University of Liverpool

Information Asset Classification Policy

Reference Number	CSD-011
Title	Information Asset Classification Policy
Version Number	v1.2
Document Status	Active
Document Classification	Open
Effective Date	22 May 2014
Review Date	28 March 2018
Author	Computing Services Department (David Hill)
Approved by	Corporate Services & Facilities Committee (Nov 2012)
Implemented by	Information Security Officer
Monitoring of compliance	Faculty Information Security Managers (Local) CSD Information Security (Central)
Comments	• **22/05/2014 - Annual Review/Update v1.0 – v1.1** • **31/07/2015 – Annual Review/Update v1.1 – v1.2** • **29/07/2016 – Annual Review** • **28/03/2017 – Annual Review**

Table of Contents

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. The Information Asset Classification Policy and its associated policies are concerned with managing the information assets owned by the University and used by Staff/Student(s) of the University in their official capacities.

2. Principles

Information asset 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 helps all Staff/Student(s) of the University to ensure that correct classification and handling methods are applied to their day to day activities and managed accordingly.

- All information assets must be handled and managed in accordance with their classification.
- 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.
- All Staff/Student(s) 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.

3. Objectives of This Policy

- To define the responsibilities of individuals for safeguarding University information assets.
- To provide a rigorous and consistent classification system which ensures that information assets are appropriately protected and managed throughout the University, in accordance with both UK legal requirements and University policies.
- To minimise the damage to the University, its customers and partners as a result of sensitive information assets being intercepted or exposed.
- To ensure that information assets which are lost, stolen, damaged or intercepted are sufficiently protected and unreadable so that unwarranted action cannot be taken against the University and its Staff/Student(s).

4. Action Implementation

Procedures will be put in place to ensure that this policy is effective. These procedures include:

- Information users being appropriately identified and having access to information for which they have a legitimate need.
- Information assets being appropriately managed and controlled in line with the requirements of this policy.
- Information assets being identified and sufficiently protected in line with the correct categorisation and handling methods.
- Ensuring that adequate control mechanisms are in place for protecting University information assets.

- Ensuring that information access control mechanisms are in place for both system and database administrators and that these mechanisms are reviewed regularly.
- Ensuring that asset owners define the physical security of computer rooms, networks, personal computers and procedures for computer maintenance.
- Ensuring the safe disposal of all information assets and equipment.

5. Data Protection Act 1998 (DPA)

The DPA requires the University to ensure appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

For more information please refer to the University's Information Security Policy and Data Protection Policy.

6. Asset Classification and Handling

Information assets owned and managed by the University 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".***

Default Classification

In the event of uncertainty or disagreement as to the classification of the information asset, it is advised that the default category and handling methods should be **Confidential** or **Strictly Confidential.**

Please contact the CSD Information Security Officer via the CSD Service Desk to clarify or resolve any uncertainty and disagreement of the classification of information assets.

7. Asset Classification Categories, Type and Handling Methods

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 contacts 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 Staff/Student(s) 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 Staff/Student(s) 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/ 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). • 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 " format	**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 • Reduced access rights/Level of privileges

Strictly Confidential **Definition:** **Access is controlled and restricted to a small number of named individuals/Authorities**	**Strictly Confidential information assets may include but are not limited to:** • 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 which includes: **Infrastructure or University network information (Including hardware and software)**	**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.**	**Individual projects may require differing controls above/or below) local circumstances. Each requirement will be reviewed on a case by case basis in line with HMG controls.** **HMG advice and guidance is subject to regular change. It is advised University Staff/Student(s) refer to the CSD Service Desk for more information and guidance from the Information Security Officer.**	

8. Classification Guidelines (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 either at the top or in the centre or at the bottom of each page. Please refer to the Classification Marking Guidelines for more information.

For more information on central templates, guidelines and University brand identity please refer to Corporate Communications Homepage .

9. Re-classification of Information Assets

Some information assets may be re-classified from one category to another based on the content and intent of the asset. There must be sound reasoning for the re-classification. If there is any doubt over the classification of an asset, contact the CSD Service Desk for more information from the Information Security Officer.

Example A*- Draft University policy(s)*

Once written, agreed and signed off by relevant stakeholders the asset/document owner can authorise the communication of the policy to the wider audience of Staff/Student(s) of the University. It has now been re-classified from ***"Confidential****" to* ***"Open"****.*

Example B *– On-going Research, Development, Study and Publication(s)*

Specific areas of research associated to the University will contain a range of information within the faculties, schools and institutes which must be managed in accordance to sensitivity. This might include (but is not limited to) documented findings, intellectual property and patent pending works. Once the research has been established, accredited and the legislative process has been completed - it may be deemed a publication of works and may be re-classified to be viewed by public authorities. It has now been re-classified from ***"Confidential"*** *or* ***"Strictly Confidential****" to* ***"Public"****.*

10. Sensitive Information assets

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

A higher level of protection must be provided for sensitive information assets which includes 'personal data' and 'personal identifiable information', which is defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences.

Identifying sensitive information is a matter for assessment in each individual case. Broadly, however, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

1. financial loss e.g. the withdrawal of a research grant or donation, a fine by the ICO, a legal claim for breach of confidence;
2. reputational damage e.g. adverse publicity, demonstrations, complaints about breaches of privacy; and/or
3. an adverse effect on the safety or well-being of Staff/Student(s) of the University or those associated with it e.g. increased threats to staff or students engaged in sensitive research, embarrassment or damage to participants, benefactors and suppliers

11. Storage and Backup

It is the responsibility of each member of the University to ensure sensitive data is stored, secured and backed up on a daily basis. All University owned and sensitive data must be stored and secured via the University approved and provided electronic storage locations, which include:

- M Drive/Departmental Drive

12. Cloud Usage and sharing your M Drive/Departmental drive data

Providing secure access which requires sharing to/from University M/Departmental data externally can be undertaken using the University's provided solution.

Please refer to http://www.liv.ac.uk/csd/datanywhere/ for more information.

For more information and guidance on the risks of cloud storage please refer to the Code of Practice for using Cloud Services in the first instance.

Should any University solution not be fit for purpose or another hosted solution is required please refer to the IT Procurement and Third Party Security Policy to ensure all relevant controls and risk mitigation is undertaken prior to processing.

13. Data Anonymisation

> "Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place" (http://ico.org.uk)

All appropriate steps must be taken prior to disclosing, sharing or publishing University data/findings to non-University staff/student(s), public authorities and person (s) to ensure the anonymity of a staff, student and/or participant is undertaken and maintained in accordance with legislation.

There are several methods that can be used for data anonymisation which allow University (professional/academic) activities to continue to use data whilst ensuring privacy and security of personal identifiers.

Omitting/ Redacting

Omitting or deleting specific personal identifiers is the most basic privacy method whereby sharing or releasing information removes personal data from any documents/records.

Omitting/Redacting must be:

- undertaken on a copy of the document/record and not via the master copy

Redaction is the separation of information by "blocking out" individual words, sentences or paragraphs or the removal of whole pages or sections prior to the release of data. Redaction should be performed or overseen by staff that are knowledgeable about the records and can determine what material is exempt.

Staff/Student(s) must ensure redaction is undertaken via:

- a copy of the document/record and not the via master copy
- specialist and/or approved software
- specialist and/or approved marker pen(s) (Hardcopy documents)

De-identification or Pseudonym

De-identification is the separation or replacement of a data set that removes the ability to link a data set to the identity of a person and/or any sensitive data sets that relate to identifiers that have the ability to cause a risk to a

Example table of de-identification/Pseudonym changes

Name > Record ID/No	Address/Postcode > City/Region/Country	DOB > Age Range	Exact Salary > Pay Band
Anne > A > **001**	765 Brownlow Hill,Liverpool L69 7ZX > **Liverpool,Merseyside England**	1983 > **20-30**	£19,386 > **Band A (£15,000-£20,000)**
Bob > B > **002**	765 Brownlow Hill,Liverpool L69 7ZX > **Liverpool,Merseyside England**	1994 > **18-25**	£22,186 > **Band B (£20,000 – 25,000)**

Audio Visual/Verbal Exchange

Audio Visual data and/or participant information can be difficult to anonymise due to the nature and format of the recordings. Audio Visual and verbally exchanged recordings, where required, should be masked, edited and/or dubbed.

It may be difficult, time consuming and financially expensive to acquire specialist software. It should be noted that in the event that this is the conclusion, consent/permission from University staff/student(s), participants and any data owner should be sought and evidence of acceptance recorded.

For more information please refer to:

- ICO Code of Practice for Data Anonymisation
- UK Data Archive

14. Sensitive IT/Research Usage

Usage of IT systems/devices for sensitive activities (professional/academic) cannot be undertaken without prior written consent. This is to ensure the University can indemnify any staff or student from University disciplinary and/or appropriate authority investigation(s).

Staff/Student(s) must contact the relevant teams prior to undertaking these activities via the CSD Service Desk (Professional Services) or Research Governance for academic activities.

15. Removal of Information Assets

Staff/Student(s) of the University must not remove sensitive information assets (Confidential/Strictly Confidential/Secret) from the University premises without the prior agreement or consent from an appropriate authority. In the event of authorised removal of information assets, it is your responsibility to adequately protect the information assets at all times and to return them in the condition in which they were originally provided to you.

16. 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. There are several ways to dispose of information assets and equipment. These include:

Secure shredding (Cross cut shredders)

The University has a number of shredders which should be used to ensure secure disposal of all sensitive information assets that are no longer needed. This removes the need for Staff/Student(s) of the University to store unwanted information assets.

Confidential waste disposal bins (Paper based)

Confidential waste bins are available within many University departments and are an alternative to secure shredding.

Computing Service Department (CSD) IT Asset Disposal Service

IT equipment including PCs, laptops, telephones, mobile phones, and printers must be disposed of in a secure manner with a certificate of destruction maintained for audit purposes**.** For more information please refer to the IT Asset Disposal Policy.

17. Workspace and IT Equipment Security

Please refer to the Workspace and IT Equipment Security Policy for more information.

18. Payment Card Data (PCI-DSS)

Payment Card Industry Data Security Standards (PCI DSS) applies to the University wherever credit/debit card payments and associated data is stored, processed or transmitted or are otherwise present in a cardholder data environment. Sensitive credit card data (SAD) must be protected in accordance with all PCI DSS security requirements.

For more information on the University's obligations for protecting credit/debit card data please refer to the Card Payment Policy.

19. Information Security Incident Response

In the event that an information asset is damaged or lost, this must be reported immediately to the CSD Service Desk and to your relevant Faculty Information Security Manager.

For more information on reporting information security incidents please refer to the Information Security Incident Response Policy .

20. CSD Service Desk Contact Details and Service Times

For all other CSD services and queries please refer to the CSD Service Desk in the first instance. You can do this by:

- Logging an online support request: http://servicedesk.liverpool.ac.uk/
- Email: servicedesk@liverpool.ac.uk
- Telephone: 44567 (internal)
- Telephone: +44 (0) 151 794 4567 (external)

21. FOI (Freedom on Information) Requests

Information that does not contain data on individuals or has no degree of sensitivity will be considered in the public domain. In line with the Freedom of Information Act 2000 – this information will normally be contained within the University's Publication Scheme and made freely available. It is envisaged the majority of information assets that is afforded 'University sensitive' status will at an appropriate time be made publicly available.

Any information requested by an unapproved authority, third party or member of the public under the Freedom of Information Act is to be referred to the University Legal, Risk and Compliance department in the first instance. Legal, Risk and Compliance will ensure all requests are responded to within the agreed timeframe and within the structured process set by the ICO (Information Commissioners Office).

Please refer to the University's Freedom of Information Publication Scheme for more information.

22. Legal Obligations and University Policies

This policy is aimed at all staff/student(s) of the University who have a responsibility for the use, management and ownership of information assets. This policy is part of the University Information Security Management System (ISMS) and should be read in conjunction with the Information

Security Policy and its sub policies and relevant UK legislation. Further relevant policies and legislation are listed in Appendix A.

23. Compliance and Monitoring

Staff are bound to abide by the University IT regulations by the terms of their employment. Students are bound to abide by the University IT Regulations when registering as a student member of the University.

Authorised staff of the University may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.

Appendix A – University ISMS Reference

- Regulations for the Use of IT Facilities at the University of Liverpool
- JANET Acceptable Use policy
- Information Security Policy
- Information Security Incident Response Policy
- Information Security Review Policy
- Workspace and IT Equipment Security Policy
- Security Investigation Policy
- IT Procurement and Third Party Security Policy
- IT Asset Disposal Policy
- Procurement Policy
- Social Media Compliance Policy
- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Card Payment Policy
- Records Management Policy
- Records Retention Policy
- Risk Management Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Retention Investigatory Powers Act 2014
- Counter Terrorism and Security Act 2015 (Prevent)
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)