National Library of Scotland
Leabharlann Nàiseanta na h-Alba

Information Security Policy

Last revised 23 February 2021

Contents

1. Definitions

For the purposes of this policy, the following terms have the corresponding definitions.

Business Owner	One of two owners of a particular Information System, along with the System Owner.
Collection Item	An item, whether meeting the definition of a record (see 'Record') or otherwise, that is held by the Library as part of its collections in accordance with sections 2-6 of the National Library of Scotland Act 2012 or similar regulations. A collection item is not a business record. This definition comes from the Records Management Policy.
Critical Information System	An Information System that is prioritised as 'critical' on the IT Systems Recovery List as amended from time to time.
Data Integrity	The accuracy and completeness of data.
Information	Any Records, irrespective of format, that is created, stored or processed by the Library, excluding Collection Items.
Information Security Incident	An event, whether suspected or proven, deliberate or inadvertent that threatens the integrity, availability or confidentiality of an Information System.
Information System	A system for the management, processing, storage, and manipulation of information, including, for example, databases, networks, servers, and software packages.
IT Asset	A computing or telecommunications device that can be used to store or process information or that otherwise supports or forms part of a computing or telecommunications infrastructure, including, for example, desktop computers. Mobile Computing Devices are a type of IT Asset.
System Owner	One of two owners of a particular Information System,

	along with the Business Owner.
Mobile Computing Device	A portable computing or telecommunications device which can be used to store or process information, including, for example, laptops, smartphones, and tablets. Portable Storage Devices are a type of Mobile Computing Device.
Personally Owned Device	A Mobile Computing Device that is not the property of the Library.
Portable Storage Device	A type of Mobile Computing Device that stores information but does not process information, including, for example, USB sticks, external or removable disc drives, and flash memory cards.
Record	Anything in which information is recorded in any form (Public Records (Scotland) Act 2011 s.13(1)). This definition comes from the Records Management Policy.
Reportable Incident	A particular Information Security Incident that is worthy of being reported, as set out in this policy.
Secure Area	A physical space on the Library's Estate to which routine access is not normally permitted to the public or most staff, and including, for example, server rooms, backup storage spaces, and archive spaces.
Senior Responsible Manager	A senior officer of the Library, normally a member of the Library Leadership Team, with responsibilities under the Business Classification and Retention Scheme for managing, or delegating the management of, particular classes of records, including their disposal. This definition comes from the Records Management Policy.
Sensitive Information	Information that contains: Personal data of identifiable living individuals (as defined by data protection legislation); Information that is exempt from disclosure under the Freedom of Information (Scotland) Act 2002 or related legislation; and/or Any information classified 'OFFICIAL-SENSITIVE' or higher in accordance with the Records Management Policy.

System Administrator	An account holder with elevated access, such as the Human Resources administrations manager and the finance systems administrations.
VPN	A Virtual Private Network connection, allowing remote devices to connect securely to the Library's on-site network in order to access local systems.

2. Policy Ownership & Responsibilities

Information Systems and the Information stored in them are strategic assets vital to the business performance of National Library of Scotland. These assets must be protected in respect of their tangible value, legal and regulatory requirements, and their critical role in the Library's ability to conduct its mission. Information and Information Systems belong to the Library as an organisation rather than individuals or groups of individuals.

The Library should maintain an information management environment that:

- protects Information and Information Systems;
- manages Information according to legislation, standards, and appropriate guidelines;
- protects the personal data and privacy of individuals;
- reinforces the reputation of the Library as an institution deserving of public trust; and
- assigns responsibilities to relevant staff, managers, contractors, partners and vendors.

2.1 Scope

This policy applies to:

- the Library's Information;
- the Library's Information Systems;
- the Library's IT Assets; and
- Personally Owned Devices when used for business functions.

2.2 Principles

The following principles guide the development and implementation of the Library's information policies and practices:

1. Information will be protected in line with relevant policies and legislation.
2. Information will be made available to those who have a legitimate right of access in accordance with the Records Management Policy.
3. Information will be classified in accordance with the Records Management Policy.
4. Data Integrity of Information will be maintained.

5. It is the responsibility of all individuals who have been granted access to Information to handle it appropriately in accordance with its classification.
6. Information and Information Systems will be protected against unauthorised access, change or control.
7. Compliance with this policy will be enforced.

2.3 Review

This policy will be reviewed every two years by the Associate Director of Digital or their deputy, for approval by the Library Leadership Team.

2.4 Responsibilities

The National Librarian and Chief Executive is responsible for information security. On a day-to-day basis this is delegated to the Associate Director of Digital.

3. Access Controls

Access to electronically-processed Information is granted in accordance with the IT Access Control Procedure.

In accordance with the Records Management Policy, access to and use of:

- electronically-processed Sensitive Information should be restricted through the IT Access Control Procedure to users with a verifiable business, statutory, or compliance need for or right of access;
- other Information should, by default, be available to all users unless there is a verifiable business, statutory, or compliance need to limit access, in which case access should be limited only so far as required.

The Business Owner is responsible for ensuring configuration ofuser access to electronically-processed Information and to Information Systems in accordance with this policy, the Records Management Policy, and the IT Access and Control Procedure.

3.1 Use of IT Systems and Networks

The use of the Library's Information Systems is governed by the Acceptable Use of ICT Equipment Policy which all potential users must agree to follow prior to using or gaining access to any Information System.

System Administrator-level access to the Library's Information Systems or IT Assets must be restricted to staff with a verifiable business, statutory, or compliance need. Prior to gaining System Administrator-level access staff must agree to follow the IT Charter.

The Library will protect on-site Information Systems by ensuring they are protected behind the perimeter firewall, through the use of VPN clients on Library-owned Mobile devices. The VPN client will not be installed on Personally Owned Devices.

3.2 Secure Areas

Physical access to Secure Areas is restricted to persons with a verifiable business, statutory, or compliance need.

Physical access controls must be in place to inhibit unauthorised access to Secure Areas.

Associate Directors are responsible for permitting access to Secure Areas within their areas of responsibility.

Unless pre-authorised as part of normal daily tasks, any person accessing a Secure Area must be accompanied by a member of staff who routinely works in that area or has a detailed understanding of the function, layout, etc. of that area, or by a relevant Associate Director.

Prior to gaining access Information Systems or IT Assets in Secure Areas, staff must agree to follow the IT Charter.

3.3 Mobile Devices

The Library may provide Mobile Computing Devices to staff as required to meet business need. Mobile Computing Devices remain the property of the Library, must be kept secure at all times, and should not be used for other purposes.

Mobile Computing Devices must be encrypted.

Use of the Library's Mobile Computing Devices is governed by the Acceptable Use of ICT Equipment Policy and the Mobile Device Security Framework, which must be complied with at all times. It is the responsibility of the staff member to report the loss of a Mobile Device in accordance with section 10.1.

3.3.1 Personally Owned Devices

The Library does not require staff to use Personally Owned Devices for business purposes. However, it is recognised that this is often convenient and such use is permitted subject to the requirements of this policy.

Use of Personally Owned Devices is governed by the Acceptable Use of ICT Equipment Policy and the Mobile Device Security Framework, which must be complied with at all times if and when devices are used for business purposes or for the storage or processing of the Library's Information.

Users must at all times give due consideration to the risks of using Personally Owned Devices and refrain from using Personally Owned Devices for business purposes if in doubt as to the safety, security, or otherwise of the Library's Information or the device in question.

4. Cyber Security

In accordance with the Scottish Government's requirement that all Scottish public bodies achieve best practice in cyber resilience, the Library will achieve appropriate accreditation to provide assurance that these standards are being met.

Access into the Library's Information Systems, network, computing devices, Mobile Computing Devices, and Personally Owned Devices (if used for business functions) must be predicated on the use of passwords or similar personal security controls.

The Library maintains and enforces a Password Policy to support cyber security. The Digital Department is responsible for preparing, maintaining, enforcing, and keeping up to date the Password Policy. The Password Policy must be enforced on Information Systems and in such a manner that users cannot circumvent the requirements of the Password Policy (e.g. through the Active Directory).

The Library should maintain and keep up to date suitable password guidelines and make this guidance known to staff. This may be achieved through reference to existing guidelines.

5. Sensitive Information Transfer

Sensitive Information may only be transferred from the Library's Information Systems for a valid and verifiable business, statutory, or compliance need or right and otherwise may not be transferred outside of the Library.

Information containing personal data of identifiable living individuals must be processed in accordance with the Data Protection Policy, including in respect of the transfer of personal data to territories outside of the UK.

When transferring Sensitive Information outside of the Library's Information Systems:

- secure networks must be used, where available;
- Information sent by non-secure networks must be encrypted;
- Information on Portable Storage Devices must be encrypted and the device password-protected in accordance with the Library's password guidance; and
- any Information transferred other than over a network (including Information sent on a Mobile Computing Device and non- electronically-processed data sent in analogue format) must be sent by recorded delivery, with a qualified courier, or delivered in-person.

Staff are responsible for Sensitive Information that they transfer outside of the Library. Staff may not transfer outside of the Library any Sensitive Information that they are not responsible for or have not been authorised to transfer.

Prior to transferring Sensitive Information outside of the Library staff must obtain permission or guidance from the relevant Senior Responsible Manager, in accordance with the Business Classification and Retention Scheme.

6. IT Asset Management

The Digital Department must maintain and keep up to date an IT Asset Register that details a description and location of IT Assets.

IT assets (other than Mobile Computing Devices) may only be moved with the consent of the IT Helpdesk. Staff intending to move an IT Asset should contact the IT Helpdesk to request a move.

IT Assets may be repurposed for uses or for users other than those for which the asset was initially acquired or configured. All IT Assets shall be subject to a reconfiguration process by the Digital Department prior to being repurposed. This process must include erasure of Sensitive Information stored on the equipment and retraction of permissions as relevant for the intended new purpose.

Surplus or redundant IT Assets must be disposed of in a secure, economic and environmentally friendly manner in accordance with the requirements of the Waste Electrical and Electronic Equipment Directive that ensures that none of the Library's Information or access permissions are preserved on the IT Asset. All Sensitive Information and licensed software must be removed from IT Assets before or during disposal, either by the Library or by an appropriately certified third party subject to a relevant contractual obligation.

Information assets are managed in accordance with the Records Management Policy.

6.1 Ownership

All Information Systems have two nominated owners, who must be named post holders:

- Business Owner
- System OwnerSystem Owner

The Business Owner is responsible for ensuring that the Information System meets relevant business needs and adds value to the Library's activities.

The System Owner is responsible for the technical administration of the Information System and for ensuring that the information system is:

- operating effectively;
- subject to business continuity planning;
- properly protected against theft or misuse;
- properly maintained under an approved maintenance or support arrangement;
- properly licensed;
- only accessed by the person(s) properly authorised by the Business Owner and; and
- properly disposed of in accordance with this policy.

The System Owner is responsible for seeking support from the Digital Department as required in order to meet their responsibilities.

7. System Management

7.1 Audit Logging

Operating system level audit logging must be maintained for all Information Systems.

Application level audit logging must be maintained for all Critical Information Systems.

Audit logging capabilities must, as a minimum, independently, selectively and in real time log:

- the actions of any user currently logged on and automatic lockout of that user if necessary; and
- the activities at a specified terminal, port or network address and automatic lockout of that input device if necessary.

Audit logs must be sufficient in detail to facilitate reconstruction of events.

To enable audit logging, all Information Systems must:

- provide adequate information for establishing audit trails relating to Information Security Incidents (as part of forensics analysis) and user activity;
- support System Administrator-selectable alerts for specified security-related events;
- record the username accountable for all activities;
- maintain the confidentiality of authenticators (e.g. passwords) by excluding them from being recorded;
- protect the audit log and its control mechanisms from unauthorised modification or destruction and prevent unauthorised deletion or disabling of the function;
- generate real-time alarms of operational problems (e.g. running out of storage space) and audit log malfunctions;
- provide individuals authorised by the Associate Director of Digital with access to enable retrieval, printing and archiving (e.g. copying to long-term storage devices) of audit log contents;
- provide System Administrators with audit analysis tools to selectively retrieve records from the audit log to produce reports, establish audit trails and perform other related functions;
- log security events including, but not limited to:
    - all sessions established;
    - invalid or unauthorized authentication attempts to access Information Systems;
    - System Administrator actions;

    - creation of and changes to user and Information System security accounts, profiles, Access Control Lists (ACLs), privileges and attributes;
    - use of privileged System Administrator accounts;
    - creation, storage and revocation of encryption keys;
    - shutdowns, restarts and backups;
    - installation and updates of software; and
    - changes to logs; and
- record event information including, but not limited to:
    - date and time of events;
    - username and MAC or IP address of event initiators;
    - event type;
    - success or failure of the event, if applicable;
    - identification of Information Systems accessed;
    - source host name and IP address generating the log event; and
    - destination host name and IP address generating the log event.

7.2 Changes to the Production Environment

All changes to the production environment, as defined under the IS Change and Release Management process, must only be performed in accordance with the IS Change and Release Management process.

7.3 Protection against Viruses and Malicious Code

All Information Systems must be protected against the introduction of viruses and other types of malicious code. All Information Systems, Mobile Computing Devices, and Personally Owned Devices (if used for business purposes) must be kept up to date through operating system and application updates and patches.

All Information Systems must have active virus protection software installed, enabled, and up to date at all times.

The Digital Department is responsible for completing routine and reactive updates to virus protection software and signature files.

Users of Mobile Computing Devices are responsible for supplying devices to the Digital Department, or connecting devices to the Library's network, when requested in order to enable routine and reactive updates to virus protection software and signature files.

7.4 Data Integrity

The Library must take appropriate steps to maintain Data Integrity in accordance with the Records Management Policy.

Information Systems must, as a minimum, have the capability to ensure that Information is not modified, altered or deleted without authorisation either in storage or in transit.

8. Business Continuity Planning

The Library must perform secure backups of all Information Systems to support business continuity planning.

In respect of any Information System, the Business Owner must agree an appropriate backup type and frequency with the System Owner. All essential components must be backed up on a schedule that is sufficient to meet relevant Recovery Point Objective(s) (RPO) and Recovery Time Objective(s) (RTO).

Information Systems must have the capability to check the integrity of data read from backup files when performing restore functions.

Backups must be managed in accordance with the Records Management Policy.

A Backup Media Inventory and supporting materials must be maintained and kept up to date by the Digital Department.

Backup media and corresponding data should be tested as part of ongoing disaster recovery testing.

9. Incident Management

Information Security Incidents are events, whether suspected or proven, deliberate or inadvertent that threaten the integrity, availability or confidentiality of Information Systems.

9.1 Reportable Incidents

The following Information Security Incidents are examples of Reportable Incidents. Any member of staff who observes or becomes aware of a real or suspected Reportable Incident must report it without undue delay to the IT Helpdesk, or to the relevant Business or System Owner.

- physical loss, theft or unauthorised destruction of Information Systems; e.g. missing or damaged hardware, software or electronic media;
- unauthorised disclosure, modification, misuse or inappropriate disposal of Information or IT Assets;
- internal or external attempts to access Information or the facility where it resides and detection of unauthorised persons in Secure Areas;
- unauthorised activity or transmission using Information Systems;
- internal or external intrusions or interference with networks (e.g. denial-of-service attacks, unauthorised activity on restricted systems, unauthorised modification or deletion of files, or unauthorised attempts to control Information Systems);
- sudden unavailability of files or data that are normally accessible;
- unexpected processes, such as e-mail transmissions, that start without user input;

- files modified without authorisation;
- files appearing, disappearing or undergoing significant and unexpected changes in size;
- systems displaying strange messages or mislabelled files and directories;
- security violation, suspicious actions or suspicion or occurrence of embezzlement or other fraudulent activities;
- prohibited mass electronic mailings;
- illegal activities; or
- violation of information security policies and procedures.

9.2 Responsibilities and Procedures

The Digital Department is responsible for recording and investigating Information Security Incidents.

All suspected Information Security Incidents that are reported must be recorded by the Digital Department. All suspected Information Security Incidents that may be Reportable Incidents must be investigated without undue delay by the Digital Department and, if appropriate, the security manager. All suspected Information Security Incidents that may involve the loss, theft, destruction, alteration, or other processing of personal data must be reported to the Data Protection Officer without undue delay.

During an investigation, the Digital Department should consider whether the user rights of any individual or group should be temporarily suspended. The Head of Digital or the Head of Security may authorise the temporary suspension of relevant user rights.

A log may be kept of the response to an incident, including details of any user suspension as relevant. Logs should be retained in accordance with the Records Management Policy.

10. Awareness and Training

All staff who use Information, Information Systems, or IT Assets in the course of their work for the Library should have an awareness of this policy and of related policies and procedures, as well as sufficient training, guidance, and support to undertake their responsibilities under this policy.

The Library provides training and induction in the substance of this policy.

Managers are responsible for making staff aware of this policy when published or revised or when an individual starts a new role. Managers are responsible for providing support in understanding the requirements of this policy and seeking support from the Digital department if required.

The Digital department should provide ongoing training and guidance, on a regular basis, on aspects of this policy. This should be made available to all staff. In particular, written guidance should be available, training and refresher sessions should be provided at appropriate intervals, and, where relevant, staff should be given opportunities for further training and support (for example, in relation to undertaking tasks with specific information management, information security, or systems security aspects).

11. Breaches of policy

All suspected breaches of this policy must be investigated in accordance with the process outlined in the Acceptable Use of ICT Equipment Policy.

Breach of this policy may lead to disciplinary action being taken against a member of staff in accordance with the Discipline Policy.

12. Related policies and documents

See also the Library's **Acceptable Use of ICT Equipment Policy**, **Business Classification and Retention Scheme**, **Collections Security Policy**, **Data Protection Policy**, **Discipline Policy**, **IS Change and Release Management process**, **IT Access Control Procedure**, **IT Charter**, **Mobile Device Security Framework**, **Password Policy**, **Password guidance**, and **Records Management Policy.**