The Highland Council

Agenda Item	**21**
Report No	**FHR/ 106/13**

Finance, Housing and Resources Committee
28th August 2013

Information Security Policy

Report by Assistant Chief Executive

Summary
This report informs members of the new Information Security Policy and seeks approval of this Policy.

1 Background

1.1 There is a need to establish an Information Security Policy to set out the Council's commitment and approach to information security.

1.2 Information security is the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to protect confidentiality, integrity and availability.

1.3 The Policy provides high level rules, responsibilities and roles that apply to members, staff and those working on behalf of the Highland Council or with access to Council Information Assets.

1.4 The creation of the Policy supports compliance with the Data Protection Act 1998. Its introduction responds to issues identified by Internal Audit and external Auditors such as the Information Commissioner Office and the Public Service Network Authority.

1.5 More detailed operational requirements are set out in in the Highland Council Information Security Management System (ISMS). This document is being reviewed and approved by the Information Management Governance Board..

1.6 The Highland Council ISMS is based upon the information security international standard ISO/IEC 27001 and the implementation of the controls of ISO/IEC 27002. These standards are referred to as the "ISMS Family of Standards" and are recognised as the International de-facto Security Standards.

1.7 The Information Security Policy provides a clear policy position on a range of issues that are required to support the operation of the ISMS and the operational Information Security Management work of the Information Management & Security Team within ICT Services.

2 Policy Overview

2.1 One of the Council's Information Management Principles (as set out in the Information Management Policy) is that Information is an asset. The Information Security Policy highlights the importance of protecting Information Assets.

2.2 In addition to making the commitment to securing Council Information it also promotes appropriate sharing of information in line with the Information Management Strategy. Information security and the Data Protection Act 1998 need not be a barrier to appropriate sharing of information. Through effective security controls and careful consideration of legal obligations we can be more confident in sharing information where appropriate.

2.3 A key principle through the Policy is a commitment to a risk based approach to Information Security and the handling of Council Information. This approach will support management in ensuring that security resources are spent on the most effective areas of the organisation. For example, would finances be better invested in implementing additional security measures to the network or would investing in the security training of personnel be more effective?

2.4 A policy on encryption is set out, to require the use of encryption where appropriate, but also to ensure the Council is able to decrypt any information so that it can meet its legal disclosure requirements.

2.5 Requirements for building and physical security are set out to protect the Councils Information Assets.

2.6 A requirement to have confidentiality agreements & Information Sharing Agreements is set out to ensure appropriate controls are in place for access to and sharing of information. This support compliance with the Data Protection Act 1998.

2.7 It outlines the requirement for Council ICT Systems to be managed in line with the information security controls set out in the ISMS. This ensures that the governance requirements must be followed for all systems managed throughout the council and by third parties on behalf of the council.

2.8 A policy position on removable media (CDs, DVDs, Memory Sticks, Portable hard drives, memory cards) is outlined – this states that they should only be used for the temporary storage and transportation of data and encryption used where appropriate for the data being held on the device.

2.9 It requires that all Computer media or paper that may contain personal or confidential data must be securely destroyed.

2.10 A Clear Desk and Clear Screen Policy is set out to require ICT Users and those handling Council Information to protect the information through the use of a clear desk and locking their computer screen when away from their device / desk.

2.11 A Password Policy is defined and will be supported by guidance to staff on how to create a complex password. More detailed password requirements are set out in the ISMS and the Information Security Policy requires system owners to follow these requirements and others as set out in the ISMS. This allows the ISMS to be updated on a regular basis with best practice and ensures the council is operating in a secure way.

2.12 A Commitment to respect Intellectual Property Rights of others and to protect the Council's own IPR is made in the Policy. This is a legal requirement.

2.13 To protect the council from attacks to its ICT there is a commitment to carry out Vulnerability Assessment and Penetration Testing where this is considered appropriate based on a risk based approach.

2.14 Information Security roles and responsibilities are set out for all Staff and any person working on behalf of the Council, Managers and Supervisors, Information Asset Owners & System Owners, the Senior Information Risk Owner (SIRO), Responsible Premises Officers, Internal Audit, Information Management Lead Officers, Information Management Link Officers and IM Professionals.

2.15 It sets out the Information Governance arrangements that support the Information Security Policy and other Information Management policies. This includes the Information Management Governance Board, ICT Security Group and ICT Partnership Board. It also sets out the Information Security Incident Reporting and Information Security Investigation Procedure that are defined in more detail in the ICT Acceptable Use Policy.

2.16 It covers the Staff Communication & Training that is required as part of the Policy. It reinforces the requirement for all staff and those handling Council Information to have undertaken the eLearning module on Information Security.

3 Communication & Implementation

3.1 The policy will be made available to Staff and Elected Members through publication of the policy on the Council Intranet and highland.gov.uk website.

3.2 The responsibilities that are placed on staff and managers through the Policy will be communicated through guidance as part of the MI Project, which forms part of the Corporate Improvement Programme.

3.3 This will be supported by the cascading of key messages through the new Information Management Governance Board that has senior representatives from each service within the council.

3.4 The Information Security eLearning module will be reviewed and work will be undertaken to increase staff up-take of this. The Information Management Lead Officers will support this in their services through their management teams.

4 Implications

4.1 **Legal & Risk:** The new Policy supports compliance with the Data Protection Act 1998. Its introduction responds to issues identified by Internal Audit and external Auditors such as the Information Commissioner Office and the Public Service Network Authority, and these issues are already recorded as a corporate risk.

4.2 **Resource:** Communication and Implementation will be carried out using existing resources.

4.3 **Finance:** There are no implications arising from the introduction of this policy.

4.4 **Equalities:** The introduction of this policy does not have a detrimental effect on any particular group.

4.5 **Climate Change:** There are no implications arising from the introduction of this policy.

5. Recommendation

5.1 Members are asked to:

i. Approve the Information Security Policy (Annex A)

Designation: Senior Information & Security Officer
Date: 21 May 2013
Author: Philip Mallard

Background Papers: Information Security Policy

Highland Council
Information Security Policy

Document Owner: Vicki Nairn, Head of E-Government

Contents

1. Document Control

Version History

Version	Date	Author	Change
V0.4	28 July 2013	Philip Mallard	Information Security Policy created

Document Authors

Philip Mallard: Senior Information & Security Officer

Distribution

Name	Role	Reason
Michelle Morris	Assistant Chief Executive	Review and acceptance
Vicki Nairn	Head of E-Government	Review and acceptance
Ken Fox	ICT Operations Manager	Review and acceptance
Jill McAlpine	Project Manager, Managing Information Project, Corporate Improvement Programme	Review
Linda Johnstone	ICT Delivery Manger, ICT Services	Review
Jon Shepherd	ICT Strategy & Projects Manager, ICT Services	Review

2. Introduction

The **Highland Council Information Security Policy** sets out the management commitment and approach to managing information security.

It provides high level rules, responsibilities and roles that apply to members, staff and those working on behalf of the Highland Council or with access to Council Information Assets. More detailed operational requirements are set out in in the **Highland Council Information Management Security System (ISMS)**.

3. Definition of Information Security

Information is an asset that, like other important business assets, is essential to the Highland Council and consequently needs to be suitably protected. This is especially important in the increasingly interconnected and shared business environment.

Information can exist in many forms e.g. It can be printed or written on paper or stored electronically. Whatever form the information takes, or means by which is shared or stored, it should be appropriately protected.

Information security is the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to protect confidentiality, integrity and availability.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisation structures, software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the security and business objectives of the Highland Council are met.

Information security and the Data Protection Act 1998 need not be a barrier to appropriate sharing of information. Through effective security controls and careful consideration of legal obligations we can be more confident in sharing information where appropriate.

4. Highland Council Commitment to Information Security

The Highland Council is committed to Information Security through the management of information security risks that occur through both internal and contracted out activities.

The Highland Council will implement and operate appropriate countermeasures and procedures to manage those risks down to an acceptable level as determined by specialists within the Highland Council and in line with best practice.

The aim is to ensuring business continuity, minimise business risk(s) and maximise the return on investment and business opportunities.

Through the **Information Management Strategy**, supporting policies and the **Information Management Strategy Implementation Plan** the Highland Council will work to put in place the changes that are required to support the **ISMS** and effective information security.

The Highland Council recognises that effective information security is achieved through a combination of policy, procedures, a risk based approach, security controls such as building security and most importantly staff information security awareness and skills. This requires an on-going commitment to continual improvement and change that can only be achieved through the support of all staff and those involved in handling Council Information Assets.

5. Policy, Legal & Standards Framework

The Highland Council recognises that it works within a legal framework that places legal obligations on both the Highland Council and its staff in relation to the management of information. The Highland Council has a framework of Information Management Policies that set out how the Highland Council works to fulfil both the statutory obligations and its duty of care to people and organisations whose information it holds.

The legislation, policy and standards set out below are particularly relevant to the Information Security Policy, but there may be others that also have some relevance and the omission from this list in no way diminishes the Highland Council's commitment to follow its obligations to comply with any statutory requirements and work within best practice.

5.1 Internal Policy

- Information Management Strategy
- Information Management Policy
- Records Management Policy
- Information Security Policy
- ICT Acceptable Use Policy
- ICT Security Policy for Mobile and Flexible Working

5.2 External Standards

- ISO/IEC 27001
- ISO/IEC 27002

5.3 Legislation / regulation

- Data Protection Act 1998
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Copyright, Designs & Patent Act 1988 & other IPR legislation

6. The Information Security Management System (ISMS)

The Highland Councils approach to the management of Information Security is defined in the **Information Security Management System (ISMS)**. This aims to coordinate and continuously improve the management of risk to information and sets out our approach to the application of our Information Security and Information Management Policies. It commits the Highland Council to design, implement and maintain a coherent set of policies, processes, and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. The ISMS provides the means to understand risk, develops ways of managing that risk, monitors how effective that has been and identifies potential areas of improvement and how it needs to adapt to the changing business environment.

The Highland Council ISMS is based upon the information security international standard **ISO/IEC 27001** and the implementation of the controls of **ISO/IEC 27002**. These standards are referred to as the "ISMS Family of Standards" and are recognised as the International de-facto Security Standards.

The ISMS will support management in ensuring that security resources are spent on the most effective areas of the organisation e.g. are finances better invested in implementing additional security measures to the network or would investing in the security training of personnel be more effective?

The ISMS is supported by the Highland Council's **Information Security Policy**, **Information Management Policy**, **Records Management Policy, ICT Acceptable Use Policy** and other related policies that may be introduced. The **Information Management Strategy** sets out the Highland Council's overall strategy for the management of its information which includes Information Security.

7. Information Security Policy Statements (in support of the ISMS)

The following are statements of Highland Council Policy on issues that are important to the delivery of effective Information Security. The Highland Council ISMS sets out operational details of how these are applied by the Highland Council and further guidance will also be provide to those affected by these policy requirements.

7.1 Cryptographic Controls and Key Management (Encryption Policy)

Staff and any person working with Highland Council Information Assets may only use encryption products that are authorised for use by ICT Services.

Only encryption products that include and make use of central key management should be used by the Highland Council. Any exceptions to this must be approved by the Head of E-Government and will require additional controls to be in place to ensure the encryption technology is appropriately managed. This must include (but not be limited to) the corporate retention of keys to enable decryption in the event of the Highland Council being required to do so.

Technical controls and measures required for safe, secure and legally compliant use of encryption products will be within the ISMS accompanying documentation and will be maintained by ICT Services.

The design and configuration of all council ICT Systems and those from third party providers used by the council to store Highland Council Information must adhere to this Encryption Policy and to the technical controls and measures that are set out as part of the ISMS. All contracts with providers and contractors must set out this requirement.

7.2 Physical / Building Security

It is the responsibility of the relevant Responsible Premises Officer (RPO) to ensure that a building used by the council is adequately secure for the storage of the information that is held within it.

Managers and Information Asset Owners should ensure that any building they use for the storage of information (on paper or electronic storage) is adequate for the type of information they are holding. If there are any weaknesses in the building security then this must be reported to the RPO. Any other physical security issues such as a lack of local lockable storage must be dealt with by the Manager / Information Asset Owner responsible for that Information Asset.

7.3 Confidentiality Agreements & Information Sharing Agreements

Prior to any systematic, routine sharing of personal information there must be an Information Sharing agreement put in place. A copy of the information sharing agreement must be provided to the Senior Information & Security Officer to add to the **Highland Council Information Sharing Register.** ICT Services is the custodian of the Register.

Highland Council employment contracts will include confidentiality clauses.

Any third party that is provided with access to Highland Council Information Assets must sign a confidentiality agreement that sets out their obligations and requires compliance with the **Information Security Policy**, **ICT Acceptable Use Policy** and all other relevant Highland Council Policies.

7.4 Management of ICT Systems

All ICT systems must follow the requirements and controls set out in the Highland Council ISMS and any supporting ISMS Policy documents. This should include but not be limited to the appropriate set up, management of systems, implementation and documentation of access controls.

All System Owners must ensure compliance with the Highland Council ISMS and should create and maintain appropriate documentation to support management in accordance with the ISMS.

System Owners must be able to provide documentation as and when requested by ICT Services and Internal Audit that demonstrates their compliance with the ISMS.

7.5 Removable Media

Removable media is a data storage device that is not attached to a computer and can be used to hold and transfer information from one computer to another. This includes CDs, DVDs, Memory Sticks, Portable hard drives, memory cards (eg SD cards).

Removable media should only be used for the temporary storage and transportation of data. Where sensitive or personal data is being held on removable media the data and/or device must be encrypted and done so in accordance with the Encryption Policy. Handling of removable media must be appropriate to the type of information held on it and should follow the **ICT Security Policy for Mobile and Flexible Working.** Only removable media that has been approved for use by ICT Services should be used.

7.6 Disposal of Information held on ICT Equipment, Removable Media and Paper

All Computer media or paper that may contain personal or confidential data must be securely destroyed. Personal and Sensitive data must be removed from ICT equipment prior to destruction or recycling.

All ICT equipment and media must be disposed via an appropriate Highland Council approved disposal service. This can be accessed by contacting the Service Desk.

Paper must be disposed of using the Highland Council confidential waste paper disposal bins. If you do not have access to these then you should contact your RPO to locate the nearest confidential waste paper disposal bin.

7.7 Clear Desk & Clear Screen Policy

All staff, those working on behalf of the council, in a Council Building or handling Council Information must ensure that they lock their screen when away from their desk and ensure that their screen cannot be read by others.

All staff, those working on behalf of the Council or handling Council Information must ensure that they leave their desk or working area clear of all personal or confidential information / documents when they are away from their desk (unless adequately managed on their behalf).

Laptops must be locked away and not left on desks at the end of the working day.

7.8 Password Policy

System Owners must follow the ISMS Password Policy rules when defining requirements, and implementing systems.

Passwords used must be complex. The Council will ensure that any ICT systems use available technical controls to force complex passwords as appropriate to the information being held within the system.

All ICT users must ensure that they follow Highland Council password guidance to create a complex password for each ICT System they access.

Passwords must be treated as confidential and not shared with others. Intentional sharing of passwords is a breach of the **ICT Acceptable Use Policy**.

If a password does become known to another person or there is a suspicion that a password has been compromised then this must be reported as a security incident by contacting the Service Desk.

7.9 Intellectual Property Rights (IPR)

The Highland Council will respect Intellectual Property Rights when handling information, working to ensure it complies with its legal obligations and to protect its own IPR.

7.10 Vulnerability Assessment and Penetration Testing

The Highland Council will carry out Vulnerability Assessment and Penetration Testing on its network infrastructure.

The Highland Council will risk assess the need to carry out Penetration Testing and Vulnerability Assessment on it ICT Systems. It is the responsibility of each System Owner to assess the need for this based on the type of system and the information held within it.

8. Information Security Management Roles & Responsibilities

This section sets out the general and specific responsibilities for information security management, including reporting of information security incidents.

8.1 All Staff and any person working on behalf of the Council

The **Information Management Policy**, **Information Security Policy** and **Records Management Policy** set out requirements for staff at all levels. The **ICT Acceptable Use Policy** provides for defined monitoring of staff ICT usage where it is reasonably suspected that Highland Council policy is not being followed in relation to this usage.

Information Security is everybody's responsibility and is something that should be considered as part of normal everyday working practice.

All those working within a Highland Council Buildings or handling Highland Council Information must ensure that they observe the **Clear Desk & Clear Screen Policy** as set out in the Information Security Policy.

If a potential security issue or incident is identified then this must be reported by the individual or delegated nominee to the Service Desk. This requirement is set out in the **ICT Acceptable Use Policy**, but this also applies equally to any security issue or incident that involves paper based information or physical security where this could impact on the security of Highland Council Information Assets.

Any remote or mobile working that may involve information handling must be consistent with the requirements set out in the **ICT Security Policy for Mobile and Flexible Working.**

8.2 Managers and Supervisors

Security of information within a business unit or building zone is the responsibility of individual managers and staff who work within those areas.

Managers are responsible for information held within their area. This includes ensuring that the information is held securely, access controls are appropriate and maintaining a list of Information Assets in the Corporate Information Asset Register.

Managers must promptly report any building physical security issues to the Responsible Premises Officer. The RPO will work with appropriate staff to remove or reduce any information security risk. Managers must report any remaining risks, after risk reduction, through their management chain to their service management team to be considered as part of the councils approach to risk management.

Managers and supervisors must ensure that all their staff have completed the Information Management online learning module and have understood their obligations under this Policy and other Information Management Policies. Managers should support their staff in this regard by highlighting relevant parts of policies that apply to the roles being performed by a member of staff.

Managers and supervisors must ensure that their work area and that of their staff is adequately secured including the implementation of the **Clear Screen and Clear Desk Policy** as set out within the **Information Security Policy**.

8.3 Information Asset Owners & System Owners

An Information Asset Owner is a person who has been identified as being responsible for a Highland Council Information Asset. A System Owner is a person who has been identified as being responsible for a Highland Council ICT System.

An Information Asset is a collection of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. All Information Assets should be recorded in the Highland Council Information Asset Register that is corporately held by ICT Services.

Each ICT System and the information held within it is also considered to be an Information Asset and is recorded as such in the Highland Council Information Asset Register.

Information Asset Owners and System Owners are responsible for ensuring that the security controls applied to their Information Asset are appropriate and that the Information Asset is held securely with access to the information being provided as appropriate.

Information Asset Owners and System Owners must ensure that the information recorded in relation to their Information Asset in the Information Asset Register is correct and up-to-date.

8.4 Senior Information Risk Owner (SIRO)

The SIRO is the senior person responsible for management of information security risks and for reporting this to the Assistant Chief Executive and Highland Council Senior Management Team. The SIRO role is performed by the Head of E-Government.

The Head of E-Government is the corporate strategic owner of Information Security as a part of Information Management Strategy.

8.5 Security Management

The Senior Information & Security Officer as the Team leader of the Information Management & Security Team within ICT Services has operational strategic ownership of Information Security as a part of Information Management on behalf of the Head of E-Government.

Information Security Incident Management and Investigations are managed by ICT Services on behalf of the Head of E-Government.

8.6 Records Management

This role is performed by the Records Manager based within the Records Management Service provided to the Council by High Life Highland. The Records Management function is overseen by the Highland Council via the Senior Information & Security Officer on behalf of the Head of E-Government.

The Records Manager is responsible for ensuring all Highland Council records are held within appropriate records management systems and structures and to advise the Highland Council on records management in support of effective management and security of information.

The Records Manager is responsible for maintaining the Highland Council Information Asset Register. This includes information on the security classification and security controls, and maintaining a register of information held within paper records stores.

8.7 Data Protection Officer

The Data Protection Officer role is performed by the Senior Web Development and FOI Officer who is responsible for dealing with requests for information under the Data Protection Act 1998, for monitoring Privacy Impact Assessment and for reporting Data Protection Breaches to the Information Commissioners Office (ICO).

The Senior Information & Security Officer is also responsible for ensuring the Council's ISMS, Information Management and Security Policies, and Information Security Incident Reporting processes support the Council's compliance with the Data Protection Act 1998.

8.8 Responsible Premises Officer (RPO)

The RPO is responsible for the physical security of buildings through the effective management of perimeter security and zoning of buildings. Physical security of information within a business unit or building zone is the responsibility of the Information Asset Owners, individual managers and staff who work within those areas.

The RPO must respond promptly to any building physical security issues that are brought to their attention by any member of staff (or visitors) to remove or reduce any information security risk. Any remaining risk must be reported by the RPO to the Senior Information & Security Officer and the relevant Information Asset Owners / managers. These Managers must then report this through their management chain to their service management team to be considered as part of the Highland Council's approach to risk management.

8.9 Internal Audit

The Highland Council's Internal Audit function includes responsibility for auditing the adequacy of the Council's Information Security Policy, procedures, internal information security controls, their implementation and Corporate and Service compliance with these.

8.10 Information Management Lead Officer

The IM Lead Officer is a senior representative from each Council Service that represents their Service on the Information Management Governance Board (IMGB) and provides a strategic lead for Information Management and Information Security within each Service.

The IM Lead Officer will be required to attend the monthly IMGB meetings, communicate and cascade information within their Service and ensure adoption of working practices that are consistent with IM Policy and Guidance.

IM Lead Officers will be supported in their role through information and guidance provided through the Information Management Governance Board. Operational Support will also be available from IM Link Officers that have been identified within their service.

8.11 Information Management Link Officer

The IM Link Officer is a role that exists to provide support to the IM Lead Officer and the Corporate IM functions in the implementation of Information Management and Information Security improvements.

9. Information Security Governance and Process

9.1 Information Management Governance Board (IMGB)

The IMGB has been created to oversee the management of the Highland Council Information Management Strategy and the implementation of this across the Council. There is an IM Lead Officer from each of the Services that will represent their Service on the Board. Each Service Director is required to identify a member of their senior management team to act as IM Lead Officer for their service.

The IMGB is chaired by the Head of E-Government as the corporate owner of Information Management Strategy and Policy and as SIRO.

The primary role of the IGMB is to identify priorities for the implementation of Information Management improvements and the strategic initiatives identified in the IM Strategy Implementation Plan.

The IMGB has a duty to consider and make recommendations to the Senior Management Team about information management issues and influence strategy and policy development.

The IMGB will review high level information security risks that are referred through from the ICT Security Group and other information security risks that relate to non-ICT issues.

9.2 ICT Security Group

Operational Information Security management is managed by ICT Services. The ICT Security Group exists to support this through the review of security incidents and identifying and evaluating security risks.

The ICT Security Group is chaired by the Senior Information & Security Officer. Membership will include the Senior Information & Security Officer, the Information & Security Officer, the Security Officer from our ICT Provider, and technical representatives from areas of the Council with technical involvement in ICT security.

The ICT Security Group will operate under Service management governance and the Senior Information & Security Officer will report back to the IMGB, identifying information security risks that require consideration by the IMGB. Any technical issues that are ICT Security risks or require ICT changes to manage the risk, will be referred to the ICT Partnership Board through normal ICT Services service management governance.

9.3 ICT Partnership Board

The ICT Partnership Board is a Board chaired by the Assistant Chief Executive that reviews strategic development of the Highland Council ICT and approves major changes. Its membership includes representatives from the Highland Council ICT provider.

It will consider any significant technical ICT security risks that are identified. The ICT Delivery Manager within ICT Services will review ICT Security risks identified by the ICT Security Group or through security management activities.

9.4 Information Security Incident Reporting

Information Security Incidents or concerns about information security must be reported through the Service Desk.

The **ICT Acceptable Use Policy** sets out the Council's expectations on all ICT Users to report all security incident or concerns. This also applies to any other user of Highland Council information or those working on behalf of the council when this concerns paper based information.

9.5 Information Security Investigation Procedure

The **ICT Acceptable Use Policy** sets out the monitoring that the Council may undertake of ICT usage. The Council may undertake a Potential Misuse Investigation into the activity of a user or investigate any information security incident, regardless of whether the incident involves information held in ICT systems or on paper. The investigation procedure is set out in more detail in the **ICT Acceptable Use Policy**.

10. Staff Communication & Training

The **Information Security Policy** and other Information Management policies will be made available to staff through the Intranet and others within scope of the policies through the Highland Council website.

Staff and any person handling Council Information are provided with an online learning module that provides an introduction to the expectations the Council places on those handling information. This includes the information security and data protection issues that staff should be aware of.

All staff must complete the Information Management online learning module and managers must ensure that this has been completed by their staff.

Any other person handling Highland Council information must also complete this training and the relevant Information Asset Owners and Manager within the Council responsible for the contract must ensure this takes place.

Further information security online learning modules may be provided to staff and these must be completed where they are relevant to their role. Staff will be informed when they must complete these additional training modules.