# Information and Communications Security Policy

## Contact Officer

*Head of ICT Services*

## Purpose

This policy outlines the key principles that the University holds in relation to maintaining the security of its information and communications systems and technology.

## Overview

Information is a key resource without which virtually all of our activities would cease. It is recognised therefore that the University must do all it can to protect its information assets. We aim to do this in ways that are appropriate and cost effective.

This security policy aims to help enable us to fulfil our responsibilities and to ensure that a high quality service can continue to be offered to our staff, students and other clients.

The main aim of the Security Policy is to protect the University from security problems that might have an adverse impact on our operations and our professional standing.

Security problems can include questions of confidentiality (data management), integrity (information being accidently or deliberately altered without permission) and availability (information not being available when it is required). For the purpose of this policy statement the widest possible definition of security will be used to include all types of incident that might have an impact on the effective use of information, including performance, consistency, reliability, accuracy and timeliness.

## Scope

This policy applies to all members of the University, including students and staff. The scope of this policy document covers use of information both upon paper and via access to electronic records.
The Policy

Responsibilities

The University will:

a. Use all reasonable, appropriate, practical and effective security measures to protect its business processes and information assets from inappropriate use.

b. Continually examine ways in which it can improve the use of security measures to protect and enhance its business interests.

c. Protect and manage its information assets in such a way as to comply with its contractual, legislative, privacy and ethical responsibilities.

and:

a. Will respect the concept of academic and individual freedom, but will expect its Users to ensure that colleagues and the University are not disadvantaged or penalized by inappropriate information security actions.

b. Will endeavour to ensure that sufficient resources are made available for the achievement of the objectives of this Security Policy.

Information Users:

a. Have an obligation to protect the University’s information assets, systems and infrastructure. They must, at all times, act in a responsible, professional and security-aware way, maintaining an awareness of and conformance to this Policy.

b. Must protect the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations.

c. If intending to access Information via electronic means, must register with Information and Learning Services and give their informed agreement to comply with relevant regulations including the JANET acceptable use policy.

d. Are responsible for identifying security shortfalls in existing security practices and/or improvements that could be made.

Good Practice Principles

1. Using risk analysis techniques the University will identify its security risks and their relative priorities, responding to them promptly and confidently, implementing safeguards that are appropriate, effective, culturally acceptable and practical.

2. To promote better sharing and exploitation of information, all Users will have access to appropriate internal information, including overall guidelines to the security measures employed, wherever possible.
3. All Users will be accountable for their actions and all actions will be attributable to an identified individual.

4. All information (including third party information) will be protected by safeguards and handling rules appropriate to its sensitivity and criticality.

5. Information owners will generally be responsible for identifying to whom their information may be released. On occasions, current legislation or contractual obligations may require its disclosure to authorised external bodies such as the police or JANET Computer Emergency Response Team (CERT).

6. The University will seek to ensure that its activities can continue with minimal disruption, or other adverse impact, should it or any of its locations or services suffer any form of disruption or security incident.

7. Actual or suspected security incidents must be reported promptly to a member of ILS.

8. Documented procedures and standards, along with education and training as appropriate, will supplement this Policy.

9. Effectiveness will be measured by the University’s ability to avoid security incidents and minimise resulting impacts.

10. All Users are responsible for identifying ways in which the Security Policy might be improved. Suggestions for improvement should be sent to the Head of ICT.

Policy Awareness

A copy of this Policy will be made available to all staff and students. Individual sections of the Policy will be updated as required and will be available on the University's website. All Users are expected to be familiar with, and to comply with, the Security Policy at all times.

Applicability and Enforcement

This Policy applies to all Users and those who use its facilities and information. Compliance with the Policy will be part of the contract of employment, a condition of Student Registration and part of the process granting others access to the facilities.

Failure to comply with the Security Policy could harm the University’s ability to achieve its mission, security objectives and/or damage the professional reputation of the establishment. Failure to comply may result in removal of access to ICT services, disciplinary action or, in extreme cases, referral to the police.

| Date Policy Approved | May 2013 |
| Approval Authority   | University Executive |
| Date of Commencement | May 2013 |
| Amendment Dates      | Version 1 |
| Date for Next Review | May 2014 |
| Related Policies, Procedures, Guidance, Forms or Templates | Regulations for the Use of ICT |