INFORMATION SECURITY POLICY

1. Introduction

1.1. Information[1] underpins all the University's activities and is essential to the University's objectives. It exists in many forms, both electronic and physical, and is stored and transmitted in a variety of ways using university owned systems and those owned privately or by other organisations. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

1.2. The University supports its members, employees and visitors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this. Information security is characterized here as being concerned with guaranteeing availability (ensuring that authorized users always have access to information when they need it); integrity (safeguarding its authenticity, accuracy and completeness); confidentiality (ensuring that sensitive information is accessible only to those authorized to use it); and disposal (ensuring proper methods of disposal of information that is no longer required).

1.3. Security of information must therefore be an integral part of the University's management and business processes, and a primary consideration for its management structure in order to maintain continuity of its business, legal compliance and adhere to the University's own regulations and policies.

1.4. The information Security policy underpins the University of Kent's charter and strategy and supports the University's large and diverse populations who have evolving requirements for information handling and processing.

2. Scope

2.1. This policy applies to all members of the University and others who handle university managed information including staff, students, contractors, consultants, and visitors of the University;

2.2. The policy relates to information managed or associated with the University whether it is being stored or processed using University facilities including its accommodation, equipment, computers and networks, or privately owned equipment or that owned by other organisations;

2.3. The policy covers all information management and processing activities whether they are undertaken on or off campus and however the information is being accessed.

[1] Information is taken to include knowledge and data for which the University has some responsibility or association either directly or through the actions of its members including staff and students. This includes information that can be linked to the University and also private information that individuals may from time to time store at the University or on university systems.

3. Policy

3.1. It is a primary principle of this policy that the information managed by the University of Kent shall be appropriately secured in order to protect the institution from the consequences of breaches of confidentiality and failures of integrity or interruption to the availability of that information while allowing members of the University to have access to the information they require in order to carry out their work.

3.2. This principle will be supported by the provision of an appropriate mix of policies, standards, guidelines, technical measures, training, support, audit, and review.

3.3. This policy is the primary policy through which related polices are referenced (Schedule 1). This document, together with subsidiary and related policies and implementation documents comprise the University's Information Security Policy.

3.4. Responsibilities and duties for users of university information are set out in section 5. Students or staff who act in breach of this policy or are negligent in their responsibilities to enforce it may be subject to HR disciplinary or HR capability procedures. In serious cases failure to comply with the security policy may be grounds for exclusion from studies or for dismissal from employment as set out in relevant HR policies.

4. Responsibilities for Information Security

4.1. Council:

- Authorise the Information Security Policy and subsidiary policies.

4.2. Senate:

- Review and renew every three years this Information Security Policy.
- Review regularly and renew the Information Security subsidiary policies.

4.3. Information Services Board:

- Overall management of the implementation of the Information Security Policy and subsidiary policies.
- Propose changes to the Information Security and subsidiary policies as necessary
- Ensure that Information Systems within the University are implemented and maintained in such a way as to support the Information Security Policy.
- Ensure that regular, independent audits of the implementation of the Information Security Policies are undertaken and appropriate actions are taken to correct any deficiencies found.

4.4. Director of Information Services:

- Ensure that there is broad awareness of information security across the university and that appropriate resources including information and advice are available as required on Information Security matters.
- Investigate any reported Information Security incidents or risks and respond appropriately.
- Authorise access to private information stored on University owned systems and services for operational reasons.
- Undertake risk assessments of information systems to determine the probability and impact of security failures, and recommend appropriate mitigation.

4.5. Academic Registrar:

- Authorise legal access to users' private information held or stored by the University in order to investigate suspected breaches of University Regulations or the law.
- Ensure that all students are made fully aware of the Information Security and subsidiary policies.

4.6. University Officers, Heads of Schools, Directors of Professional Services Divisions, and Line Managers:

- Ensure that all information in their area is managed in conformance with this Policy.
- Make themselves familiar with risk assessments for the information systems used within their area of responsibility, and ensure that relevant mitigation measures are implemented as appropriate.
- Ensure that all staff, contractors and visitors are made fully aware of the Information Security and subsidiary policies, and are given appropriate support and resources to comply.

4.7. Staff and Students and other users of the University's systems / information:

- To apply the principles of information security set out in section 3 and comply with the Information Security and subsidiary policies.
- Report any Information Security incidents or risks to the Director of Information Services.

November 2016

Ownership

Owner	Department / Team
John Sotillo	Information Services

Author

Author(s)	Department / Team
Matthew Trump John Sotillo	Information Services

Contributors and Reviewers

Contributors / Reviewers	Department / Team
Juliette Pattinson; Frank Richardson; Mark Ellis; Jayne Hornsby; David Hayling; Matthew Trump; Richard Jones	Information Security Working Group

Revision History

Version	Status	Date Issued	Reason for issue	Issued by
4D	Draft	26/04/2016	Working party review	JPMRS
5D	Draft	09/05/2016	Revision following Working Group comments and issue to User groups for comment	JPMRS
1	Recommended	25/08/2016	Revised following ISB feedback	JPMRS
1.1	Published	23/11/2016	Senate approved, including Senate recommendation to reduce review period to three years.	DHH

Schedule 1

The following list are examples if subsidiary and related policies which will form part of the Information Security Policy:

Direct subsidiary policies

- Use of IT Regulations
- Acceptable Use Policy
- Regulations for Use of Information Technology
- Staff Desktop Policy
- Bring Your Own Device Policy
- Systems Management Policy
- Third Party Access Policy
- Information Handling Policy
- Cryptography Policy
- Software Management Policy
- Institutional Access Policy
- Operation Policy (ISP11)
- Account Management and Authentication Policy
- Network Management Policy
- Software Copyright Policy

Supporting and referenced policies

- Workstation Disposal Policy (part of WEEE)
- Data Protection Code of Practice
- Records Management Policy