INFORMATION SECURITY POLICY

	Version 2.02
	A University wide Information Security policy produced by the Digital Campus Sub Committee.

Contents

1 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 RESPONSIBILITIES

Role	Responsibilities
Information Strategy Committee	Approval of Policies
Digital Campus Sub Committee	Consult and Review Policies
Information Services Directorate	Advise on Policies. Create Standards inline 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 GOVERNANCE

Responsibility for the production, approval, implementation, review and communication of this Policy is delegated to the Digital Campus Sub Committee of the University’s Information Strategy Committee.

This policy will be reviewed annually as part of the annual security report to the Audit and Risk Committee.

Last Review date: 31/03/2022

4 CORE POLICIES

Core policies are high level strategic statements applicable to all

4.1 INFORMATION SECURITY

1. **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.**

2. **The University is committed to following and developing the Scottish Governments Public Sector Action Plan on Cyber Resilience.**

3. **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.**

4. **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.**

5. **Information will be managed so that the University can ensure appropriate legal, regulatory and contractual obligations are complied with.**

6. **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.**

7. **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

1. **The University will ensure all data and systems are classified, taking into account regulatory requirements.**

2. **The University will maintain a systems register detailing classification of systems.**

3. **The University will provide access to appropriately qualified risk and security experts to assist business and service owners in classifying and implementing appropriately secure systems and procedures.**

4. **The University will clearly signpost which of its storage systems are appropriate for which classification of data.**

5. **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

1. **The University has legal, regulatory and operational requirements to monitor activity across its network and systems.**

2. **Information relating to this monitoring (e.g. logs) will be retained for long enough to meet these requirements and for no longer.**

3. **The University will protect the integrity and confidentiality of its information and systems by gathering security logs to help identify threats and support investigations.**

4. **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.**

5. **Security logs will be analysed and reviewed regularly for each system.**

6. **All monitoring activities must be authorised and documented. Certain monitoring activities will be regularly performed to help identify suspicious or unauthorised activity.**

7. **All personnel authorised to perform monitoring functions will do so in accordance with the relevant legislation, ethics, procedures and safeguards.**

8. **The University will hand over information to agencies with investigatory powers, when legally required to do so.**

5 USER POLICIES

User policies are policies applicable to all users.

5.1 ACCEPTABLE USE

5.1.1 ACCESS

1. **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.**

2. **Scanning of devices or services on the University network is prohibited, without appropriate authorisation.**

3. **It is prohibited to connect networking devices to the University infrastructure without prior and explicit written permission of the Network Manager - Information Services Directorate.**

4. **All end user devices must be authenticated against central Information Services Directorate managed systems.**

5. **All University owned device must be managed by a qualified member of Information Services Directorate or faculty IT.**

6. **All University owned device must be under vendor support.**

7. **The University requires all users provide a personal email address for password resets and for contact should your account be suspended.**

8. **Authorised Information Services Directorate staff have the right to withdraw the access to any University service to protect University resources.**

9. **All University purchased devices must go through central procurement.**

10. **Password for University accounts must not be used for any other accounts.**

11. **Sharing of University password is not permitted.**

12. **License agreements of available software must not be broken.**

5.1.2 PERSONAL USE

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

1. **Activities are lawful.**

2. **At the user's own risk.**

3. **Withdrawn if deemed to be excessive or threatens integrity of University services.**

4. **Must not interfere with University obligations.**

5. **Must not hinder the use of others.**

The following uses are explicitly **prohibited**:

1. **Personal commercial activity.**

2. **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.**

5.2 PHYSICAL SECURITY

1. **All infrastructure hardware (e.g. servers. switches, routers) must be located in secured and restricted areas.**

2. **All end user devices must be securely stored when not in use.**

3. **Computer workstations must be locked when workspace is unoccupied.**

4. **All sensitive/confidential information in hardcopy must be secured in workspace at the end of the day or when unoccupied for an extended period.**

5. **Any theft or loss of a University device or University data must be reported to the Helpdesk upon becoming aware of the theft or loss.**

5.3 PERSONAL DEVICES

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

1. **All other Information Security Policies are valid and must be met.**

2. **Your personal device must have equivalent security to University provided device standards.**

3. **You must have familiarised yourself with your device and its security features and enabled options to ensure the safety of University information.**

4. **You must report any theft or loss of University data to the Helpdesk upon becoming aware of the theft or loss.**

5. **You must ensure that University data is securely removed from a device before disposal or transfer of the device.**

6. **You must accept that the University cannot take responsibility for supporting devices it does not provide.**

7. **You must accept that they University may scan the device for security issues when it is connected to the University network.**

8. **If using a smartphone to access University data, you must consent to your device being used as a second authentication method to University systems.**

9. **Any personal device must not be connected to the wired campus network, the wired network is only for university owned devices.**

6 MANAGEMENT POLICIES

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

6.1 INCIDENT RESPONSE

1. **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.**

2. **A suitably resourced and trained incident response team will be assembled for managing a security incident.**

3. **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.**

6.2 CLOUD

1. **Any purchase or use of a cloud service will align with University strategic goals and be: centrally registered with a named business owner; approved by Information Services Directorate; regularly reviewed; supported by a contract.**

2. **There will be a risk assessment performed for the full lifecycle of the service including: creation, processing, storage, transmission, exit strategies and destruction of information.**

3. **The risk assessment will take into consideration the classification of data assigned and its suitability for use in the cloud.**

4. **A Data Protection Impact Assessment must be undertaken and any sharing of data with a 3rd party must adhere to legal requirements.**

5. **Multifactor login for administration must be enabled if available.**

6.3 CHILD ACCESS

1. **Children attending an organised event can be granted a temporary account.**

2. **Children's use of IT equipment must be appropriately supervised by the individual(s) responsible for them on campus.**

3. **It should be recognised that the IT facilities provided will be appropriate for the use of adults.**

4. **Risk assessments are required for children on campus; in completing these risk assessments the use of IT systems and equipment should be considered.**

5. **This policy does not apply where the child is a registered student or member of staff, however, departments will have to account for this in ensuring the health, safety and welfare of this young person under all relevant legislation.**

6.4 BUSINESS CONTINUITY

1. **Business continuity plans for all IT related services must be documented and should be the result of a risk assessment.**

2. **Each plan must be prepared by or in conjunction with the service owner and relate to likely scenarios.**

3. **Roles and responsibilities must be defined and documentation/training available.**

4. **Business continuity plans must be reviewed and tested on a regular basis.**

5. **Backups must be protected from loss, damage, unauthorised access and subject to the same level of protection as the live information.**

6. **Backups must be regularly verified by successfully testing restoration.**

6.5 3rd PARTY ACCESS

1. **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**

2. **A contract must be in place between the University and the 3rd party, detailing the level of service offered, terms and conditions, and any charges which may apply.**

3. **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.**

4. **3rd parties requiring connection to the University network must provide a business owner, technical guardian and contact details.**

5. **Remote access by 3rd parties to University systems must be authenticated against a central Information Services Directorate managed system, with appropriate logging in place.**

6. **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.**

7. **3rd parties requiring access to University data must evidence information security practises in line with or exceeding the University policies and standards, on an ongoing basis.**

8. **3rd parties requiring access to University data must be centrally registered detailing a University business owner; technical guardian; contact details. This access should be formally reviewed on a regular basis.**

9. **For 3rd parties requiring access to University data a Data Protection Impact Assessment must be undertaken and any sharing of data with a 3rd party must adhere to legal requirements. Data Processing/Sharing documentation must be completed as appropriate**

7 APPENDIX: GLOSSARY

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.

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.

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.

University owned device – a device which is owned by the University.