UNIVERSITY OF SUSSEX

IT Services

INFORMATION SECURITY POLICY

1. OVERVIEW AND PURPOSE

1.1 The University of Sussex's Information Technology Services (ITS) underpin almost all of the University's key activities and are essential to the University's primary purpose, i.e. to advance learning and knowledge through teaching and research for the benefit of the wider community.

1.2 It is crucial that University staff, students, and others working with the University have access to the information and/or technology they require in order to carry out their work and study.

1.3 The University also acknowledges that the information it holds and processes, and systems and devices used to carry out work and study, must be appropriately secured in order to meet relevant legal and compliance obligations, and to protect the reputation and integrity of the institution.

1.4 As such, appropriate and necessary information security[1] measures must be in place and their effectiveness must be monitored accordingly, in order to maintain business continuity and ensure compliance, and to enable adherence to other relevant policies, standards and procedures.

1.5 The aim of this policy is to outline the principles and framework in place to manage and implement information security across the institution, to make clear responsibilities in relation to information security at all levels within the University, and to promote a 'security aware' culture.

2. SCOPE

2.1 This policy applies to all users of University information and University Information Technology Services[2] including software, computers and/or networks, whether on-campus, via remote connections or in cloud services.

2.2 For the purposes of this policy, 'all users' includes the following, whether remunerated or not:

- Students (any person enrolled on a course or module of study at the University);
- Employees (whether permanent, fixed-term, temporary or casual);
- Contract, seconded and agency staff;
- Volunteers, apprentices, and interns; and

[1] Preservation of confidentiality, integrity and availability of information

[2] 'University information and Information Technology Services' refers to any digital information or service provided or procured by the University and accessible through the University networks or over the Internet

- Others associated with (i.e. performing services for or on behalf of) the University (for example, Emeritus Professors, agents and consultants).

2.3 Use of devices not owned or supplied by the University are also covered when connected in any way to University-provided Information Technology Services.

2.4 This policy underpins the University's suite of other technical and information security-related standards and processes; these documents and additional guidance linked at the end of this policy must all be considered in conjunction with this policy.

3. RESPONSIBILITIES

3.1 All Users

3.1.1 All users (as defined in section 2.2 of this policy) must comply with this policy as well as related information security codes of practice and procedures and for completing any mandatory information security training provided by the University.

3.1.2 All users must report any information security-related risks and issues they become aware of via the appropriate route(s), as outlined in this policy and/or other related policies, codes of practice and procedures.

3.1.3 Where users are also owners or administrators of specific platforms or systems used at the University, they are also responsible for ensuring that these are managed securely and appropriately, in accordance with this policy – e.g. that access is only provided to those for whom it is required.

3.2 Pro-Vice Chancellors, Executive Deans and Professional Service Directors

3.2.1 Pro-Vice Chancellors, Executive Deans and Professional Service Directors shall drive a culture that values, protects and uses information for the benefit and success of the University, its staff and students.

3.2.2 Pro-Vice Chancellors, Executive Deans and Professional Service Directors shall ensure that staff within their Faculty or Division are aware of this policy.

3.3 Chief Digital and Technology Officer (CDTO)

3.3.1 The CDTO has overarching accountability for performance, security, and availability of technology services provided across the University.

3.3.2 The CDTO is responsible for ensuring that information security risks and recommended mitigations are recorded and maintained on the risk register.

3.3.3 The CDTO may delegate day to day responsibility for the multiple facets of information security and related matters to the IT Leadership team (i.e. Assistant Directors within ITS) and directly to the Cyber Security Team.

3.4 **Senior Information Risk Officer (SIRO)**

3.4.1 The SIRO must be informed by the CDTO of any significant cyber security incidents or events.

3.5 **Cyber Security team**

3.5.1 The Cyber Security team must maintain the University's security posture in alignment with its defined risk appetite and for safeguarding University data from unauthorised access.

3.5.2 The team advises the University on information security matters and monitors the adoption of information security-related standards. They also identify, analyse, and manage potential cyber threats, working closely with technical colleagues to provide expert advice on risk mitigation.

3.5.3 Additionally, the team develops and maintains cyber security training materials to promote awareness and best practices across the University.

4. **POLICY**

4.1 **Information Security Principles**

4.1.1 The University must protect information assets through consistent application of a process of risk assessment and the implementation of appropriate controls[3] to manage and mitigate risk and ensures compliance with all statutory, regulatory and contractual requirements.

4.1.2 The University must ensure that information is handled legally, securely, efficiently and effectively when using all technology, including generative and other forms of AI, automation and emergent technologies that process and/or transfer information to third-party services or platforms. Where used, these technologies and services must be deployed in a manner that does not put at risk the University's information assets or expose the University to an increased risk of cyber-attack and disruption.

4.1.3 Information must be appropriately secured, in accordance with the University's Statement of Risk Tolerance and Appetite, in order to protect the University and its stakeholders from the consequences of unauthorised access or disclosure, and specifically the consequences of breaches of confidentiality, failures of integrity or interruption to the availability of information.

4.1.4 The University will ensure that all users have access to the information and/or information technology services they require in order to carry out their studies or work and will facilitate appropriate training and support to ensure that they are able to adhere to their information security responsibilities.

4.1.5 Information security incidents, including but not limited to suspicious activity, data loss, suspected account compromise or lost / tampered equipment, will be

[3] A measure that is modifying risk

effectively managed by IT Services and resolved, lessons identified will be implemented to continuously improve information security controls and maturity.

4.2 **Organisation and Governance**

4.2.1 An appropriate framework, detailing roles and responsibilities, is maintained by IT Services to manage, oversee and monitor compliance with information security requirements.

4.2.2 Security controls must be put in place to ensure that confidentiality[4], integrity[5] and availability[6] of information is assured.

4.2.3 Controls should be commensurate with risk but must always adhere to minimum standards set by University policies, codes of practice, procedures, legal and regulatory standards.

4.2.4 Security controls must be maintained when information is taken off site, accessed whilst off-site or accessed using mobile technologies regardless of who owns the device.

4.2.5 All information security measures will be reviewed and tested on a regular basis via relevant methods and as required, including – where appropriate – the use of internal audits.

4.3 **Training, Awareness and Personnel**

4.3.1 In addition to the mandatory e-learning to be completed by staff, other training and education campaigns will be delivered to support effective information security across the University. This will be delivered in collaboration with HR and other relevant teams to maximise effectiveness of these training & awareness activities.

4.3.2 Information security awareness and education campaigns will be delivered throughout the year and measured for effectiveness in order to deliver continuous improvement.

4.3.3 Users that hold specific responsibilities for security will have role specific information security training, as required.

4.4 **Risk and Asset Management**

4.4.1 Information security risks must be managed in accordance with the University's Risk Management Framework.

4.4.2 Appropriate risk assessments will be carried out for information and IT assets to determine the level of control required to keep risks within acceptable levels. The CDTO, in consultation with the SIRO, will determine the most appropriate person to review and approve the risk assessment.

[4] Non-public information is only available to authorised users
[5] Information is complete, accurate and fit for purpose
[6] Information is available when and where it is needed

4.4.3 Risk assessments will be included in the business case for any new IT systems and will be repeated periodically and when significant changes occur.

4.4.4 Identifying and implementing security controls will be achieved by an appropriate mix of risk assessments, policies, standards, guidelines, technical measures, training, support, audit and review.

4.4.5 Consideration must be given to procedures relating to the classification and handling of information and access to information assets managed accordingly, i.e. on the basis of the relevant classifications.

4.5 **IT Security and Access Control**

4.5.1 Digital services must be protected by appropriate technical measures, as defined by the University.

4.5.2 Cyber security and the management of security vulnerabilities must be integrated into each phase of the IT product or service life cycle, from the initiation of a project to develop or procure a system to its maintenance and de-commissioning/disposal, with the identification of whole life costs as part any hardware or software refresh cycles.

4.5.3 Access to systems and information assets must be restricted to authorised users for appropriate and authorised activities only in accordance with organisational requirements. Access will be granted on a least privilege[7] basis.

4.5.4 Appropriate mechanisms and processes must be implemented by system owners and suppliers in order to detect unauthorised access, modifications or malicious behaviour.

4.5.5 Accounts must be appropriately deprovisioned upon termination and user accounts will be reviewed regularly.

4.5.6 The University will ensure that its information technology services, third party arrangements and information sharing are designed, configured and facilitated with sufficient and appropriate measures implemented to minimise the risk of information security breaches.

4.6 **Third Party Security**

4.6.1 The information security position of vendors and third-party service providers must be assessed to ensure that information and personal data remain secure and adequately protected, and the University is able to meet relevant legal and compliance obligations.

4.6.2 Due diligence checks and information security risk assessments must be carried out for all procurements of digital, data and technology products and services.

[7] Privilege is the concept of only allowing users to do certain things. For example, a standard user is typically prevented from changing operating system files, while a system administrator is typically permitted to do so, because this is part of maintaining a computer system.

4.6.3 A record of third-party service providers and risks will be maintained by the contract owner and this information must be made available for periodic compliance checks of third parties against the University's security requirements.

4.6.4 When transferring information to third parties (including use of cloud or third party hosted services by individual users), relevant policies, standards and legislation must be adhered to, and this must be authorised at an appropriate level, i.e.:

- The appropriate data sharing agreement and/or contract clauses must be in place and reviewed accordingly by relevant colleagues (e.g. Data Protection Officer, Office of the General Counsel, IT Services); and

- Minimum agreed levels of security controls must be maintained.

4.7 **Physical Security**

4.7.1 The University campus and IT facilities must be protected by appropriate environmental and physical security arrangements.

4.7.2 Assurances that appropriate arrangements are in place will also be required where third parties have responsibility for hosting or processing University information held physically.

4.8 **Incident Management**

4.8.1 Information security incident management tools must be implemented by Cyber Security team and system owners (as appropriate) to ensure incidents are detected, reported, investigated and appropriately managed.

4.8.2 All incidents involving actual or suspected/potential breaches of information technology security must be reported immediately to the IT Service Desk through any available channel so they can be reviewed as soon as possible.

4.8.3 An incident response will be triggered following a triage procedure and in accordance with the University's emergency response plans and processes.

4.8.4 Information security breaches involving personal data[8] must be reported to the University's Data Protection Officer via the University's published personal data breach reporting process(es).

4.8.5 The IT Services teams will investigate all security incidents and take appropriate action in accordance with this and other relevant policies, standards, procedures, University Regulations, legal and regulatory requirements.

4.9 Breach of this policy

4.9.1 Any suspected or actual breach of this policy or related Codes of Practice must be reported to the CDTO who will take appropriate action and inform the relevant internal and external authorities.

[8] Personal data refers to any information relating to an identified or identifiable living individual.

4.9.2 Where there is a deliberate misconduct or behaviour amounting to wilful breach of this policy, or gross negligence causing a breach of the policy, the matter may be considered under the University's disciplinary procedure.

4.9.3 University policy is that activity which relates to the prevention or detection of crime or breaches legal or regulatory or compliance standards will be referred to the Police, or supervisory and regulatory bodies as required.

5. LEGISLATION AND GOOD PRACTICE

5.1 The Committee of University Chairs Higher Education Code of Governance requires that effective arrangements are in place for the management of information and to meet all relevant legal and regulatory requirements. Similarly, the Office for Students identifies Public Interest Governance Principles that include accountability and risk management and are applicable to information governance.

5.2 The University is also responsible for complying with relevant UK legislation, including data protection legislation, the Freedom of Information Act 2000 and the Counter-Terrorism and Security Act 2015 (i.e. its Prevent Duty[9]).

5.3 The Janet Network connects education and research organisations in the UK (including universities) to each other, as well as to the rest of the world. Users of the University of Sussex's network must also abide by the regulations outlined in the Janet Acceptable Use Policy. Non-compliance with Janet regulations by University users could result in access to this service being suspended or withdrawn completely for the entire institution.

[9] The Prevent Duty aims to safeguard people from becoming terrorists or supporting terrorism. The University's obligations include having suitable IT policies and procedures in place to meet the requirements of the Duty

Review / Contacts / References

Policy title:	Information Security Policy
Date approved:	October 2025
Approving body:	Vice-Chancellor via UEB
Last review date:	October 2025
Revision history:	Version 6.4 – October 2025 Version 6.3 – October 2025 Version 6.2 - September 2023 Version 6.1 – June 2022 Version 6.0 – April 2022 Version 5.0 – October 2021
Next review date:	October 2028 (or sooner, if required)
Related internal policies, procedures, guidance:	Regulations of the University Information Security: Codes of Practice Roles and Responsibilies RACI Data Protection Policy Personal data breach reporting process Information Classification and Handling Records Management Risk Management Policy Payment Card Industry Data Security Standard Compliance Requirements Finance System Access Requirements Information on counter-terrorism safeguards (Prevent Duty)
Division:	IT Services
Policy Owner:	Chief Digital and Technology Officer, IT Services
Point of Contact:	Cyber Security Manager, IT Services