premises or working remotely you must:

* Keep them secret and confidential and you must not disclose them to any other person unless authorised to do so by **sport**scotland. If in doubt ask your director or line manager.
* Familiarise yourself with the provisions of the Act and comply with its provisions ([www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)).
* Process personal data strictly in accordance with the Act and any other policies and procedures issued by **sport**scotland (as laid out in this Toolkit).
* Not make personal or other inappropriate remarks about clients or colleagues on manual files or computer records noting that the person who is the subject of such remarks has a right to see information **sport**scotland holds on that individual.

2.2 **sport**scotland views any breach of the Act as gross misconduct which may lead to summary dismissal under its disciplinary procedures.

2.3 If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

2.4 The **sport**scotland policy can be found at <http://ssc-sharepoint/sp/lp/Legal%20Policies%20Documentation/Forms/AllItems.aspx> .

**3. FREEDOM OF INFORMATION (SCOTLAND) ACT 2002 (“the Act”)**

3.1 The Act, subject to certain conditions and exemptions, ensures that any person who makes a request to **sport**scotland for information it holds, will be entitled to receive it. The **sport**scotland policy in this respect can be found at <http://ssc-sharepoint/sp/lp/Legal%20Policies%20Documentation/Forms/AllItems.aspx>.

3.2 A Freedom of Information request must be made in writing and could come in to any member of staff. Such requests should be directed to the Legal Officer immediately.

3.3 The response to a Freedom of Information request must be made in writing (or in the requested format) within 20 working days. The Act does not define a Freedom of Information request. However, the following are examples of the types of requests for information which should be responded to according to **sport**scotland’s procedures for Freedom of Information response:

* Unusual requests for information from members of the public (e.g. those which differ from requests received as normal working requests);
* Requests for information which require staff to investigate whether **sport**scotland actually holds the information in the first instance;
* Requests which refer to information that may be exempt under the Act;
* Requests which are specifically labelled as Freedom of Information requests; and
* Any request for information which seems unusual, and which you have concerns about answering.
  1. **sport**scotland has a duty to have in place a Publication Scheme to provide information proactively in an easily accessible form, so that people can access it without having to make an individual request. This can be accessed at:

<http://www.sportscotland.org.uk/footer_links/foi/classes_of_information/classes_of_information/>

* 1. To ensure that the organisation retains (and destroys) information in line with the Act and other overarching legislation such as the Data Protection Act 1998, it has in place a retention and destruction schedule. This is more fully referenced in Section 5.2.

**4. PUBLIC RECORDS (SCOTLAND) ACT 2011 (“the Act”)**

4.1 Complete, accurate and up to date record keeping is an important part of business continuity.

4.2 The Act promotes efficient and accountable record keeping by Scottish public authorities.

4.3 As part of the duties under the Act, **sport**scotland is obliged to prepare, implement and review a records management plan (known as a “RMP”) which sets out proper arrangements for the management of our records.

4.4 Any queries regarding the Act should be directed to the Information Asset Manager in the first instance.

5. **LEGISLATIVE REQUIREMENTS AND STAFF RESPONSIBILITY**

5.1 Efficient records management practices will assist **sport**scotland to meet its duties under the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002 and the Public Records (Scotland) Act 2011. Staff must ensure that all business records (including emails and handwritten notes) are kept in the appropriate files. Staff should not store business records in their personal paper files or on personal computer drives.

**6. OTHER LEGISLATION / STATUTORY INSTRUMENTS / EU DIRECTIVES**

6.1 Other key pieces of legislation / statutory instruments / EU directives are also relevant and must be adhered to and include but are not limited to the:

* Computer Misuse Act 1990
* Regulation of Investigatory Powers Act 2000
* Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
* Public Interest Disclosure Act 1998 (commonly known as the Whistleblowers’ Act) 1999
* Human Rights Act 1998
* Defamation Act 2013
* EqualityEquality Act 2010
* Trade Marks Act 1994
* Protection of Children Act 1999
* Obscene Publications Act 1959
* Consumer Protection (Distance Selling) Regulations 2000
* Copyright, Designs and Patents Act 1988
* Copyright, etc and Trade Marks (Offences and Enforcement) Act 2002
* Copyright and Related Rights Regulations 2003
* Copyright and Rights in Databases Regulations 1997
* Enforcement of Intellectual Property Rights 2004/48/EC
* Waste Electric and Electronic Equipment Directive (WEEE Directive) 2002/96/EC
* Criminal Justice and Public Order Act 1994
* Electronic Communications Act 2000
* Public Records (Scotland) Act 2011

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 4 : Roles and Responsibilities** |

**1. ORGANISATIONAL ARRANGEMENTS**

1.1 This Toolkit provides the detail of the arrangements in place to ensure that the organisation delivers against its statutory/ legislative information security requirements whilst supporting efficient and effective communication.

1.2 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.

**2. ROLES & RESPONSIBILITIES**

**2.1** **Senior Information Risk Owner (SIRO)**

The Director of Corporate Services, as the Senior Information Risk Owner (SIRO), is responsible for ensuring that appropriate policies and processes are in place to appropriately manage and safeguard the organisation’s information assets. The SIRO is required to own the risk policy and 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.

**2.2 Information Asset Owner (IAO)**

The Head of Office Support Services, as Information Asset Owner (IAO) for **sport**scotland, is responsible for the adequate protection of information which is collected, processed and stored within **sport**scotland. The IAO is required to understand what information is held, what is added, what is removed, how information is moved and who has access and why. Annually the IAO is required to provide a written judgement of the security and use of these assets to support the audit process.

**2.3 Information Technology Security Officer (ITSO)**

The ICT Manager, as Information Technology Security Officer, 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.

**2.4 Information Asset Manager**

The Information Asset Manager is a specific post which has been created specifically within **sport**scotland with the following key responsibilities to develop, maintain and support the delivery of the organisation’s information governance policies, processes and procedures and to ensure staff awareness of these.

**2.5 ICT Helpdesk**

2.5.1 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](mailto:ithelpdesk@sportscotland.org.uk), and the Out of Hours service can be contacted on 07807 022 615.

2.5.2 The ICT Helpdesk also has a role to play where there are breaches of any area of this toolkit and will:

* Act as central point of contact for recording all breaches of this policy, 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.

**2.6 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.

**2.7 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 Head of Office Support Services (as IAO), the ICT Manager (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.

**2.8 Legal Officer**

The Legal Officer is responsible for:-

* + maintaining the Freedom of Information and Data Protection Policiesies;
  + coordinating responses to Freedom of Information and Data Protection requests and queries; and
* providing legal advice in relation to any Freedom of Information or Data Protection requests.

If youyou have any queries about the legal implications of a Freedom of Information or Data Protection request, the Legal Officer will be able to provide assistance.

**2.9 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.

**2.10 All Staff**

2.10.1 Your responsibilities are detailed in full within each of the following sections and must be read, understood and implemented without exception. Confirmation of this understanding will be sought through electronic completion of the document attached as Appendix 1.

2.10.2 All staff are required to report any breaches or potential breaches of this policy and toolkit immediately to the ICT Helpdesk or to their line manager. 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.

**2.11 Management Responsibility**

2.11.1 Managers (including Partnership Managers) are responsible for ensuring that the requirements of this computer user toolkit are met within their individual departments/areas of responsibility.

2.11.2 You should ensure that:

* Your team members/partners/contractors are aware of their responsibilities as laid out in this toolkit.
* Your team members/partners take immediate and appropriate steps to investigate and rectify any risks to information security arising from the work situation.
* Your team members/partners/contractors 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)
* You inform ICT of any changes to staff/contractors 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.
  + 1. Requests for user accounts for new staff will only be accepted from the HR department. You must ensure HR are made aware of any hardware requirements in line with the staff member’s role and responsibilities so these can be passed to the ICT department. ICT will supply user accounts and hardware according to the following SLAs:
* New User Account – 2 Weeks
* Provision of ID and Access Card – 2 Weeks (after commencement of employment)
* Provision of Mobile Phone – 3 Weeks
* Provision of Laptop – 5 Weeks
* Provision of desk phone from existing pool of numbers – 1 Week
* Provision of new phone and line out with existing pool of numbers – 8 Weeks

**2.12 Contractors**

2.12.1 The appointment process for contractors requires that they adhere with all **sport**scotland policies and procedures whilst working for and/or on behalf of **sport**scotland. It is the responsibility of the appointing manager to ensure understanding and compliance on an individual basis. Confirmation of this understanding will be sought through electronic completion of the document attached as Appendix 1. On compliance with the requirements of this toolkit will be dealt with in line with the individual contractual arrangements, which may lead to the individual concerned being excluded from **sport**scotland premises.

2.12.2 Requests for new user accounts for Contractors must be made via the HR department and will follow the same SLAs as requests for new staff. In addition, the end date of the contractors contract (if known) must also be supplied to the ICT department.

**2.13 Partners**

* + 1. As a consequence of its role as the National Agency for Sport in Scotland, **sport**scotland works in partnership with a range of bodies and individuals. There may be circumstances where these partnership arrangements require working within **sport**scotland premises and provision of access to **sport**scotland held information. It is a requirement that all such bodies and/or individuals are identified by the relevant Head of Service/Managers and intimated to the ICT Manager/Helpdesk prior to access to information systems being given. Individual levels of access (buildings and systems) must be stipulated at this point by the relevant Partnership Manager. These levels of access will be included in an associated Service Level Agreement (based on the standard template attached as Appendix 2). Non compliance with the policy will be dealt with in line with the relevant Service Level Agreement and sanctions may lead to the individual concerned being excluded from **sport**scotland premises.

2.13.2 Requests for access or equipment for Partners will only be accepted from the Head of Pathways and will adhere to the same SLAs as requests for new staff.

**2.14 Visitors**

As a consequence of its role as the National Agency for Sport in Scotland, **sport**scotland has a number of visitors to its premises who may require access to the internet. This access is provided through Guest Networks in each of our sites. Access codes are available from the Office Services Teams/Receptions in each of the sites or from the ICT Helpdesk. *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](mailto:ithelpdesk@sportscotland.org.uk), and the Out of Hours service can be contacted on 07807 022 615.

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 5.1 ICT System Security** |

**1. GENERAL PRINCIPLES**

**REDACTED**

**2. SYSTEM SECURITY**

**REDACTED**

**3. PASSWORDS**

**REDACTED**

**4. VISITORS**

**REDACTED**

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 5.2 : Information Governance** |

**1. INTRODUCTION**

1.1 As a Non Departmental Public Body (NDPB), **sport**scotland falls within the requirements of the Scottish Government Security Policy Framework and Information Risk and other legislation as outlined in Section 3.

**2. SHAREPOINT**

* 1. SharePoint is a web-based system used for storing, sharing and managing **sport**scotland’s information. SharePoint allows all authorised users to easily access and share information across the organisation and cuts down on the amount of duplication and obsolete data. To support users in its correct application a user guide has been produced.
  2. At initial induction all users undergo a one to one training session with the Information Asset Manager. This covers all areas outlined in the User Guide attached as Appendix 3. This guide provides information on how to create documents, version control, security/permissions and how to manage documents.
  3. In addition, a series of help guides have been produced to support users in the longer-term and to ensure full use is made of this facility. On-going workshops on best practice are also available to staff as well as one to one sessions on best practice.

**3. ELECTRONIC FILE NAMING CONVENTION**

3.1 Naming records consistently, logically and in a predictable way distinguishes similar records from one another at a glance, and in doing so facilitates the storage and retrieval of **sport**scotland’s electronically held records.

3.2 All users are required to name documents using the following standard procedure:

* Text following the date should have only spaces between words (hyphens or underscores should not be used).
* Document names must be short, but meaningful.
* When including a personal name in the document name give the family name first followed by the initial.
* Order the elements in a document name in the most appropriate way to retrieve the record, e.g.:

For documents where the subject matter is the most important:

**Bloggs J Athlete Queries Letter recd 2009-12-03**

For meetings where the date is the most important:

**2009-12-03 Board Agenda**

**2009-12-03 Board Minutes**

* This procedure should apply also when entering the subject of an email. It is important when transferring Emails into livelink to rename them by taking out RE: and FWD: otherwise email will not be grouped by subject matter or date.

**4. DOCUMENT CLASSIFICATION**

4.1 In line with the requirements of the Security Policy Framework, **sport**scotland requires to classify all its documents based on an assessment of potential compromises to confidentiality, integrity or availability of information. This is standard across all public sector organisations and seeks to assist in the appropriate protection of shared information.

4.2 Whilst there are no national definitions for integrity or availability, the defined impact levels are Protect, Restricted, Confidential, Secret and Top Secret.

* 1. In **sport**scotland it is expected that all documents are annotated (in the header) as :
* NON-PROTECTED – to be used for all documents which are made publicly available or which would be if requested under Freedom of Information guidelines. This would include Board Minutes, Investment Papers, Research Papers.
* PROTECTED – to be used for documents which would be exempt from publication under the Freedom of Information Act. This would include any draft document to be published in final form within 12 weeks, Board papers where there is viewed to be prejudice to effective conduct of public affairs (e.g. security).
* CONFIDENTIAL – to be used for documents which are covered by the Data Protection Act, e.g. personnel records.

**5. VERSION CONTROL**

5.1 To assist in the appropriate management of documentation and to assure readers of its status, it is essential that an appropriate version control method is applied.

5.2 Each document is required to detail (in its Footer) the version and the date of writing/last amendment. A whole number would denote the approved version number and the number after the decimal point the draft number – in an ascending manner, e.g. 2.3 (2nd approved version and 3rd draft).

5.3 SharePoint also allows for the previous versions to be identified.

**6. RETENTION & DESTRUCTION SCHEDULE**

* 1. To ensure that **sport**scotland retains all information in line with the Freedom of Information Scotland Act, it has created a Retention and Destruction Schedule which covers all areas of the organisation. SharePoint will manage electronically the retention and destruction schedule.
  2. The retention and destruction schedule is attached as Appendix 4 and it will be seen that this covers:
* retention periods
* retention media (electronic, hard copy)
* archive arrangements
* information owners
* destruction methods
* overarching policies
  1. The Retention and Destruction Schedule aligns to the **sport**scotland file plan and the structure of the Intranet, which in turn align to the key business areas.

**7. LOSS OF INFORMATION**

**REDACTED**

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 5.3 : Use of Outlook/E-Mail, the Internet and Intranet** |

**1. INTRODUCTION**

1.1 All **sport**scotland computer users are required to ensure that their use of e-mail, internet and intranet is appropriate and follows the guidance outlined below in respect of content, copyright and good practice.

1.2 As outlined in Section 5.2, information contained in e-mails, internet and intranet must be maintained in line with the Retention and Destruction Schedule (Appendix 4), with only Important e-mails being saved to Sharepoint as appropriate. All internal and external e-mails are archived automatically with our filtering partner, Mimecast, in line with our retention policies, and emails can be retrieved from this archive if required.

1.3 The internet, intranet and e-mail should not be used for any purpose which would be subject to disciplinary or legal action in any other context. If you are in doubt about a course of action take advice from your line manager, ICT Manager or Information Asset Manager. ppropriate. All staff internet access is logged and filtered using Bloxx proxy filters. Access is monitored in line with **sport**scotland policies and current legislation.

**2. USING E-MAIL**

**REDACTED**

**3. CALENDARS**

**REDACTED**

**4. USING THE INTERNET AND INTRANET**

**REDACTED**

**5. PERSONAL USE**

**REDACTED**

**6. EXAMPLES OF UNACCEPTABLE BEHAVIOUR**

**REDACTED**

**7. Compliance**

7.1 Employees who do not support this policy may be subject to disciplinary action.

7.2 Compliance with this policy will be monitored by the Senior Management Team.

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 5.4 : Mobile Communication (Laptops, Blackberries, Mobile Phones, USB Keys)** |

**1. INTRODUCTION**

**REDACTED**

**2. MOBILE DEVICE**

**REDACTED**

**3. WORKING REMOTELY**

**REDACTED**

**4. LOSS OF MOBILE COMMUNICATION DEVICE**

**REDACTED**

**5. ICT ASSET REGISTER**

**REDACTED**

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 5.5 : ICT Purchasing** |

**1. INTRODUCTION**

**REDACTED**

**2. ICT PURCHASING & MANAGEMENT**

**REDACTED**

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 6 : Training & Communication** |

**1. INTRODUCTION**

1.1 In order to ensure all computer users are aware of the details of the Toolkit and their individual roles and responsibilities in its delivery, a comprehensive communication plan requires to be developed and implemented.

**2. COMMUNICATION**

2.1 In order to ensure a consistent approach and in recognition of various elements of the Toolkit where economies of scale can be achieved, it is intended that these be drawn together in an organisational communication plan (which details where site specific communications is required).

2.3 The Communication Plan will align to the Training Plan and include:

* the provision of access to hard and electronic copies of the Toolkit
* version control methods (including updates to the Toolkit and associated requirements)
* ongoing reminders/refreshers

**3. TRAINING**

* 1. **Initial Induction** 
     1. All users have a one to one session during their first few days with the ICT Helpdesk Facilitator and the Information Asset Manager. This session provides an introduction and overview to the requirements of this Toolkit.
     2. In addition, all users are provided with access to this Toolkit and asked to ensure full understanding, raising queries with the ICT team or line manager as appropriate. Assurance is sought in this respect through the return of Appendix 1 or 2 as appropriate.
  2. **Workshops** 
     1. A series of information and awareness raising workshops are organised and run by the ICT Manager and Information Asset Manager. These seek to ensure that all users are aware of their responsibilities in discharging the requirements of this Toolkit and have the opportunity to raise any queries following some experience of its application.

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 7 : Monitoring & Review** |

**1. INTRODUCTION**

**REDACTED**

**2. SURVEILLANCE & MONITORING**

**REDACTED**

.

**3. REVIEW**

**REDACTED**

|  |
| --- |
| **sport**scotland  **Information and Computer User Toolkit – Version 1**  **Section 8 : Appendices** |

Appendix 1 : **REDACTED**

Appendix 2 : **REDACTED**

Appendix 3 : **REDACTED**

Appendix 4 : **REDACTED**