Keele UNIVERSITY

INFORMATION SECURITY POLICY

1. INTRODUCTION

Keele University is reliant on its information assets to function effectively. It is essential that the University's information assets are protected against the consequences of breaches of confidentiality, failures of integrity and interruptions to availability. An information security breach could damage the University's reputation, cause distress to individuals, and result in substantial fines from the Information Commissioner's Office.

1.1 Purpose

The purpose of this Policy is to:

- set out the University's intentions in managing information security as part of effective governance
- ensure the protection of all the University's information assets and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these assets
- ensure that the University's authorised users are aware of and are in a position to comply with all current and relevant UK and EU legislation
- ensure that the University's authorised users understand their own responsibilities for protecting, preserving and managing the confidentiality, integrity and availability of the University's information assets
- set out the University's intentions in managing information security as part of effective governance

1.2 Scope

This Information Security Policy:

- Applies to all staff, students, governors, consultants, contractors, partnership organisations and partner staff of Keele University
- Covers all information handled, stored, processed or shared by the University irrespective of whether that information originates with or is owned by the University.
- Applies to all computer and non-computer based information systems owned by the University or used for University business or connected to University managed Networks
- The University's data can broadly be classified as personal data and non-personal data:
    - personal data is treated in accordance with the University's Data Protection Policy and is afforded the highest standard of protection as detailed in the Data Classification and Handling Guidance
    - non-personal data can include:

- sensitive organisational data such as commercially sensitive planning data, research data, data protected by confidentiality agreements or legally privileged information – all of these categories of data are also afforded a high level of protection
- other organisational data that is either already made public (e.g. on University website) or is potentially disclosable to the public (e.g. pursuant to a request under the Freedom of Information Act) – such data must be accurate, must be kept up-to-date and must be protected from destruction and unauthorised interference.

2. POLICY

2.1 Information Security principles:

- Information assets are identified, classified and protected in accordance with the Information Asset register documentation. Any security controls which are implemented must be proportionate to the defined classification. Information assets are controlled by the Information Asset Managers as outlined in the Information Governance Framework document
- All the University's information assets whether electronic or in hard-copy form must be protected against unauthorised access
- The University's information assets must be available to all those who have a legitimate need to access them
- The integrity of the University's information must be maintained so that it is accurate and complete
- All users of the University's information systems will comply with the University's information security and data protection policies and guidance including the IT Conditions of Use. It is the responsibility of users to ensure that they continually familiarise themselves with and fully understand the contents of the policies and guidance. Failure to comply with the information security policies and guidance may result in disciplinary action.
- All users of the University's information systems will abide by and adhere to all current UK and EU legislation as well as regulatory and contractual requirements.
- All information assets will be classified according to their required levels of confidentiality. The classification of the asset will determine the security controls that will be applied to it and how it must be handled
- All information assets will be assigned an owner who will be responsible for ensuring that the asset has the correct information classification, has adequate protection and is handled at all times in accordance with its classification.
- Key information assets will be subject to annual risk assessments to identify the probability and impact of security failures. The results of the risk assessments will determine the appropriate security controls to be applied to the assets.
- All users of Keele information systems shall receive information security training appropriate to their role.

- All suspected and actual information security breaches must be recorded and reported through the IT Service Desk by completing an electronic incident form. The incident will automatically be brought to the attention of the Head of Projects and Service Assurance who will take the appropriate actions according to the information in the incident report.

2.2 Training

The annual Information Security training is mandated by UEC and therefore must be undertaken by all staff, contracted or FTE. If the contracted staff have completed a suitable level of security training in their primary organisation, The University will accept a certificate on submission to the Organisational Development team.

The Information Security training will be provided via the Learning Pool online learning system. It will be developed annually by the Head of Projects and Service Assurance.

Training completion rates are monitored through the Qlikview reporting system available at:
https://qlikviewreports2.keele.ac.uk/qlikview/index.htm

- The Information Security Training Management Summary report details the percentage uptake within Faculties and Directorates plus the actual staff who have completed the training.
- The InfoSecurity Training report details those staff who:
  - Have never completed the training module
  - Have completed the training at least once but have not renewed it and therefore are no longer compliant
  - Will need to complete the training in the next three months to remain compliant

If you do not have access to the Qlikview reports or you cannot see the reports using your current access rights please log a call with the IT Service Desk.

2.3 Supporting Guidance and Procedures

The following documents, whilst not included in this policy document provide the wider clarification of Information Security and therefore the same levels of application and adherence are required and expected to ensure a fully robust Information Security environment.

- Data Classification and Handling Guidance
- Clear Desk and Screen Guidance
- Information Security Risk Management Guidance
- IT Monitoring and Interception Guidance
- Mobile Device Guidance
- Bring Your Own Device Guidance
- Removable Media Guidance
- Third Part Access for Staff Guidance
- IT Guidance (supplement to the IT Conditions of Use)
- Two Factor Authentication Guidance
- Password Management Guidance

3. ROLES AND RESPONSIBILITIES

3.1 Vice Chancellor and the University Executive Committee

The Vice Chancellor has the ultimate responsibility for information security at the University. The Vice Chancellor, supported by the University Executive Committee, will ensure that the University complies with relevant external requirements including legislation and contractual obligations. The Vice Chancellor and the University Executive Committee are responsible for the overall direction and commitment to information security. The Committee will approve information security policies and guidance, provide high level support for security initiatives and review the adequacy of the University's Information Security Management System. Deans and Directors will take responsibility for operational compliance within their areas of responsibility.

3.2 Senior Information Risk Owner (SIRO)

A Senior Information Risk Owner (SIRO) for the University's overall information security objectives shall be designated by the Vice-Chancellor. The SIRO shall be a member of the University Executive Board. The key responsibilities of the SIRO shall be to:

- ensure that this policy and the information security objectives are compatible with the strategic direction of the University
- ensure that data and information assets are identified; that the top level data and information governance roles are allocated and that the post-holders are appropriately briefed on their information security roles and carry out their functions with due diligence
- own the risks associated with the information security objectives and ensure that control action owners are identified
- ensure that exception procedures are in place to authorise at an appropriate level acceptance or mitigation of significant information security risks that deviate from agreed standards
- determine when and by whom breaches of information security shall be reported to relevant external authorities
- ensure there is clear direction and visible management support for security initiatives and promote continual improvement
- ensure the Vice-Chancellor and Council are adequately briefed on risk management issues
- The SIRO is supported by the Head of Projects and Service Assurance and the Information Asset Owners

3.3 Head of Projects and Service Assurance

The Head of Projects and Service Assurance is responsible for:

- creating, reviewing and maintaining information security policies and guidance
- monitoring and reporting on information security within the University
- developing the annual information security training module
- undertaking risk assessments of key information assets

- evaluating security technologies, processes and the implementation of appropriate levels of security control
- assessing the adequacy of information security controls for new or changed systems/services
- providing an advisory service on information security
- investigating suspected or actual security incidents

3.4 Information Asset Owners (IAOs)

The Deans and Directors that sit on the University Executive Committee also act as the IAOs for their respective areas. They actively support the SIRO by providing reports on a regular basis as determined by, and agreed with, the Information Governance Group. A more detailed description of their roles and responsibilities are documented in the Information Governance Framework document. Ensure all staff in their areas of responsibility have completed the mandated annual Information Security training.

3.5 Information Governance Group

The Information Governance Group considers all matters concerning the management of information security and information governance. The Group reports to the University Executive Committee. The remit of the Group is outlined in the Information Governance Framework document.

3.6 Heads of Schools, Departments, Centres and Institutes, and Line Managers

Heads of Section and Heads of Departments, Schools, Centres and Institutes are responsible for ensuring that their department complies with the University's information security requirements and has effective systems in place for the managing of information security in accordance with this policy and the supporting documentation and guidance. Ensure all staff in their areas of responsibility have completed the mandated annual Information Security training.

Line managers will investigate in a timely manner any security concerns that their staff may have and if necessary report them to the Head of Projects and Service Assurance. Ensure all staff in their areas of responsibility have completed the mandated annual Information Security training.

3.7 All Staff, Students and Third Party Visitors and Contractors

All the University's system users are responsible for complying with the University's information security policies and guidance. All University system users will sign the IT Conditions of Use before being supplied with their network account credentials. Users are responsible for reporting any suspected security incidents immediately to the IT Service Desk or, if appropriate, to their line manager. If required, to undertake the mandated annual Information Security training.

4. RELATED POLICIES AND PROCEDURES

- Data Protection Policy
- IT Conditions of Use
- Information Governance Framework
- Email Policy

5. REVIEW, APPROVAL & PUBLICATION

- The Head of Projects and Service Assurance is responsible for the review of this policy
- The policy should be reviewed and updated every two years
- The policy will be approved by UEC and Council

6. ANNEXES

No annexes required

7. DOCUMENT CONTROL INFORMATION

Document Name	Information Security Policy
Owner	Simon Clements, Head of Projects and Service Assurance, Information and Digital Services
Version Number	Version 2.1
Equality Analysis Decision and Date	TBC
Approval Date	19 September 2019
Approved By	Council
Date of Commencement	19 September 2019
Date of Last Review	[Day/month/year]
Date for Next Review	September 2022
Related University Policy Documents	Data Protection Policy
For Office Use – Keywords for search function	