Information Security Policy	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Data - Chief Operating Officer - Compliance Committee
Associated Policy Statements:	
Authorised Owner:	Head of Information Security
Authorised Co-ordinator:	Lead Information Security Assurance Specialist
Effective date:	13/07/2022
Due date for full review:	14/07/2024
Sub documentation:	Information Security Policy Framework Data Protection Policy Acceptable Use Policies Statement Using Your Own Applications and Devices Policy Terms of Reference: Compliance (Data) Committee

Approval History

Version	Reason for review	Approval Route	Date
0.1	First draft		8/10/2013
0.2	Second draft		22/10/2013
0.3	Third draft – EB Feedback	Executive Board Committee (or other)	11/02/2014
0.4	Annual review (2016) inclusion of mandatory training and other minor revisions		10/10/2016
0.5	Annual review. Updates to include reference to data strategy, GDPR and CRAIC protocol	Information Security and Governance Group	4/12/2017
0.6	Annual review, minor tweaks	Data and InfoSec Steering Committee	16/12/2019
0.7	Minor updates	Executive Board	31/11/2020
1.0	Review and re-write.	Compliance (Data)	13/07/2022

1. Purpose

This document forms the University of Surrey's Information Security Policy. It sets out the framework within which the University will manage the security of the information for which it is responsible, maintaining an appropriate balance between accessibility and security.

1.1. The University recognises the need for its staff to have access to the information they require in order to carry out their work.

1.2. The University also recognises that the information it manages must be appropriately secured in order to maintain its reputation for trustworthiness, to protect the institution from the consequences of breaches of confidentiality, failures of integrity or interruption to the availability of that information, and to comply with the law and to comply with contractual agreements.

1.3. This policy complements and supports existing IT Policies found here: https://portal.surrey.ac.uk/https/surreynet.surrey.ac.uk/staff-services/it-services/cyber-security-and-it-policies

2. Scope and Exceptions to the Policy

This policy applies to:

2.1. All information for which the University has a legal, contractual or compliance responsibility, whether that information is stored or processed electronically or by other means (the Information).

2.2. The equipment, systems, credentials, etc. that are used to access the Information, safeguard Information Security, or could have some bearing on Information Security (the Information Systems).

2.3. All staff or any other person or organisation having access to the Information or Information Systems.

2.4. This policy is concerned with the confidentiality, integrity and availability of the Information (the Information Security).

Exceptions to this Policy:

2.5. The principles of information security are underpinned by legislation and the consequences of a serious breach of information security are severe. Therefore, exceptions to the principles outlined in this policy are not expected to be allowed. In highly exceptional cases, and with a very high level of justification, any request to relax the normal information security requirements may be subject to a risk assessment and must be authorised in writing by the Chair of Compliance (Data) committee.

3. Definitions and Terminology

Information security	the preservation of confidentiality, integrity and availability of information.
Information	data which has meaning.
Information asset	all data with meaning that can be exploited to advance the University's objectives or confer competitive advantage.
CSIRT Protocol	the University's protocol to manage the initial response to actual or suspected data and security breaches.
Processing	means any operation on data, including organisation, adaptation and alteration; retrieval, consultation or use; disclosure, transmission, dissemination and otherwise making available; or alignment, combination, blocking, erasure and destruction. Processing includes the sending of information via email and other mechanisms such as instant messaging and social media.

4. Policy Principles

The following key principles underpin this policy statement.

4.1. The University will maintain an appropriate balance between convenient access to information and security of that information which will be a critical element of the University's management systems.

4.2. The level of Information Security to be applied in individual circumstances shall be driven primarily by the Classification of the Information concerned and consideration of the risks involved.

4.3. University information will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.4. This shall be achieved by an appropriate mix of policies, standards, guidelines, technical measures, training, support, audit and review.

4.5. This policy is the primary policy under which all other technical and security-related polices reside.

4.6. Training in the fundamentals of Information Security shall be mandatory for all staff and other people with access to University Information.

4.7. Information Security risks shall be assessed continuously and recorded in the appropriate University Risk Registers. This shall include measures such as, but not limited to, internal and external review, audit and penetration testing.

4.8. Significant residual risks to University information will be escalated to risk owners, and via Compliance (Data) committee as required.

Procedures:

4.9. All staff shall follow University policies and system instructions to ensure that no breaches of information security result from their actions.

4.10. All staff shall report any actual or suspected data or security breaches to their line managers, IT support or the Information Compliance Unit (ICU) as soon as possible. Any response will then be managed according to the Cyber Security Incident Response Team (CSIRT) Protocol.

4.11. All staff shall retain data in accordance with the Data Protection policy and the provisions of the Data Management Strategy. Particular consideration should be given to the classification of data 3 (confidential, restricted or unrestricted) and the consequent access granted to colleagues, students or third parties.

4.12. IT Services shall provide appropriate technical measures to ensure digital data is secured for its confidentiality, integrity and availability; and guidance for staff to ensure the measures are effective.

4.13. The University shall provide adequate Information Security training and guidance for all staff appropriate to the information security risks involved in their roles. This training is mandatory.

4.14. The University shall provide adequate data retention capacity and technical security measures to enable staff to comply with the published data retention schedules and other system specific information security requirements.

4.15. Professional Services Department Heads and Directors of Faculty Operations shall ensure that adequate departmental business continuity arrangements are in place in their departments to prevent failures of compliance, operational disruption or reputational damage following an information security incident.

4.16. Professional Services Department Heads and Directors of Faculty Operations shall ensure that all equipment capable of storing or transmitting data is held securely and that the risk of theft or misuse is minimized.

4.17. The University shall ensure that its systems, networks, databases and third-party arrangements are designed and installed with appropriate measures implemented to prevent information security breaches.

4.18. The University shall prepare, test, publish and occasionally review protocols for responding to suspected information security breaches.

Detailed procedures for achieving appropriate standards of information security are included in the subordinate policies making up the Information Security Policy Framework. See supporting documentation for more details.

Roles & Responsibility:

Compliance (Data)	Overall responsibility for the University's strategic plans for information security rests with the Senior Information Risk Owner as Executive Board member serving as the Chair of Compliance (Data). Compliance (Data) will supervise the development of an appropriate policy framework and suitable operational procedures to comply with all the principles detailed in section 2.1.
Head of information Security	The Head of Information Security is responsible for ensuring that the arrangements for governing the scoping, development, implementation and maintenance of University IT systems, networks and databases comply with the principles of good information security.
Data Protection Officer	The Data Protection Officer ensures that policies, procedures, and information governance frameworks and training are in place to address the obligations of the organisation to data subjects
System Owners	System owners are responsible for ensuring that IT systems they manage are configured appropriately and used effectively to ensure that the risks of an information security incident are minimised. These owners are assumed to be responsible for the organisational and technical measures necessary to ensure that good information security practice is built into their system's day to day operation.
Line Managers	To ensure that their staff are aware of the Policy, the IT Acceptable Use Policy, and any other Information Security Policies relevant to their work. To ensure that staff and other people with access to personal data and sensitive Information undertake the Information Security training at the earliest opportunity. To ensure that the business processes and practices in their areas comply with the Information Security Policies.
University Staff	To comply with the Information Security Policy and supporting related policy documents, including the Acceptable Use Policies Statement. To complete all required training and follow related policies and guidance. To report any breaches or suspected breaches of Information Security in accordance with the Information Security Incident Response Policy. To inform ITS of any potential threats to Information Security.

5. Governance Requirements

5.1. Implementation: Communication Plan

5.1.1. As this policy sets out overarching responsibilities, definitions and principles of the University's approach to information security, its implementation will be limited to awareness raising via the Leaders' Alert communication channel and publication on SurreyNet/MySurrey. The related policy framework and detailed subordinate policies will be implemented via a range of methods to be determined separately. (see Information Security Policy Framework).

5.2. Consequences of Non-Compliance

Failure to comply with this policy can lead to:

5.2.1. Damage and distress being caused to those who entrust us to look after their personal data, risk of fraud or misuse of compromised personal data, a loss of trust and a breakdown in relationships with the University.

5.2.2. Damage caused by unavailability, inaccessibility or corruption of University information assets.

5.2.3. Damage the University's reputation and its relationship with its stakeholders (including research funders and prospective students and collaborators).

5.2.4. Significant legal and financial consequences. Monetary penalties of the Information Commissioners Office can reach up to 20 million euros or 4% of turnover. Individual civil action for breaches of data protection can also be taken by individuals.

5.2.5. Failure to comply with this policy may result in revocation of your access to the University's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether or not the breach takes place at your normal place of work.

5.3. Review

This policy will be reviewed biennially or as necessary.

Minor changes which do not change the meaning of the policy, will be proposed to the Compliance (Data) committee before being implemented.

Major changes that alter the meaning of the policy or significant re-writes will be considered by the Compliance (Data) committee.

5.4. Legislative Context and Higher Education Sector Guidance or Requirements

The following legislation is, or may be, relevant to information security:

- The General Data Protection Regulation 2016/679
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Computer Misuse Act 1990
- The Counter Terrorism and Security Act 2015 (in particular the 'prevent duty')
- The Payment Card Industry Data Security Standard (PCI DSS)
- Copyright, Designs and Patents Act 1988

6. Stakeholder Engagement and Equality Impact Assessment

6.1. Equality: The University is strongly committed to equality of opportunity and the promotion of diversity for the benefit of all members of the University community. The University's approach is to promote equality across the full range of its activities, in employment, teaching and learning and as a partner working with and within local, national and international communities. Equality Analysis is a process which examines how the impact of the policy has been considered on the diverse characteristics and needs of everyone it affects. This policy has been reviewed and no negative impact on equality has been identified.

6.2. Health & Safety: This policy is unlikely to have direct Health & Safety implications. For further information, please see the University Health & Safety policy.