1. Introduction

Keele University recognises that all information and information systems are valuable assets which play a major role in supporting the University's strategic objectives. Information security is important to the protection of the University's reputation and the success of academic and administrative activities. It is also an integral part of the information sharing which is essential to academic and corporate endeavour. The management of personal data has important implications for individuals and is subject to legal obligations. The consequences of information security failures can be costly and time-consuming.

The IT Information Security Policy sets out appropriate measures through which the University will facilitate the secure and reliable flow of computer based information, both within the University and in external communications. It comprises this document, which sets out the principles and framework, and specific policies and guidelines itemised in Annex A. The approach is based on recommendations contained in British Standard 7799 ‘A Code of Practice for information Security Management.

2. Objectives

The objective of the IT Information Security Policy is to ensure that all computerised information and information systems upon which the University depends are adequately secure and protected in line with legislative requirements and business process needs.

3. Scope

The IT Information Security Policy applies to computerised information, but excludes paper, oral, film, microfiche or other 'hard-copy' documents. It covers all information transmitted by electronic means. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal. Appropriate protection is required to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual
obligations.

This policy applies to all staff and students of the University and to other users associated with the University. With regard to electronic systems, it applies to use of University owned facilities and privately/externally owned systems when connected to the University network directly or indirectly. ('Owned' is deemed to include leased, rented or on-loan).

This policy applies to all University owned/licensed data and software, whether being used on University systems or privately/externally owned systems, and to all data and software provided to the University by sponsors or external agencies.

4. Policy Statement

The University is committed to protecting the security of electronic information through the preservation of:

- confidentiality: protecting information from unauthorised access and disclosure
- integrity: safeguarding the accuracy and completeness of information and processing methods
- availability: ensuring that information and associated services are available to authorised users when required

The University will develop, implement and maintain policies and procedures to achieve appropriate levels of information security. These will cover the range of elements that need to be addressed in the management of information security, in particular the following areas:

4.1 Authorised Use

University information systems are provided to support the University's activities including learning, teaching, research, administration and approved business activities. Only staff, students and other persons authorised by appropriate University authority are entitled to use the University's information systems.

4.2 Acceptable Use

All users have an obligation to use the University's information and information systems responsibly. Rules for the latter are defined in the “Conditions of Use of Computing and Information Systems”.

http://www.keele.ac.uk/media/keeleuniversity/fait/it/servicedeskinformation/policyandguidance/ITConditions.pdf

4.3 Monitoring and Privacy
The University respects the privacy of its users and there is no routine monitoring of e-mail content or individual Web access. However, the University reserves the right to make interceptions in certain circumstances under the terms of the Regulation of Investigatory Powers Act. These circumstances are set out in the policy document “Monitoring and Interception of IT Systems”.


4.4 Protection of Software

All users must comply with the Copyright, Designs and Patents Act 1988 under which it is an offence to copy software or licensed products without the permission of the owner of the copyright.

4.5 Retention and Disposal of Information

All staff have a responsibility to consider security when using and disposing of information in the course of their work. The University policy regarding retention periods for certain kinds of information is available from

http://www.keele.ac.uk/recordsmanagement/recordsretentionschedule/

Schools, Departments and Research Institutes should establish procedures appropriate to the information held and processed by them, in line with the above policy and ensure that all staff are aware of those procedures.

4.6 Security Evasion

It is an offence within the University Regulations to either knowingly or through recklessness install software that is designed, or intended, to circumvent or otherwise disable applied University security systems, or to exploit security vulnerabilities, in order to access without authorisation University data or network traffic, or a users personal data. This is primarily to avoid the introduction of virus or malware software onto the system, but also covers the practice of system logging or network scanning for unauthorised access to user data, or the use of password discovery techniques to access another users account.

‘Recklessness’ is a term used for those occasions where software is installed by a user without giving prior notification to IT Services or where the medium used to install the software has not been previously scanned by the applied University security software, whilst not malicious or intended as a deliberate act, can otherwise be viewed as negligent. Where the intention is viewed as malicious,
then this offence will fall under the Computer Misuse Act, and will be therefore treated as a criminal act to be dealt with as appropriate.

4.7 Business Continuity

The University will implement, and regularly update, a business continuity management process to counteract interruptions to normal University activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

The University disaster recovery policy can be viewed here:

http://www.keele.ac.uk/media/keeleuniversity/fait/it/servicedeskinformation/policyandguidance/disaster_recovery_2012.pdf

Staff are also expected to take reasonable steps to also ensure business continuity within their areas. These steps include ensuring that all University documents are saved to a University network drive and not on a local hard-disk drive/portable device. Staff who are leaving the University should also ensure that all business critical emails and documents are made accessible to colleagues for use after your departure from the University.

4.8 Transmission of Information to Third Parties

All staff have a responsibility to ensure adequate data security when transmitting sensitive information to third parties electronically. "Sensitive data" comprises information about individuals and business information relating to the University. Where transmission is compulsory through external regulations, users must supply information in accordance with (or more robustly if considered appropriate) definitions set out by the third party. Where the third party has not defined the means of transmission, users must ensure the method they chose to supply the information is secure. Directors and Faculty Deans have a responsibility to inform the Data Protection Officer of all electronic data submissions provided by them to third parties.

The University Policy for the Transmission of Sensitive Data to Third Parties is currently under review. Users requiring advice on best practice are asked to contact the Data Protection Officer in Planning & Academic Administration or the Deputy Director of Information Services in the Finance & IT Directorate in the first instance.

5. Legal and Contractual Requirements

The University will abide by all UK legislation and relevant legislation of the European Community relating to the creation, storage, processing and destruction of information. This includes the following Acts and the guidance contained within the Information Commissioner’s Codes of Practice:
The University will also comply with all contractual requirements related to the holding and processing of information, including:

- JANET (UK Joint Academic Network) Acceptable Use Policy issued by UKERNA (United Kingdom Education and Research Networking Association)
- Code of Conduct on the Use of Software and Datasets issued by JISC (Joint Information Systems Committee)
- The terms and conditions of licenses and contracts
- The terms and conditions of authentication systems

6. Responsibilities

6.1 Managerial

The Library and Information Strategy Committee owns the IT Information Security Policy. The IT Security Group, reporting to the above group, monitors and assists in the implementation of the policy and reporting on breaches.

IT Services within the Finance & IT Directorate will be responsible for the policy, coordination of the implementation and dissemination, and will monitor its operation. They will work in collaboration with other administrators as appropriate.

Deans, Directors, Heads of Schools / Administrative Departments and Research Institute Directors, with support from IT Services, are responsible for ensuring that information and information systems used within their areas of responsibility are managed and used in accordance with information security policies.

6.2 Individuals

All persons granted access to University information systems has an individual responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the policies, codes of conduct and guidelines outlined in this policy.

Each individual is responsible for protecting the University's information assets, systems and infrastructure, and will protect likewise the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations.
It may be necessary for some individuals to sign confidentiality agreements as part of their terms and conditions of employment. This may also apply to contractors or agency staff.

### 6.3 Reporting of Incidents and Breaches

All staff, students and other users should report immediately any observed or suspected security incidents where a breach of the University's security policies has occurred, and any security weaknesses in, or threats to, systems or services. Reports should be made to the relevant Head / Director, the owner of the information, and, where the IT infrastructure is involved, the Deputy Director of IT Services or nominee. Incidents of a critical nature must be reported *immediately* to the Deputy Director of Information Technology.

Those responsible for information or information systems, for example database and IT systems administrators, must ensure that appropriate security arrangements are established and maintained.

### 7. Policy Awareness and Disciplinary Procedures

The Information Security Policy will be made available to all staff and students via the web and maintained by IT Services. Staff, students, authorised third parties and contractors given access to the University information systems will be advised of the existence of relevant policies, codes of conduct and guidelines. Users will be asked to confirm that they understand the policy before being given access to some systems.

Failure to comply with the Information Security Policy may lead to suspension or withdrawal of an individual's access to information systems.

Failure by a member of staff to comply with the Information Security Policy may lead to disciplinary action under the University’s staff disciplinary procedures.

Failure of a student to comply with the Information Security Policy may lead to the instigation of the disciplinary procedures and, in certain circumstances, legal action may be taken. The Student Codes of conduct and disciplinary procedures are set out in full in University Regulation 20: Student Discipline, which can be found on the web at:

[http://www.keele.ac.uk/regulations/regulation20/](http://www.keele.ac.uk/regulations/regulation20/)

Failure of a contractor to comply with this policy could lead to the cancellation of a contract and, in certain circumstances, legal action may be taken.

### 8. Maintenance

The Information Security Policy will be monitored by IT Services and reviewed regularly by
the IT Security Group. Revisions will be subject to appropriate consultation and will be considered by the University Executive Committee or its sub-committee and formally approved by Council.

The IT Security Group will report all major incidents and breaches to the Library and Information Strategy Group.

Heads of Schools / Departments and Directors may be required to carry out periodic risk assessments and establish and maintain effective contingency plans. They will also be required to carry out regular assessment of the security arrangements for their information systems.

Those responsible for information or information systems must carry out periodic risk assessments of their information and the security controls in place. Risk assessments should take into account changes in business requirements, changes in technology and any changes in the relevant legislation and revise their security arrangements accordingly.

9. Physical and Environmental Security

The University recognises the need to place all centrally used information storage systems in secure, environmentally controlled areas with adequate power and fire protection. IT Services have the responsibility to ensure this occurs.

10. Cascading / Disposing of PC’s and Storage Devices

Schools, Research Institutes and Departments are required to ensure all information storage devices (PC’s, Storage Devices, Cabinets, etc) in their ownership are adequately protected against theft and environmental damage. It is the responsibility of the relevant Head or Director to ensure that this occurs.

Schools, Research Institutes and Departments who wish to dispose/recycle PCs have a responsibility to ensure that all University related information is securely destroyed before disposing of them in accordance with current national legislation. The information contained on a PC hard drive cannot easily be securely destroyed, so you MUST contact either your local IT Support staff or the IT Service Desk to request that a technician carry out this work for you. Once this work has been done, you can arrange for the PC to be collected for recycling by contacting the Senior Steward, Accommodation Operations & Projects, Commercial and Business Engagement.

PC replacement policies used by Schools, Institutes and Departments should always, wherever possible, aim to replace equipment that is no longer suitable for use. However, there are circumstances where an existing PC may need to be cascaded to another member of staff on campus. In these situations, the data stored on these PCs should also be securely removed before passing the PC on to someone else. This must
be done either by contacting your local IT Support staff or the IT Service Desk and requesting the PC is securely wiped prior to being re-used.

NOTE: The above procedures and responsibilities are also applicable to all IT storage devices including external hard drives, USB pen drives, laptops, tablet devices and any other electronic device capable of storing University data.

Acknowledgments

This policy includes material adapted from policies developed by Warwick University, who kindly agreed to this use of their material. In turn, their policy was developed from those in use at Imperial College and Oxford Brookes University.

NDP 02.02.2007
Revised 15.11.2007
Revised 02.03.2012
Annex A

Related Policies, Guidelines and Documents

1. Freedom of Information

Guidance on the Freedom of Information Act 2000 can be found on the Planning and Academic Administration web site at:

http://www.keele.ac.uk/foi/

2. Data Protection Act

Guidance on the Data Protection Act 1998 can be found on the Planning and Academic Administration web site at:

http://www.keele.ac.uk/dpa/

3. Record Management Code of Practice

The University policy on Record Management can be found at:

http://www.keele.ac.uk/recordsmanagement/

4. Records Retention Schedule

The University has a records retention schedule, which advises on the minimum retention periods and the appropriate disposal of information. This is available at:

http://www.keele.ac.uk/recordsmanagement/recordsretentionschedule

5. Management of Student Records

Guidance and best practice documentation is available at the JISC web site. All staff dealing with student record management should read this document:

http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/managing-student-records
Annex B

IT Security Group – Terms of Reference

Scope

To monitor and have oversight of IT availability, integrity and confidentiality across the University.

Terms of Reference

- To review and recommend for approval the information security policy and other related policies and procedures.
- To review and monitor information security incidents to ensure that lessons are learnt and relevant improvements made.
- To approve and monitor developments to improve information security, in line with approved information security policy.
- To promote information security throughout the University.
- To review disaster recovery plans and to monitor effectiveness.

Membership

Director of Finance and IT (Chair)
Deputy Director of IT
Senior Members of IT team
Data Protection Officer or nominee from Planning and Academic Administration
Representatives from Faculties and Directorates

Frequency and Timing of Meetings

The group will meet quarterly

Reporting Line

The group will report to the Library and Information Strategy Committee.