Information Security Policy

V1.8

27 July 2026

Document Title	Information Security Policy		
Issue Status	V1.8	**Issue Date**	01/07/2020
Author	Daniel Glennie	**Title**	Security Manager
Tel:		**E-Mail**	Daniel.glennie@improvementservice.org.uk
Security Classification	OFFICIAL	**Retention Period**	Per policy
Review Period	Annual	**Last Reviewed**	**27/07/2026**

Version No	Date	Summary of changes
0.1 DRAFT	11/08/2019	Initial release for comment
0.2 DRAFT	28/09/2019	Revised after initial release
0..9 DRAFT	01/11/2019	Revised to align with ISO27001
1.1. DRAFT	03/06/2020	Added teleworking section
1.2	01/07/2020	Added mobile device section; submit to ISMS Board
1.3	01/07/2021	Annual Review – minor edits to reflect staff changes
1.4	01/07/2022	Annual Review – minor edits to reflect staff changes
1.5	01/07/2023	Annual Review – no changes
1.6	01/07/2024	Annual Review – no changes
1.7	12/08/2025	Annual Review – minor edits in scope to add cloud data
1.8	27/07/2026	Annual Review – no changes

Review

Name	Organisation
Daniel Glennie	Improvement Service
ISMS Board	Improvement Service

Authorisation

Document Approvals

Document Authorisation	Title/Organisation	Signature	Date
ISMS Board			01/07/2020
ISMS Board			01/07/2022
ISMS Board			01/07/2023

Introduction

Information is an asset that the Improvement Service has a duty and responsibility to protect. The availability of complete and accurate information is essential for the organisation to function in an efficient manner and provide products and services to customers and partners.

The Improvement Service holds and processes confidential and personal information on private individuals, employees, partners and suppliers, along with information relating to its own operations.

This policy's goal is to protect the Improvement Service's information assets from external and internal threats, whether deliberate or accidental.

Aim

This policy aims to:

- enable secure information sharing
- encourage consistent and professional use of information
- ensure that everyone is clear about their roles in using and protecting information
- protect the organisation from legal liability and the inappropriate use of information

The Information Security Policy is a high-level document that adopts a number of controls to protect information. These controls are delivered by people, policies, processes and technologies and supported by training and tools.

Scope

This Information Security Policy outlines the framework for management of Information Security within the Improvement Service.

Along with its supporting policies, guidelines and procedures, it applies to all staff and employees of the Improvement Service and to contractual third parties and agents who have access to the Improvement Service's information systems or information.

The Information Security Policy applies to all forms of information including:

- speech, spoken face to face, or communicated by phone or radio
- hard copy data printed or written on paper
- information stored in manual filing systems
- communications sent by post / courier, fax, electronic mail
- data stored on and processed by servers, PCs, laptops, mobile phones
- data stored on and processed by cloud-hosted infrastructure like AWS and OneDrive
- data stored on any type of removable media, CDs, DVDs, tape, USB memory sticks, digital cameras

Terms and Definitions

For the purpose of this document the following terms and definitions apply.

Term	Definition
Asset	Anything that has value to the organisation
Control	Means of managing risk, including policies, procedures, guidelines, practices
Guideline	A description that clarifies what should be done and how

Information Security	Preservation of confidentiality, integrity and availability of information
Incident	An event that affects the confidentiality, integrity or availability of information
Policy	Overall intention and direction as formally expressed by management
Risk	Combination of the probability of an event and its consequence
Third Party	Person or body that is recognised as being independent
Threat	Potential cause of an unwanted incident, which may result in harm to a system
Vulnerability	Weakness of an asset that can be exploited by one or more threats

Table 1 – Terms and Definitions

Structure of this Policy

This policy is based upon ISO 27001:2022 and is structured to include the main security category areas within the standard.

Risks

Data and information which is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

Data and information may be put at risk by poor education and training, misuse and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, noncompliance with standards and legislation as well as possible judgements being made against the Improvement Service.

The Improvement Service will undertake risk assessments to identify, quantify and prioritise risks. Controls will be selected and implemented to mitigate the risks identified.

Risk assessments will be undertaken using a systematic approach to identify and estimate the magnitude of the risks.

Information Security Policies

Information Security Policy Document

This Information Security policy is approved by the IS Board and Senior Management Team and is communicated to all staff and employees of the organisation, contractual third parties and agents of the organisation.

Review

The security requirements for the organisation will be reviewed at least annually by the Security Manager, approved by the IS Board. Formal requests for changes will be raised for incorporation into the Information Security Policy, processes and procedures.

Organisation of Information Security

Information Security Responsibilities

The IS Board has approved this policy.

The Security Manager is the designated owner of the Information Security Policy and is responsible for the maintenance and review of the Information Security Policy, processes and procedures.

The Senior Leadership Team is responsible for ensuring that all staff and employees, contractual third parties and agents of the organisation are made aware of and comply with the Information Security Policy, processes and procedures.

The Improvement Service's auditors will review the adequacy of the controls that are implemented to protect the organisation's information and recommend improvements where deficiencies are found.

All staff and employees, contractual third parties and agents of the Improvement Service accessing the organisation's information are required to adhere to the Information Security Policy, processes and procedures.

Information Security Coordination

The security of information will be managed within an approved framework through assigning roles and co-ordinating the implementation of this security policy across the organisation and in its dealings with third parties.

Specialist external advice will be drawn upon where necessary to maintain the Information Security Policy, processes and procedures and to address new and emerging threats and standards.

Human Resources Security

Security policies will be communicated to all employees, contractors and third parties to ensure that they understand their responsibilities.

Security awareness, education and training will be provided for all employees.

Security responsibilities will be included in job descriptions and in terms and conditions of employment.

Security responsibilities will be reviewed periodically and on termination or change of employment responsibilities.

Verification checks will be carried out on all new employees, contractors and third parties.

Failure to comply with the Information Security Policy, processes and procedures will lead to disciplinary or remedial action.

Further guidance on Human Resources Security can be found here.

Asset Management

All assets (data, information, software, computer and communications equipment, service utilities and people) will be accounted for and have an owner.

Asset owners will be responsible for the maintenance and protection of those assets.

All assets will be appropriately protected.

Information will be classified and protected accordingly.

'Information assets are designed primarily for business use. The use of assets for personal activities is permitted subject to the Acceptable Use Guidance note.'

All assets will be returned on termination of employment or at the request of the Improvement Service.

Assets that are no longer required or that have reached end of life will be disposed of in line with secure disposal or recycling guidelines.

Further guidance on Asset Management can be found here.

Access Control

Access to all information will be controlled.

Access to information and information systems will be driven by business requirements. Access will be granted, or arrangements made for employees, partners and suppliers according to their role, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be implemented for access to all information systems and services.

User rights and privileges will be monitored and reviewed regularly.

All users must keep their passwords confidential and unique user identities must not be shared.

Passwords must be changed whenever there is an indication of possible system compromise.

When a user account is no longer required, e.g. through staff resignation or a change in duties, the account must be disabled immediately.

Unused accounts will be monitored and appropriate action taken in line with the procedures for disabling and deleting accounts.

Removal of accounts must also include the removal of any associated access rights.

Further guidance on Access Control can be found here.

Remote and Mobile Working

As an agile business, the Improvement Service is constructed to support a flexible working regime that includes staff working remotely and from home. More information on flexible working can be found in the Flexible Working Policy in the staff handbook.

To support remote and mobile working, the Improvement Service recognises the importance that mobile devices, such as smartphones and tablet computers, have in helping to achieve business objectives.

However, mobile devices also represent a significant risk to data security. If the appropriate security measures are not applied, unauthorised access to key business data and infrastructure may be possible.

Remote Working

This section applies specifically to all workers who:

- spend a large proportion of their time working from home; and/or
- travel and therefore use hotels, customer premises etc.

Staff working remotely are expected to take suitable precautions to ensure that the same principles of information security and governance that apply in the office are extended to the remote or home environment.

The following policy statements apply to all home and remote workers:

- All remote working must be undertaken safely from an information security perspective
- Information security risks related to each specific remote working scheme must be identified, assessed and managed
- All remote workers must follow the procedures and guidance for home and mobile working found on the Information Security portal

Mobile Devices

The following statements apply to all mobile devices connecting to Improvement Service assets.

- Where possible, devices supplied by the Improvement Service should be used to connect to Improvement Service data, networks and services
- The use of personal devices to connect to Internet-based services such as Office 365 is permitted but must follow the guidelines for mobile and remote working. This guidance can be found on the Information Security portal
- The use of such devices will be monitored and access refused to those that do not meet approved security requirements
- Users must not try to connect personal devices to the internal wired network in the IHub. This network is managed by West Lothian Council and only approved devices are allowed to connect. These devices will be subject to compliance rules such as encryption, password, key lock, etc. and enforced by West Lothian Council IT department using centralised control software
- Users must not try to connect personal devices to the West Lothian Council network remotely (from home, customer premises etc.). Only approved devices supplied by the Improvement Service can be used in this situation
- All devices supplied must be returned to the Improvement Service when they are no longer required or prior to the recipient leaving the Improvement Service.

Further guidance on Remote and Mobile Working can be found here.

Cryptography

Digital personal data that cannot be sufficiently secured by physical controls must be encrypted, both at rest and in transit.

Where data being handled is subject to an agreement with an external organisation specifying the use of encryption, the agreed handling procedures, encryption technologies and standards must be used. A separate Data Sharing Agreement and Information Exchange Protocol may be required.

Where data is to be encrypted and no overriding requirements (e.g. from an external body) apply, the recommended minimum encryption standards (or better) must be applied.

Encryption keys must be managed in a way that prevents access by an unauthorised person but facilitates access by the Improvement Service when required (e.g. in an emergency or an investigation).

Further guidance on Cryptography can be found here.

Physical and Environmental Security

Critical or sensitive information processing facilities will be housed in secure areas.

Secure areas will be protected by defined security perimeters with appropriate security barriers and entry controls.

Critical and sensitive information will be physically protected from unauthorised access, damage and interference.

Sufficient protection against external and environmental threats must be implemented to ensure the ongoing operation of the Improvement Service and its business.

All users will adhere to a clear screen and clear desk policy. Workstations will be configured to lock out after a period of inactivity.

All users must ensure that they lock their screens whenever they leave their desks to reduce the risk of unauthorised access.

All users must ensure that their desks are kept clear of any information or removable storage media in order to reduce the risk of unauthorised access.

Visitors must, at all times, openly display visitor badges obtained from reception. A record must be kept of all visitor access. The record must contain:

- the identity of the individual
- the times of entry and departure

Visitors must be escorted within the facilities at all times.

It is the responsibility of every individual to challenge any person not displaying a valid security pass or any unescorted visitor and to report any matter which could undermine the physical security of the Improvement Service and its business.

Further guidance on Physical and Environmental Security can be found here.

Operations and Communications Security

The Improvement Service will operate its information processing facilities securely.

Improvement Service assets will be protected against viruses and malware.

Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities will be established.

Information will be backed up in relation to its business criticality and backup and recovery processes will be documented and tested regularly.

Log information will be collected and monitored to help identify issues relating to confidentiality, integrity and availability of information.

Access to logs will be protected to prevent tampering.

Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

The capacity demands of the Improvement Service will be monitored and future projections made to ensure that there is no detriment to service availability.

Further guidance on Operations and Communications Security can be found here.

Systems Acquisition, Development and Maintenance

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to mitigate any risks identified will be implemented where appropriate.

Only approved software will be installed and used within the Improvement Service and will be subject to change management processes.

Further guidance on Systems Acquisition, Development and Maintenance can be found here.

Supplier Relationships

The Improvement Service has supplier relationships that vary in terms of value and importance, size and scale, where a one-size policy does not fit all. The Improvement Service will take a risk-based approach to supplier engagement that considers the type of supplier, the contract risk and importance, along with the projected financial spend to arrive at an appropriate risk-based agreement for the organisation.

The Improvement Service will prefer to work with suppliers that already meet the majority of its Information Security needs for the services that they provide and have a good track record of addressing information security concerns responsibly.

The Improvement Service prefers to select leading and well-trusted services that are known for their robustness, reliability and security and wherever possible look to suppliers that have already achieved appropriate security accreditation, preferably ISO 27001 or its equivalent.

The IS Board, or nominated representative, may make decisions on risk acceptance where a provider does not meet those high levels of security or is unable/unwilling to demonstrate it (e.g. because the Improvement Service is a small company) but the Improvement Service still wishes to adopt their service(s).

For critical or strategic service suppliers, the Improvement Service will ensure that information security is included as part of the commercial agreement.

For other suppliers, the Improvement Service will assess that the service and supplier are credible and that information security as well as quality and performance are fit for the price being charged and the perceived level of risk. In these cases, the Improvement Service will generally contract on their standard terms and conditions, tolerating risks of not having rights of audit, vetting staff etc. Where appropriate the Improvement Service will look to ensure that the supplier has achieved Cyber Essentials Plus or higher.

Further guidance on Supplier Relationships can be found here.

Information Security Incident Management

Information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner. Appropriate corrective action will be taken.

Formal incident reporting and escalation will be implemented.

All employees, contractors and third-party users will be made aware of the procedures for reporting the different types of security incident or vulnerability that might have an impact on the security of the Improvement Service's assets.

Information security incidents and vulnerabilities will be reported as quickly as possible to the Security Team.

The Improvement Service must be capable of providing data from IT systems that could be used as evidence for legal purposes.

Further guidance on Information Security Incident Management can be found here.

Business Continuity Management

The Improvement Service will put in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A Business Continuity management process will be implemented to minimise the impact on the Improvement Service and recover from the loss of information assets. Critical business processes will be identified.

Business impact analyses will be undertaken of the consequences of disasters, security failures, loss of service and lack of service availability.

Business Continuity and Disaster Recovery plans must be reviewed and tested regularly.

Business Continuity and Disaster Recovery plans must take account of any potential overlap in the different business areas of the Improvement Service, as well as partners, suppliers and other stakeholders.

Further guidance on Business Continuity Management can be found here.

Compliance

The Improvement Service will abide by any law, statutory, regulatory or contractual obligations affecting its information systems.

The design, operation, use and management of information systems will comply with all statutory, regulatory and contractual security requirements.

The following table identifies legal and regulatory obligations and requirements that may apply to the operation of the information systems in the Improvement Service

Table 2 - Applicable Legislation

Legislation	Year
Convention on Cybercrime	2001
Official Secrets Act	1989
The Data Protection Act / General Data Protection Regulation (GDPR)	2018
Public Records Act	1958 / 1967
Freedom of Information (Scotland) Act	2002
Malicious Communications Act	1988
The Human Rights Act	1998
The Computer Misuse Act	1990
Copyright (Computer Programs) Regulations	1992
Civil Evidence Act 1968 and the Police and Criminal Evidence Act	1968
The Communications Act	2003
The Regulation of Investigatory Powers Act (RIPA)	2000
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations	2000
Wireless Telegraphy Act	1949
The Communications Act	2003
Serious Organised Crime and Police Act 2005	2005

Privacy and Electronic Communications Regulation	2003
Equality Act	2010
WEEE Regulations	2013
Public Sector Action Plan (PSAP)	2017

Security Policy Framework

More details on specific policy areas are available through the Security Policy Framework. The diagram below identifies specific policy areas and guidance materials:

Authority

Staff, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

Review

This policy will be reviewed annually. Last Reviewed on 27/07/26, next review due on 27/07/27.