Information Security Policy

Operational Owner:	Chief Information Security Officer
Executive Owner:	Chief Operating Officer
Effective date:	30/11/2020
Review date:	30/11/2021
Related documents:	Information Security Policy Framework Terms of Reference: Information Security and Governance Group

Approval History

Version	Reviewed by	Brief reason for review	Approved by	Date
0.1	James Newby	First draft		8/10/2013
0.2	James Newby	Second draft		22/10/2013
0.3	James Newby	Third draft – EB Feedback	Executive Board Committee (or other)	11/02/2014
0.4	James Newby	Annual review (2016) inclusion of mandatory training and other minor revisions		10/10/2016
0.5	James Newby	Annual review. Updates to include reference to data strategy, GDPR and CRAIC protocol	Information Security and Governance Group	4/12/2017
0.6	Eddy Donald	Annual review, minor tweaks	Data and InfoSec Steering Committee	16/12/2019
0.7	Nicola Orpin	Minor updates	Executive Board	31/11/2020

1 Introduction

The University's information is an important asset. It must be protected from the consequences of breaches of confidentiality, failures of data integrity and interruptions to its availability. The University must therefore take appropriate organisational and technical measures to protect its information.

1.1 Purpose

1.1.1 This policy provides the management direction to ensure that information security is considered appropriately and embedded into all University processes and systems and that individual responsibilities for achieving adequate levels of information security are established. The policy aims to minimise potential damage to the University by reducing the number and impact of information security incidents. The measures set out in this policy, including training requirements, are mandatory.

1.2 Scope

1.2.1 The policy provides a high-level overview of the definitions, management responsibilities and principles of good information security practice. It therefore focuses on the high-level measures required to achieve adequate information security. More detailed organisational and technical requirements will be set out in subordinate policies designed to deal with specific aspects of information security. Detailed procedures for complying with the provisions of this policy are therefore not included but will be covered by the subordinate policies included in the Information Security Policy Framework.

1.3 Definitions

1.3.1 **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.

System owner: Head of Department or Director of Faculty Operations with prime responsibility for managing and maintaining an information system, database or network; this includes the day to day operation of that system.

CSIRT Protocol – The University's protocol to manage the initial response to actual or suspected data and security breaches

2 Policy

2.1 Policy Principles

2.1.1 All information for which the University is responsible shall be appropriately secured to protect against the consequences of breaches of confidentiality, failures in data integrity or interruptions to availability and to protect it against damage, loss or misuse. Consistent with this principle:

- All staff shall follow University policies and system instructions to ensure that no breaches of information security result from their actions
- 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 the Cyber Security Incident Response Team (CSIRT) Protocol
- 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

(confidential, restricted or unrestricted) and the consequent access granted to colleagues, students or third parties.

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

2.2 **Procedures**

2.2.1 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.

3 Governance Requirements

3.1 Responsibility

3.1.1 Overall responsibility for the University's strategic plans for information security rests with the Executive Board member serving as the Chair of the Data and InfoSec Steering Committee (DISC). The DISC will supervise the development of an appropriate policy framework and suitable operational procedures to comply with all the principles detailed in section 2.1.
Detailed responsibilities for delivering each aspect of the information security principles outlined in section 2.1 will be incorporated into the various related policies and procedures making up the Information Security Policy Framework. The following responsibilities for information security principles apply:
• The Chief Information Security Officer 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.
• 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.
• All staff who are users of information systems must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects its confidentiality, integrity and availability. This includes engaging with University provided information security training.

3.2 Implementation / Communication Plan

3.2.1 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 SurreyLife. 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)

3.3 Exceptions to this Policy

3.3.1 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 the Information Security Steering Group.

3.4 Review and Update

3.4.1 The policy will be reviewed annually or as necessary.

Minor changes which do not change the meaning of the policy, will be proposed to the Data and Infosec Steering Committee (DISC) before being implemented.

Major changes that alter the meaning of the policy or significant re-writes will be considered by the Data and Infosec Steering Committee (DISC)

3.5 Legislative context

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

Data Protection Act, 2018 and the
General Data Protection Regulation
Computer Misuse Act 1990
Copyright, Designs and Patents Act, 1988

3.6 Stakeholder Statements

3.6.1 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.

3.6.2 Health & Safety:

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

3.6.3 Other: