University of Sunderland – Business Assurance
Information Classification Policy

Document Classification: **Public**

Policy Reference – Central Register	_____
Policy Reference – Faculty / Service	**IG 004**
Policy Owner	**Director of Business Assurance**
Date Policy Written	**May 2013**
Author	**Assurance Manager, Business Assurance**
Date Policy Last Updated	
Date to Information Governance Group	**13th June 2013**
Date to Executive	**26th July 2013**
Date for next Review	**March 2017**
Comments	

Information Classification Policy

Contents

Information Classification Policy

1. INTRODUCTION

Information is a vital asset to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities create information assets in one form or another.

Information classification ensures that individuals who have a legitimate right to access a piece of information can do so, whilst also ensuring that assets are protected from those who have no right to access them. This policy aims to assist all members of the University to ensure that correct classification and handling methods are applied to their day to day activities and information is managed accordingly.

- All members of the University, who have access to information assets, have a responsibility to handle them in accordance with their classification.
- Information asset owners are responsible for ensuring that the University classification scheme (which is described in the Information Security Policy) is used appropriately.
- University information assets should be made available to all who have a legitimate need to access them.
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events.

2. PURPOSE AND SCOPE

This policy applies to all University staff and independent contractors.

It applies to all information, in all formats.

In adopting a consistent approach to classifying information, the University of Sunderland will:

- Reduce the risk of damage to its reputation, status and interests due to a loss of sensitive information;
- Reduce the risk of embarrassment or loss of assurance arising from the loss of another organisation's sensitive information;
- Increase the confidence in trading and funding partnerships and in the outsourcing of sensitive activities;
- Simplify the exchange of sensitive person information internally and with third parties, while insuring risks are appropriately managed.

3. DEFINITIONS

3.1. Information Classification

Classified information is protectively marked so that both the originator and recipient know how to apply appropriate security to it. The classification level is based on the likely impact on the organisation if the information is leaked or disclosed to the wrong third party.

3.2. Information Asset

Information held which is of value to an organisation. This includes (but not exclusively) statutory, financial and commercial information.

Further guidance will be available in the University's Information Risk Management policy and associated guidance documents

3.3. Information Security Incident

An information security incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy. This could involve a breach of the Data Protection Act 1998 where the incident concerns personal data.

4. DUTIES AND RESPONSIBILITIES

Overall responsibility for this policy lies with the **Director of Business Assurance**, who performs the role of the University's Senior Information Risk Owner (SIRO)
The SIRO is responsible for:

- Ensuring that an overall culture exists that values and protects information within the organisation
- Owning the organisation's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used
- Owning the organisation's information incident management framework

The Assurance Manager (Business Assurance - Information Governance), responsible to the Director for Business Assurance, is responsible for drawing up information governance policy, process and guidance for good information security practice and ensuring compliance with this policy.

The **IT Security Manager (ITS),** reporting to the Head of Technology Services, is responsible for developing IT Security Policy, standards and guidelines. He/she is also responsible for ensuring that effective IT Security systems, controls and training programs are operationally implemented, fit for purpose and available across the University.

The **Legal Support & Data Protection Officer** is responsible for developing policy, process and guidance relating to Data Protection and can provide advice on collecting, using and protecting personal information.

The University Deans of Faculty and Directors of Support Services have responsibility for ensuring compliance with the University's Information Governance policies and ensuring any issues of non-compliance are addressed. They have responsibility for ensuring that an appropriate member of staff, in each Faculty and Service, takes on the role of "Information Champion".
The Information Governance Group is responsible for recommending policy direction on records management to the Executive and monitoring that agreed policies are followed.

Information Champions are accountable to their Dean of Faculty/Director of Service and have a responsibility to monitor information governance compliance and awareness and be the primary point of contact and source of information and support within the

Faculty/Service. The Information Champions Group will report to the Information Governance Group.

Individual employees have responsibility for ensuring that they comply with this policy and any related policies and guidance. Staff should attend training and awareness sessions provided by the University. Employees also have a duty to report any incidents or 'near misses' in relation to information security.

Responsibility for definition and the appropriate protection of an information asset remains with the originator or owner.

5. POLICY DETAILS

5.1. Asset Classification and Handling

University information assets which are sensitive or have value must be protected at all times. Consideration must be given to day to day activities, protection outside normal working hours and protection both on and off campus.
All information in the University must be classified into one of the following categories by those who own or are responsible for the information:

- Public
- Open
- Confidential
- Strictly Confidential
- Secret

Much information will fall into the *Public* or *Open* categories, but for good reason, such as personal privacy or protection of University interests, some information assets will be categorised as ***Confidential*** or ***Strictly Confidential***. In exceptional circumstances information may be classified as ***Secret***.

5.2. Default Classification

In the event of uncertainty or disagreement as to the classification of the information asset, the default category and handling methods will be **Confidential.** Guidance should be sought from the Business Assurance team.

5.3. Classification Markings (Paper/Electronic Copy)

Classification markings must be clearly visible on all University information assets containing a category of classification information. The appropriate markings are to appear clearly on each page.

5.4. Secure Disposal

Information assets which are considered sensitive (i.e. Secret, Strictly Confidential or Confidential), and are no longer needed or are deemed to have reached "end of life" must be securely disposed of using the University's confidential waste disposal procedures. This must include the disposal of IT equipment used for the storage and processing of information in accordance with the Data Destruction section of the IT Security Policy and subsequent standard.

6. INFORMATION CLASSIFICATION

Category	Type	Asset Handling Methods

Public **Definition:** **May be viewed by anyone, anywhere in the world**	**Public information assets may include but are not limited to:** • Principal University contacts e.g. name/email address/telephone numbers for public-facing roles will be made freely available • Announcements from authorities • Publications • Press releases • Course information	N.B some contact details are associated with specific job roles and responsibilities only and should not be released to the general public without consent.
Open **Definition:** **Access is available to all members of the University.**	**Open information assets may include but are not limited to:** • University contacts e.g. name/email address/telephone number • "Approved" communications e.g. University news/updates to ensure their relevance to day to day activities • Policies/procedures/processes	**Secure handling may include but is not limited to:** University information should be formatted to enable basic security e.g. word documents converted into PDF to avoid tampering and disrepute. These include documents such as but not limited to: • Procedures • Policies • Guidelines
Confidential **Definition:** **Access is limited to specified members of the University, with appropriate authorisation or on a need to know basis.**	**Confidential information assets may include but are not limited to:** • Personal details or identifiable information includes: (name/address/telephone number/email address/date of birth/National Insurance number). • Information relating to the private wellbeing of a University member • Information which is specific to one department • Wage slips • Death certificates • PDR documents • Employee contract data • Non-Disclosure Agreements • Documents in "draft " forma	**Secure handling may include but is not limited to:** **Paper Documents (In Transit/Rest)** • Secure storage - locked (files/folders/cabinets) • Approved third party courier • Use sealed envelopes instead of the usual transit envelopes • Secure disposal **Electronic Information assets (In Transit/Rest)** • Encryption • Password protection • SFTP (Secure file transfer protocol) • Secure file stores • Secure disposal • Access rights/Level of privileges

Sensitive and Confidential **Definition:** **Access is controlled and restricted to a small number of named individuals/Authorities**	**Sensitive and Confidential information assets may include but are not limited to:** • • Personal details or identifiable information classed as 'sensitive' in the Data Protection Act 1998. This includes ethnic or racial origin/religious beliefs, physical or mental health/sexual life/ political opinions/trade union membership/ the commission or alleged commission of criminal offences) Bank details (sort code/account number) • Credit Card Details (PAN/CVV2/Expiry Date/PIN) • Financial data • Medical records • Student transcripts • Examination papers • "On-going" research papers • Servers • Server rooms • Usernames and Passwords • Test data • Investigations/disciplinary proceedings • Submitted patents/IPR • University and Third party Contract/Supplier information	**Secure handling may include but is not limited to:** **Paper Documents (In Transit/Rest)** • Secure storage - locked (files/folders/cabinets) • Approved third party courier • Use sealed envelopes instead of the usual transit envelopes **Electronic Information assets (In Transit/Rest)** • Encryption • SFTP (Secure file transfer protocol) • Secure file stores • Asset tags • Secure disposal • Access rights/Level of privileges
Secret **Definition:** **Access is subject to, or obtained under the Official Secrets Act.**	**Access is subject to, or obtained under the Official Secrets Act.** Further guidance available from Assurance Manager (Information Governance), Business Assurance	

7. RELATED POLICIES

This policy should be read in conjunction with the policies listed in Appendix A of the Overarching Information Governance Policy.