Information Security Policy v2.2

A University wide Information Security policy produced for the Information Services Strategic Risk Group.

Contents

1.0 Scope

This Information Security Policy (the "Policy") applies to all users ("Users") of (i) the University network; (ii) devices connected to the University network; and (iii) users of services and information related to the University network.

2.0 Responsibilities

Role	Responsibilities
Information Strategy Committee	Approval of Policies
Information Security Strategic Risk Group	Consult and Review Policies
Information Services Directorate	Advise on Policies. Create Standards in line with Policies and Guidance on adherence to Standards and maintain central registers
Data/System/Service Business Owners	Create Process and Procedures that comply with the Policies and Standards
Data/System/Service Guardians	Implement Process and Procedures
Users	Be familiar with and adhere to the Policies and Procedures at all times

3.0 Governance

Responsibility for the production, approval, implementation, review and communication of this Policy is delegated to the Information Security Strategic Risk Group.

4.0 Core Policies

Core policies are high level strategic statements applicable to all.

4.1 Information Security

a) The Information Security Policy supports the University and IT strategic visions by defining the high-level approach taken to reducing associated risks to its reputation, finances and operations.
b) The University is committed to following and developing the Scottish Government's Public Sector Action Plan on Cyber Resilience.
c) The University will develop and communicate information security policies, standards, processes and procedures that all staff, students and third parties are required to comply with.

d) Information managed by the University shall be appropriately secured to protect confidentiality, integrity and availability, following the University's Risk Framework and Information Services Directorate Standards.
e) Information will be managed so that the University can ensure appropriate legal, regulatory and contractual obligations are complied with.
f) The University acknowledges that information security is the responsibility of every member of staff, student and third parties. The University is committed to an ongoing programme of awareness, training and education to address this.
g) The Information Security Policy will be regularly reviewed, consulted on and updated if required, to adequately balance security and usability requirements.

4.2 Data Handling

a) The University aims to ensure that key data and systems are classified, considering regulatory requirements.
b) The University will make qualified risk and security personnel available to assist business and service owners in classifying systems and implementing appropriate security measures and procedures.
c) The University will clearly signpost which of its storage systems are appropriate for which classification of data.
d) It is the responsibility of users to understand the classification of data they are working with and ensure the required procedures are followed to maintain security.

4.3 Monitoring

a) The University has legal, regulatory and operational requirements to monitor activity across its network and systems.
b) Information relating to this monitoring (e.g. logs) will be retained for long enough to meet these requirements and for no longer.
c) The University will protect the integrity and confidentiality of its information and systems by gathering security logs to help identify threats and support investigations.
d) All systems will be assessed and configured to log appropriate security event information and the logs will be protected against unauthorised access and accidental or deliberate modification.
e) Security logs will be analysed and reviewed regularly for each system.
f) All monitoring activities must be authorised and documented. Certain monitoring activities will be regularly performed to help identify suspicious or unauthorised activity.
g) All personnel authorised to perform monitoring functions will do so in accordance with the relevant legislation, ethics, procedures and safeguards.
h) The University will provide monitoring information to authorised agencies with investigatory powers when legally obligated to do so.

5.0 User Policies

User policies are applicable to all users.

5.1 Acceptable Use - Access

a) Access to the University network(s) does not imply authorisation to all services on the network. Access to services and devices, without authorisation, is a criminal offence.
b) Scanning of devices or services on the University network is prohibited, without appropriate authorisation.
c) It is prohibited to connect networking devices to the University infrastructure without prior and explicit written permission of the Network Manager - Information Services Directorate.
d) All University owned end-user devices must authenticate through the University's central directory system before accessing University resources. All University owned devices must be managed by a qualified member of Information Services Directorate or faculty IT.
e) All University owned devices must be under vendor support.
f) The University requires all users to provide a personal email address for password resets and for contact should a user's account be suspended.
g) Authorised Information Services Directorate staff have the right to withdraw the access to any University service to protect University resources.
h) All University purchased devices must be procured through centralised or Faculty IT purchasing processes.
i) Password for University accounts must not be used for any other accounts.
j) Sharing of University passwords is not permitted.
k) License agreements of available software must not be broken.

5.2 Acceptable Use – Personal Use

5.2.1 Personal use of University IT systems are permitted under the following conditions:

a) Activities are lawful.
b) At the user's own risk.
c) Withdrawn if deemed to be excessive or threatens the integrity of University services.
d) Must not interfere with University obligations.
e) Must not hinder the use of others.

5.2.2 The following uses are explicitly prohibited:

a) Personal commercial activity.
b) Access or disseminating material of a pornographic, criminal or offensive nature including material promoting terrorism, except when prior written authorisation has been granted by the appropriate body and Information Services Directorate.

c) University-owned devices cannot be taken on non-work-related travel without prior written authorisation from the appropriate University body and Information Services Directorate. Further information can be found on the Travel Policy site.

5.3 Physical Security

a) All infrastructure hardware (e.g. servers, switches, routers) must be located in secured and restricted areas.
b) All end user devices must be securely stored when not in use.
c) Computer workstations must be locked when workspace is unoccupied.
d) All sensitive/confidential information in hardcopy must be secured in workspace at the end of the day or when unoccupied for an extended period.
e) Any theft or loss of a University device or University data must be reported to the Helpdesk immediately.

5.4 Personal Devices (BYOD)

Use of personal devices for university purposes are permitted under the following conditions:

a) **Policies**
All other Information Security Policies are valid and must be met.
b) **Security Compliance**
Personal devices must meet University security standards, including antivirus, encryption, and strong passwords.
c) **User Responsibility**
Users must understand and enable security features on their devices to protect University data.
d) **Data Security**
Users should avoid storing University data on personal devices, where possible. Confidential or sensitive data, including personal data, should only be held on personal devices if appropriate security standards are engaged, e.g. encryption. All University data must be securely deleted from personal devices before device disposal. All University data held on personal data is still the property of the University and all relevant policies still apply.
e) **Incident Reporting:**
Theft or loss of a device containing University data must be reported to the Helpdesk immediately.
f) **Device Management:**
The University may scan personal devices for security issues when connected to the network.
g) **Support Disclaimer:**
The University does not provide support for personal devices.

h) **Monitoring:**
You must accept that the University may scan the device for security issues when it is connected to the University network.

i) **Access:**
Any personal device must not be connected to the wired campus network, the wired network is only for University owned devices.

5.5 Remote Working

Where remote working is permitted by your department, you must work under the following conditions to ensure the security of University data and systems:

a) **Network Use:**
Employees should prioritise working from trusted, secure networks, such as home or private networks. Use of public or unsecured Wi-Fi networks should be avoided whenever possible.

b) **VPN Usage:**
The University's Virtual Private Network (VPN) should be used when accessing or handling sensitive or confidential University data, especially from public or untrusted networks. Only University managed devices can be used on the VPN. For routine activities, such as accessing cloud-based or web applications (e.g. Office 365) that do not require direct interaction with the University's internal network, VPN use is not necessary if you are on a trusted, secure network.

c) **Device Security:**
Devices used for remote work, whether University-owned or personal, must comply with university security standards, including up-to-date antivirus software, firewalls, and encryption of sensitive data.

d) **Access Control:**
Multi-Factor Authentication (MFA) must be used to access University systems remotely. Passwords must not be shared or reused across multiple platforms.

e) **Data Handling:**
Users should avoid storing University data on personal devices, where possible. Confidential or sensitive data, including personal data, should only be held on personal devices if appropriate security standards are engaged, e.g. encryption. All University data must be securely deleted from personal devices before device disposal. All University data held on personal data is still the property of the University and all relevant policies still apply.

f) **Workspace Security:**
Employees must ensure that their remote workspace is secure, including locking devices when not in use and preventing unauthorised access by others in the household or vicinity.

g) **Incident Reporting:**
Any security incidents, including loss or theft of devices, unauthorised access, or suspected data breaches while working remotely, must be reported immediately to the University Helpdesk.

h) **Compliance:**
All remote work must comply with the University's Information Security Policy and any specific departmental guidelines. Employees are responsible for ensuring their remote working practices align with these policies

6. Management Policies

Management policies are policies that are aimed at business/system/service owners.

6.1 Incident Response

a) The University is committed to identifying, responding to and recovering from security incidents to minimise the impact and reduce the risk of similar incidents occurring.
b) A suitably resourced and trained incident response team will be assembled for managing a security incident.
c) A review will take place, where appropriate, to identify the root cause and highlight any improvements that can be made to the University's security posture.
d) This policy will align with the University's Incident Response Plans, specifically the Cyber Incident Response Plan.

6.2 Cloud Access

a) Any purchase or use of a cloud service will align with University strategic goals, will have a named business owner, regularly reviewed and supported by a contract.
b) Where required there will be a Cybersecurity risk assessment performed as part of the purchase process for the full lifecycle of the service including creation, processing, storage, transmission, exit strategies and destruction of information.
c) The risk assessment will take into consideration the classification of data assigned and its suitability for use in the cloud.
d) Where required, a Data Protection Impact Assessment must be undertaken to identify any privacy risks. Multifactor login for administration must be enabled.

6.3 Child Access

a) For the purposes of this policy, a child is deemed to be an individual under the age of 18, except where the individual is a registered student or member of staff (see 6.3 f).
b) Children attending an organised event can be granted a temporary account.

c) Children's use of IT equipment must be appropriately supervised by the individual(s) responsible for them on campus.
d) It should be recognised that the IT facilities provided will be appropriate for the use of adults.
e) Risk assessments are required for children on campus; in completing these risk assessments the use of IT systems and equipment should be considered.
f) This policy does not apply where the child is a registered student or member of staff. However, departments will still have to ensure the health, safety and welfare of this young person under relevant University policies and legislation.

6.4 Business Continuity

a) Business continuity plans for all IT related services must be documented and should be the result of a risk assessment.
b) Each plan must be prepared by or in conjunction with the service owner and relate to likely scenarios.
c) Roles and responsibilities must be defined and documentation/training available.
d) Business continuity plans must be reviewed and tested on a regular basis.
e) Backups must be protected from loss, damage, unauthorised access and subject to the same level of protection as the live information.
f) Backups must be regularly verified by successfully testing restoration.

6.5 3rd Party Access

a) The University may, at its discretion, provide access to services for 3rd parties. This may include:
    - Research collaborators and partners
    - Maintenance and service providers
    - Commercial tenants
b) A contract must be in place between the University and the 3rd party, detailing the level of service offered, terms and conditions (including applicable data protection clauses), and any charges which may apply.
c) 3rd parties requiring connection to the University network must evidence information security practises in line with or exceeding the University policies and standards, on an ongoing basis.
d) 3rd parties requiring connection to the University network must provide a business owner, technical guardian and contact details.
e) Remote access by 3rd parties to University systems must be authenticated against a central Information Services Directorate managed system, with appropriate logging in place.
f) 3rd party remote access for maintenance and support purposes must be disabled when not in use, with an auditable request process in place for enablement.

g) 3rd parties requiring access to University data will align with University strategic goals with a named business owner, be regularly reviewed and supported by a contract/agreement.
h) Where 3rd parties require access to University personal data or otherwise sensitive or confidential data, appropriate risk assessments should be undertaken. For personal data this may include a Data Protection Impact Assessment. Relevant agreements governing access should be put in place, which include appropriate data protection clauses, where required.

7.0 Glossary

a) Personal device – a device which is owned by the individual and not by the University. This includes, but is not limited to, smartphones and home PCs.
b) Networking device – a device which is configured for its primary purpose to be to provide networking services. This includes, but is not limited to, routers, wireless access points, switches or any system with multiple network interfaces, which may be configured to bridge, forward, route or relay traffic between those interfaces.
c) End User device – a device designed to be used by an End User. This includes, but is not limited to PCs, laptops, smartphones, tablets, owned by the University, the individual or other 3rd parties.
d) University owned device – a device which is owned by the University.

Version Control

Version	Date	Changes
1.0	March 2020	Initial version
2.0	July 2022	Minor changes
2.1	November 2024	Non work-related travel guidance and remote working section added, linkage to University Incident Response plans. Additional 'light touch' changes to update some wording. Cosmetic changes and addition of a version control table
2.2	October 2025	Review – typo in section 6.3 (a)

Date of next review:

November 2026