# Information Security Policy

## Contents

## 1. Introduction

**1.1.** Information is a key resource for the University to function effectively. It must be protected from threats to its confidentiality, integrity, and availability, which will result in substantial negative reputational, financial, or legal consequences when not handled appropriately.

## 2. Purpose

2.1. The purpose of this policy is to:

- Detail the University's approach to manage information security as part of effective Information Governance.
- Ensure the protection of all the University's information assets and to mitigate the risks associated with their theft, loss, misuse, damage, or abuse.
- Ensure that users are aware of and are enabled to comply with all current and relevant university policies and UK legislation.
- Ensure that the University's users understand their own responsibilities for protecting, preserving, and managing the confidentiality, integrity, and availability of the University's information assets.
- Support the increasingly diverse students, researchers and colleagues working patterns and locations associated with a Global University.

2.2. This policy, taken together with other policies as cited in section *7 Related Policies and Procedures*, represents Keele Universities cumulative approach to Information Security.

## 3. Scope

3.1. This policy deals with information security with respect to core principles that must be observed by groups of individuals, training expectations, consequences for failure to comply with this policy and compliance with other supporting policies that create the university's approach to information security.

3.2. This policy applies to the following:

- All Students enrolled at the University.
- All Staff Colleagues employed by the University.
- Casual, temporary or agency staff colleagues working for, or on behalf of, the University.
- All contractors, consultants, and suppliers working for, on behalf of, or in partnership with the University:
    - Members of Council, governing boards and associated committees, Honorary, Emeritus, visiting persons, external partners, and associate members carrying out a function on behalf of the University, including (but not limited to): external examiners, committee lay members, sessional teachers, Sponsored IT Account holders, and recruitment agents.
- University tenants consuming University IT Facilities.

## 4. Policy

4.1. **Information Security** Principles must be used to protect information (items in bold type are referenced in *Appendix A*).

4.2. **Information Assets** means Information or data; the systems and locations in which it is stored; and how it is accessed.

4.3. **Information Asset Register** documentation should be held by all departments according to the Data Classification & Handling Policy, and the Data Protection Policy. The classification of the asset will determine the security controls that will be applied to it and how it must be handled.

4.4. An Information Asset is controlled by the **Information Asset Managers (IAMs)** as outlined in the Information Governance Framework.

4.5. **Information Asset Owners (IAOs)** have overall responsibility for specific Information Assets as outlined in the Information Governance Framework.

4.6. An Information Asset, whether electronic or in physical form, must be protected against unauthorised access using appropriate people, process, and technological controls.

4.7. Use of Generative AI tools must be conducted in accordance with current guidelines and AI Policy on PolicyZone.

4.8. Any data generated as a result of using Generative AI Tools will be considered property of the university.

4.9. An Information Asset must be available to all those who have a legitimate need to access them.

4.10. An Information Asset must be maintained so that it is accurate and complete.

4.11. An Information Asset must be deleted in a timely manner in accordance with the Records Retention Scheule.

4.12. On cessation of association with the University (paid or voluntary) all data that belongs to the University as defined in the Data Handling and Sharing Policy shall be surrendered back to the University uncopied and intact.

4.13. Upon termination of employment, or cessation of association with the University, any physical assets (e.g., Laptop, Phone) must be surrendered back to Information & Digital Services for secure redeployment or secure recycling as per the IT Asset Management Policy. Failure to comply may result in civil or criminal proceedings.

4.14. Any sharing of information must be proportionate to the defined Data Classification as defined in the Data Classification and Handling Policy.

4.15. It is the responsibility of all users of University Information Assets 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 suspension of your IT account and or disciplinary action.

4.16. All users of the University's information systems will abide by and adhere to all current UK legislation as well as regulatory and contractual requirements.

4.17. 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.

4.18. All suspected and actual information security breaches must be recorded and reported through the IT Service Desk by completing the electronic incident form. The incident will automatically be brought to the attention of the Information Compliance team who will take the appropriate actions, liaising with the IDS Cybersecurity team according to the information in the incident report.

## 5. Training

5.1. Information Security Training is mandatory for all staff or any IT account holders irrespective of role held in the university.

5.2. All users of Keele information systems shall receive information security training appropriate to their role.

5.3. IT Administrators of university systems must successfully complete the annual mandatory IT Administrator training before undertaking any administration duties connected with their role.

5.4. Information Security Training must be renewed every two years and be completed within 2 weeks of a new position undertaken by the postholder.

5.5. Information Security training completion is the responsibility of the individual.

5.6. The responsible line manager must ensure completion, considering any special circumstances for those who cannot complete the training.

5.7. The Information Security training will be provided via the chosen University platform and reviewed on a regular basis for relevancy and efficiency.

5.8. Regular phishing simulations are undertaken across all IT Account holders to train and guard against social engineering threats.

5.9. The Information Security Training Management Summary report details the percentage uptake within Faculties and Directorates and is used to maintain effective completion rates.

## 6. Roles and responsibilities

6.1. The roles expected of specific members of the University are described here for the purpose of clarity.

### 6.2. Vice Chancellor and the University Executive Committee (UEC)

- The Vice Chancellor, supported by the University Executive Committee, will ensure that the University complies with relevant legislative and contractual obligations.
- The Vice Chancellor and the University Executive Committee are responsible for the overall direction and commitment to Information Security.
- The University Executive 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.

- Chief Operating Officer will ensure development and oversight of robust incident response, and business continuity, plans.
- Deans, Directors and Line Managers will take responsibility for operational compliance within their Directorate or School.

### 6.3. Chief Information Officer

6.3.1. The Chief Information Officer (CIO), will operate as lead member of the University Executive Committee in matters relating to cyber and information security, providing leadership in ensuring an effective institutional position in respect of cyber and information security.

6.3.2. The key responsibilities of the CIO are:

- Ensures that the information security strategy aligns with the University's business objectives.
- Oversees the creation and enforcement of information security policies and procedures.
- Works closely with the Head of Cybersecurity to develop and manage the University information security program.
- Identifies and evaluates information security risks at the strategic level, implementing robust security controls.
- Ensures that risk mitigation strategies are integrated into planning and operations.
- Provides strategic guidance in high-level decision-making, including during major security incidents.
- Promoting a Security Culture and advocates for a security-first mindset across the University.
- Supports strategic training and awareness programs to reduce human-related security risks.

### 6.4. Senior Information Risk Owner (SIRO)

6.4.1. The Senior Information Risk Owner (SIRO) role 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.

6.4.2. The key responsibilities of the SIRO are:

- 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 competency and 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 the mechanism and frequency 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 Data Protection Officer, Head of Cybersecurity & Operations, and the Information Asset Owners.

### 6.5. Data Protection Officer

6.5.1. The Data Protection Officer assists the University to operate in compliance with Data Protection Legislation by improving accountability, providing advice, and helping to monitor compliance.

6.5.2. They also help implement the requirements of Data Protection Legislation across the organisation such as:

- The principles of data processing.
- Data Subjects' rights and complaints.
- Data protection by design and by default.
- Records of processing activities.
- Security of processing.
- Notification and communication of data breaches.

### 6.6. Head of Cybersecurity & Operations

6.6.1. The key responsibilities of the Head of Cybersecurity & Operations are:

6.6.1. The Head of Cybersecurity & Operations defines and maintains the security posture of the university.

6.6.2. The Head of Cybersecurity & Operations is responsible for:

- Operational Management of all aspects of cyber security institutionally.
- Creation, review and maintenance of Information Security policies and Codes of Practice.
- Monitoring and reporting on information security within the University.
- Subject matter expert contributions to and approval of, in liaison with the IDS Training Manager, the annual information security training module and phishing simulations.
- Incident management procedures for major IT incidents.
- Undertaking risk assessments of key information assets.
- Appropriate engagement events to promote information security topics.

### 6.7. Information Asset Owners (IAOs)

6.7.1 Information Asset Owners are responsible for:

- 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.

### 6.8. Information Governance Group

6.8.1. The Information Governance Group is responsible for:

- 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.

### 6.9. Deans, Heads of Schools, Directorates, Centres, Institutes, and Line Managers

- Deans, Heads of Section and Heads of Directorates, Schools, Outreach 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.
- Line managers must 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.

### 6.10. 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.
- By accessing University systems, all users are agreeing to abide by all university policies listed in section 7.
- Users are responsible for reporting any suspected security incidents immediately to the IT Service Desk or, if appropriate, to their line manager.

## 7. Related policies and procedures

7.1. The issues covered by these regulations are complex and you are strongly urged to read all associated Keele University policies and guidance.

### 7.2. Internal Keele Policy and guidance

7.2.1. All relevant documents are available on the Policy Zone:

- IT Acceptable Use Policy
- Data Classification and Handling Policy.
- Data Protection Policy.
- Clear desk and screen Policy.
- Information Governance Framework.
- Records Management Policy.
- Records Retention Schedule.
- Freedom of Information (FOI) Policy.
- Email Code of Practice.
- IT Interception and Monitoring Policy.

7.3. Details of IT related guidance can be found on the Information & Digital Services staff intranet pages.

### 7.4. UK Government Legislation

You may also wish to familiarise yourself with the following UK Government Policies:

- Computer Misuse Act 1990
- Data Protection Act 2018 (DPA)
- The Freedom of Information Act 2000 (FOIA)
- Privacy and Electronics Communications Regulations 2019 (PECR)

## 8. Review, approval and publication

8.1. This policy is owned by the Information and Digital Services Directorate and will be reviewed annually by the Head of Cybersecurity & Operations or the authorised nominee.

## 9. Approval and Publication

9.1. Approval will be secured from UEC, and Council and upon approval will reside in Policy Zone and on the Staff Intranet.

## 10. Annexes

10.1. Annexe A – Glossary of terms & definitions.

## 11. Document control information

| | |
|---|---|
| **Document Name** | Information Security Policy |
| **Owner** | Head of Cybersecurity & Operations, Information & Digital Services. |
| **Version Number** | 2 |
| **Equality Analysis Form Submission Date** | 14/08/2025 |
| **Approval Date** | 25 September 2025 |
| **Approved By** | Council |
| **Date of Commencement** | 25 September 2025 |
| **Date of Last Review** | 25 September 2025 |
| **Date for Next Review** | 25 September 2026 |

| | |
|---|---|
| **Related University Policy Documents** | [List all applicable] |
| *For Office Use – Keywords for search function* | |

## Annexe A – Glossary of terms & definitions

| Term | Definition |
|---|---|
| **Information Asset** | Information or data; the systems and locations in which it is stored; and how it is accessed. |
| **Information Asset Owner (IAOs)** | Senior member of staff of Directorate / Faculty who has overall responsibility for specific Information Assets and who ensures that those assets are handled and managed appropriately, protected against risk and their value to the organisation is recognised. |
| **Information Asset Register** | An Information Asset Register documents the types of information held by an organisation with the purpose of helping it to understand and manage its Information Assets (e.g. identify duplication, increase business efficiency, and manage risks). |
| **Information Asset Manager (IAMs)** | The IAM's role is to be responsible for the maintenance of Information Asset Registers in their area, to raise any information management issues and risks to the IAO, monitor completion of mandatory Information Security training and to ensure staff are aware of best practice and compliance requirements. |
| **Information Governance** | Comprises Information Management and Information Security: set of multidisciplinary structures, policies, procedures, processes, and controls required to manage information in support of an organisation's regulatory, environmental, operational and risk requirements. It allows organisations to ensure information is processed lawfully, securely, efficiently, and effectively. |
| **Information Security** | The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction, including from cyber-attacks, to ensure confidentiality, integrity and availability. |
| **Privacy and Electronics Communications Regulations 2019 (PECR)** | Regulations which give people specific privacy rights in relation to electronic communications including specific rules on:<br>• Marketing calls, emails, texts, and faxes<br>• Cookies (and similar technologies)<br>• Secure communications.<br>• Privacy as regards traffic and location data, itemised billing, and directory listings. |
| **Subject Access Request (SAR)** | A request made for an individual's own Personal Data, or someone acting on their behalf with their permission, under the UK GDPR Article 15 |
| **Data Protection Act 2018 (DPA)** | Regulates the Processing of information relating to individuals, including the holding, obtaining, recording, use or disclosure of such information. The UK's Data Protection Act 2018, which supports and should be read in conjunction with the UK General Data Protection Regulation (UK GDPR). |
| **Data Protection Legislation** | The UK General Data Protection Regulation (UK GDPR) and UK Data Protection Act 2018 (DPA). |
| **UK GDPR** | UK GDPR means the European Union General Data Protection regulation (EU GDPR) as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 and sits alongside an amended version of the Data Protection Act 2018 (DPA). The UK GDPR is a legal framework that sets out principles for the collection and processing of personal information. |