Information Security Policy

Information Handling

1 Objective

1.1 This policy aims to ensure that effective measures are in place for the protection of the University's sensitive information assets against loss or unauthorised disclosure. The phrase 'sensitive information assets' means any records or data (whether in paper or electronic format) which are unsuitable for open public access.

2 Scope

2.1 Managers within Schools and Professional Services Divisions are responsible for the sensitive information assets in their area. This policy sets out standards and guidelines to assist managers and their staff in the identification, usage, storage, transfer and destruction of sensitive information assets. Compliance with this policy will assist the University in meeting its legal requirements.

3 Identification of sensitive information assets

3.1 Managers within Schools and Professional Services Divisions should periodically audit the information assets for which they are responsible and conduct an Information Risk Assessment to determine if they are in any way sensitive.

3.2 Sensitive information assets may be divided into two different classes:

(a) Confidential.
This is where access to the information asset is restricted by the University following an Information Risk Assessment.

Sensitive information assets in this class include (but are not limited to): commercially or financially valuable information, student coursework and exam scripts, internal reports, general research data held by academic staff, Protected Personal Information (information that links an identifiable individual with information that, if released, would put them at significant risk of harm or distress); any source of information relating to 1000 or more individuals not in the public

domain, even if the information is not considered likely to cause harm or distress.

(b) Strictly Confidential.
This is where access to the information asset is restricted:

(i) for legal reasons (whether through legislation, Court Order or contract); or
(ii) because the loss or unauthorised disclosure of the information asset would prejudice national security or the prevention and detection of crime; or
(iii) because commercial or business-critical Confidential information has been categorised as material of particularly high sensitivity; or
(iv) because the volume of Confidential information means that its loss or unauthorised disclosure would have a significantly greater adverse impact than the loss or unauthorised disclosure of any item in isolation.

Sensitive information assets in this class include (but are not limited to): collections of Protected Personal Information, research data specifically covered by patent or legal agreement, information protected by clauses in commercial contracts, evidence of criminal activity, highly sensitive financial information.

3.3 Managers within Schools and Professional Services Divisions should assign a named Information Owner to take primary responsibility for the usage, storage, transfer and destruction of each sensitive information asset. Notwithstanding this assignment of primary responsibility, all users of the sensitive information asset should endeavour to safeguard its confidentiality and integrity.

4 Usage and storage of sensitive information assets

4.1 The following standards and guidelines apply to the usage and storage of both Confidential and Strictly Confidential sensitive information assets:

(a) access to a sensitive information asset will in all cases be restricted to a group of individuals within and/or beyond the University. The distribution of the sensitive information asset should be controlled as closely as possible by the Information Owner;

(b) classification markings stating ‘Confidential’ or ‘Strictly Confidential’ as appropriate should wherever possible be made clearly visible on the

sensitive information asset, whether in paper or electronic format. The alternative markings that are understood by the University to indicate either Confidential or Strictly Confidential sensitive information assets are set out in the procedural appendix to this policy. Classifications should be periodically reviewed by the Information Owner and markings may be upgraded or downgraded as appropriate;

(c) the storage (including electronic storage on portable devices or media such as laptops or USB sticks) and publication of a sensitive information asset should be carried out in accordance with the procedural appendix to this policy;

(d) the Information Owner should promote a clear desk and screen policy, particularly in circumstances of heightened risk, to aid the protection of the sensitive information asset.

4.2 The following additional standards and guidelines apply to the usage and storage of Strictly Confidential sensitive information assets:

(a) key documents and reports comprising the Strictly Confidential sensitive information asset should normally be self-contained and should not rely upon the availability or integrity of external sources over which the Information Owner may have no control, unless those external sources have been the subject of a suitable risk assessment and all the other provisions of the Third Party Access Policy;

(b) any breach of security involving a Strictly Confidential sensitive information asset must be reported as soon as possible to the Governance Office and/or the Director of IT Services who will advise the Information Owner and senior management on handling the breach.

5 Transfer and destruction of sensitive information assets

5.1 The following standards and guidelines apply to the transfer and destruction of both Confidential and Strictly Confidential sensitive information assets:

(a) the removal of a sensitive information asset from the University of Sussex campus (whether in paper or portable electronic format) should be carried out in accordance with the procedural appendix to this policy;

(b) a third party organisation from which the University receives a sensitive information asset may have its own policies regarding the handling of the asset. All users must ensure that they comply with the relevant organisation's policies before handling any such sensitive information asset;

(c) all records (whether in paper or electronic format) containing a sensitive information asset must be confidentially destroyed in accordance with the University's Records Management Policy, Master Records Retention Schedule and associated guidance.

5.2 The following additional standards and guidelines apply to the transfer and destruction of Confidential sensitive information assets:

(a) a Confidential sensitive information asset should only be transferred outside the University's networks (including by email) when all risks have been considered and reasonable confidentiality can be assured throughout the transfer;

(b) prior to sending a Confidential sensitive information asset to third parties, the Information Owner should take reasonable precautions to ensure that the information security measures adopted by the third party will achieve the necessary standards of confidentiality and integrity.

5.3 The following additional standards and guidelines apply to the transfer and destruction of Strictly Confidential sensitive information assets:

(a) a Strictly Confidential sensitive information asset should only be transferred outside the University's networks (including by email) when all risks have been thoroughly assessed and reasonable confidentiality can be assured throughout the transfer. Data encryption and password protection of information assets should be used where possible and in accordance with specified procedures;

(b) prior to sending a Strictly Confidential sensitive information asset to third parties, the Information Owner should take every precaution (including formal undertakings where required) to ensure that the information security measures adopted by the third party will achieve the necessary standards of confidentiality and integrity.

6 Relationship with existing policies and legislation

6.1 This policy interacts closely with the University's Information Security Policy (and subsidiary policies), the Records Management Policy (and subsidiary documents), the Code of Practice on Handling Personal Information, the Third Party Access Policy, and various items of national legislation including the Data Protection Act 1998 and the Human Rights Act 1998.

7 Contacts

7.1 Governance Office
Sussex House
University of Sussex
Falmer
Brighton BN1 9RH

dpo@sussex.ac.uk

8 Issue and Review

8.1 This Information Handling Policy has been approved by the University's Information Services Committee.

8.2 This Information Handling Policy will be formally reviewed every five years.

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jeremy Maris	IT Services

Contributors and Reviewers:

Contributor/Reviewer	Department/Team
Jerry Niman	Consultant
Matthew Trump	Information Service Assurance Manager

Revision History:

Version Number	Status D/R/A/I[1]	Date Issued	Reason for Issue	Issued by
0.2	D	19/01/2010	Governance draft following initial discussion	
0.25	D	29/01/2010	Revision re Protected Personal Information	
0.31	D	8/02/2010	Revision post ISWG	
0.4	R	10/2/2010	Protective marking and layout	
1.0	A	16/2/2010	Approval by ISC	
1.1	D	16/01/2015	7a dependence on external sources for Strictly Confidential documents permitted subject to suitable risk assessment.	
1.2	R	23/02/2015	Issued to ISC for Approval	PD
1.3	I	3/3/15	Approved by ISC for issue	PD
1.4	I	20 June 2017	Minor Amendments	MT

[1] D = Draft; R= Ready for approval; A = Approved for issue; I = Issued

PROCEDURAL APPENDIX

Information Classification Matrix

	Unclassified	Confidential	Strictly Confidential
Criteria	Protection of information is at the discretion of the Information Owner.	Protection is required : (i) following an Information Risk Assessment; or (ii) because it is Protected Personal Information.	Protection is required: (i) in order to comply with national or international legislation; or (ii) through contract or Court Order; or (iii) because the loss or unauthorised disclosure of the information asset would prejudice national security or the prevention and detection of crime; or (iv) because commercial or business-critical Confidential information has been categorised as material of particularly high sensitivity; or (v) because the volume of Confidential information means that its loss or unauthorised disclosure would have a significantly greater adverse impact than the loss or unauthorised disclosure of any item in isolation.

	Unclassified	Confidential	Strictly Confidential
Risk	None or low.	Medium.	High/Critical.
Access	General Public. May be restricted by the Information Owner to "campus only".	Specified (authenticated) staff, students or third parties.	Controlled and restricted to a small or very small number of (authenticated) staff, students or third parties.
Examples of asset	Campus maps. Public lectures, seminars etc. Promotional material. Staff directory information. Information subject to disclosure under the Freedom of Information Act.	Individual staff /student records. Commercially or financially valuable information. Student coursework and exam scripts. Internal reports. General research data held by academic staff.	Collections of staff records. Research data specifically covered by patent or legal agreement. Information protected by clauses in commercial contracts. Evidence of criminal activity. Highly sensitive business or financial information.

Information Handling matrix

	Unclassified	Confidential	Strictly Confidential
Marking		Top and bottom of every page Arial font Minimum 12 point bold, in black	As for Confidential
Storage (physical)		In lockable furniture	In lockable furniture in a room with restricted

	Unclassified	Confidential	Strictly Confidential
			access.
Access	General Public. May be restricted by the Information Owner to "campus only".	Specified (authenticated) staff, students or third parties.	Controlled and restricted to a small or very small number of (authenticated) staff, students or third parties.
Encryption of information assets: a) processed or stored on University servers		Encryption not required.	Encryption may be required by the Information Owner.
b) processed or stored on University managed portable computing devices e.g. laptops or stored on USB sticks)		Encryption required.	Encryption required. Permission to process or store on portable devices must be specifically granted by the Information Owner.
c) processed or stored on personally owned "home computers" or mobile devices		Information must be stored on University specified encrypted media.	Assets are not permitted to be stored or processed on personally owned home computers or mobile devices.
Movement by mail		In a sealed envelope addressed to named individual or job title marked "Addressee Only".	As for Confidential, however when sending away from the building the envelope must be marked 'Strictly Confidential' and placed inside a second, sealed envelope with no external classification markings. A return address must be provided on the outer envelope.
Movement by email		Subject should include the line CONFIDENTIAL.	Only if email and/or attachment is encrypted, and using encrypted communication protocols
Web access	Via www.sussex.ac.uk	Authenticated access via secure server, e.g. Sussex Direct, Study Direct.	Assets must only be accessible via business applications. .Remote access must be through a secure VPN and must utilise challenge-response authentication, or other

	Unclassified	Confidential	Strictly Confidential
			risk-assessed mechanism offering equivalent level of security
Disposal (physical) Note: all disposal must be in accord with the Master Records Retention Schedule.	Via recycling waste bins.	Shredded or placed in confidential waste receptacle that is collected by an approved waste collector.	Shredded.
Disposal (Electronic) Note: all disposal must be in accord with the Master Records Retention Schedule.		Copies of assets stored on portable computing equipment or storage must be securely deleted in a manner specified by IT Services as soon as practicable after the copy of the asset is no longer required.	As for Confidential.

Note on Protected Personal Information and the Data Protection Act.

Protected Personal Information (PPI) is defined as:

- information that links an identifiable individual with information that, if released, would put them at significant risk of harm or distress;

or

- any source of information relating to 1,000 or more individuals not in the public domain, even if the information is not considered likely to cause harm or distress.

Protected Personal Information in electronic format must be stored and processed on University provided Network Storage. If copied from University Network Storage the information MUST ALWAYS BE ENCRYPTED, e.g.

(i) when stored on portable electronic devices or local storage (e.g. laptop computers, USB sticks, CD ROMs etc.)

(ii) when collections of information are in transit in electronic form (including by email).

The encryption used must comply with IT Services technical advice.

Documents, in physical or electronic format, that contain Protected Personal Information MUST BE PROTECTIVELY MARKED in accord with the Information Handling Policy.

Special handling procedures must be used for Protected Personal Information that cannot be encrypted (e.g. backup tapes, video or audio recordings, etc.).