1. Introduction
The University must protect its information assets – defined for the purposes of this Policy as computers, hardware, networks, software and all of the data they contain - and its reputation. This will help the University to:

- Ensure that a high quality service is offered to our staff, students and other clients.
- Ensure that it does not lose opportunities for funding through a poor reputation for information security.
- Maintain and improve its reputation and meet its legal obligations and strategic business and professional goals.
- Prevent data loss, including research and teaching data, and criminality.
- Ensure that staff are fully aware of their personal responsibilities for protecting data in accordance with University or any external organisation's guidelines.

2. Objective
This Policy addresses the security of the University's information assets as defined above. The Policy's objective is to protect Newcastle University from information security incidents that might have an adverse impact on its operations, reputation and professional standing.

Information security incidents include but are not limited to: confidentiality (the wrong people obtaining information); integrity (information being altered without permission, whether deliberate or accidental) and availability (information not being available when it is required).

The widest possible definition of information security will be used to include all types of incident that impact the effective use of information. This includes the performance, robustness, reliability and accuracy of equipment, electronic or paper systems and data.

The scope of this policy is all of the University's information. This initial version of the document sets out a framework and addresses the organisation's corporate data, touching in addition on research and teaching related data. Subsequent refinements, based on wider consultation, will reflect as many individual needs as possible.

3. Principles
3.1 Approach

- Use all reasonable, appropriate, practical and effective information security measures, including internationally recognised standards and the classification of information, to protect important processes and assets. This will also include practical measures such as encrypting memory sticks and managing passwords.
- Recognise the concepts of appropriate academic and individual freedom, and the value of collaboration. Such freedom also brings responsibilities. The needs of the individual as well as the organisation will always be considered in the context of this Information Security Policy as well as legal and contractual requirements.
- Continually examine ways in which information security measures can be improved, in order to protect and enhance the University’s operations.
- The University will protect and manage its information assets to enable it to meet its contractual, legislative, privacy and ethical responsibilities. As a publicly funded organisation, the University is aware of the need to ensure public accountability and value for money.
3.2 Responsibilities

- Information Systems and Services (ISS) is responsible for overseeing the security of the University’s Information Assets.
- Everyone granted access to Newcastle University's computing and information systems is responsible for protecting its information assets and likewise protecting the information assets of those third parties to which access is granted.
- All members of the University are responsible for reporting shortfalls in existing information security practices and suggested improvements that could be made to ISS.

3.3 Sensitivity of information

- Much of the information in the University is not confidential. In many cases, it is desirable to share information as widely as possible. This policy applies to the safe keeping of both confidential and non-confidential information. Specific measures will apply to confidential information.
- The University’s definition of what constitutes confidential and non-confidential information is on the Records Management section of the University Website.
- Information will be shared as appropriate within and outside the University in order to facilitate business. Information may be designated as, or otherwise considered to be, confidential. However, the University has obligations under the Data Protection Act 1998 and, as a public authority, under the Freedom of Information Act 2000 which mean that information designated as ‘confidential’ may have to be disclosed. The Records Manager is available to advise on whether a record must be disclosed.

3.4 Practices

- Risk analysis techniques will be used to identify information security risks and their relative priorities. Identified risks will be responded to promptly, implementing safeguards that are appropriate, effective, culturally acceptable and practical.
- Wherever practicable, rights to access and process information will be granted to roles and then people matched to those roles.
- Wherever practicable, all actions will be attributable to an identified individual.
- All use of computer and information systems and information (including third party information) will be attributable, protected by safeguards and handling rules in accordance with current legislation.
- The University will routinely monitor information systems usage, in line with current legislation, to assure the continued integrity and security of the University's information systems and to assist in the resolution of an information security incident.
- The University will ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer any information security incident. This will be done in line with the University’s Business Continuity Plan.
- Actual or suspected information security incidents will be reported promptly to the ISS Helpdesk or via the University’s Whistleblowing Procedure. The ISS Helpdesk, or the Registrar via the Whistleblowing Procedure, will allocate the incident to an appropriate member of ISS staff who will manage the incident to closure, and analyse it for lessons to be learnt. In every material case the Director of ISS will be informed.
- ISS will have delegated responsibility for maintaining detailed Information Security Procedures which will cover each of the areas of this policy.
- Documented Guidelines, education and training will supplement this Information Security Policy.

The Director of ISS will monitor compliance with, and the effectiveness of the Policy on a regular basis, on behalf of Audit Committee. The Director of ISS will review, and bring forward for approval, revisions to the Information Security Policy as appropriate.
4. Policy Awareness
The Director of ISS will publicise this Information Security Policy to all members of the University and others granted access to University computing facilities. All such members and guests of the University are expected to be familiar, and to comply, with the Information Security Policy and Guidelines. The Director of ISS or nominee will be responsible for interpretation of the Information Security Policy.

5. Applicability and Enforcement
This Policy and compliance with it applies to all members of Newcastle University and its subsidiary companies and to others who use its computer and information systems.

The Director of ISS is responsible for ensuring that suitable guidelines, education and training are in place to assist all members of Newcastle University in complying with this policy.

The Director of ISS or nominee will be responsible for ensuring that any transgression of this policy is dealt with using the University’s disciplinary procedures as appropriate.

Newcastle University will require all joint ventures to adopt Information Security Policies which are broadly consistent with this document and will not allow access to the University’s Information Assets until it is satisfied that appropriate arrangements are in place.

Approved by Executive Board 2/12/2008
Approved by Council 8/12/2008