University of Dundee

Information Security Classification Scheme

Purpose:

This document provides a framework for staff and students to consider risks in respect of different types of data held, used and transmitted within the University. It also provides guidance on the storage and transmittal of information based upon the level of risk.

Coverage:

The document provides examples of information and data which alongside the classifications. Those examples are not comprehensive, but should be sufficient to inform any consideration of sensitivity when working with information not mentioned explicitly. Some specialist areas of the University may have additional security classifications in place, based upon local needs and activities. They may be read in conjunction with this scheme.

Responsible officers:

The University Secretary the responsible officer. This scheme is maintained by the Director LLC&CI and the Head of Information Governance.

All staff are responsible for ensuring that University information is held and transmitted appropriately.

Notes:

- The University asserts its rights under the Copyright, Designs and Patients Act 1988 and in respect of its intellectual property. Nothing in this classification may be taken to mean otherwise.
- The classification of information can and will change over time as information is published, released, becomes obsolete or is transferred to the University's Information Governance or Archive Services. Periodic review of security restrictions will be necessary and the University reserves the right to vary classifications as required.
- For advice on the retention and appropriate disposition of information, please contact Information Governance.
- Actions leading to the inappropriate or unauthorised disclosure of information designated 'critical', 'confidential' or 'private' may be a disciplinary matter.

Change Control:

Draft	CIO and Records Manager & Information Compliance Officer	July 2014
Consultation	CTO, Information Management Committee	Summer 2014
Revision	CIO	September 2014
Approval	Senior Management Team	November 2014
Web version	CIO and Records Manager & Information Compliance Officer	December 2014
Review and addition of 'Highly Confidential' category and disposal instructions.	Director LLC&CI, Head of Information Governance	March/April 2018
Consultation with Data, Records and Information Committee.		May 2018

Security classification

Class	Rationale	Examples
Open	Information considered 'public' or 'unclassified' and which may be seen by anyone whether directly linked with the University or not. Access to open information is unrestricted.	• Prospectus, programme and course information. • Module reading lists. • Staff names and contact details. • Governance committee minutes (where items of reserved business and/or personal or otherwise confidential information has been removed). • Press releases (not under embargo). • Open content on the University web site. • Fliers and publicity leaflets. • Researcher profiles and publications. • Released research data. • Information released under the Freedom of Information (Scotland) Act.
Private	Information where dissemination is normally restricted e.g. to members of the University, its partners, suppliers or affiliates. Access to private information is normally restricted and governed by appropriate policies or contracts.	• Teaching materials • Exam papers (post-examination) • Class lists • Many research communications, including current research data • University timetable • Draft press releases • Current procurement information or completed commercial and research contracts/agreements
Confidential	Information which is sensitive. Dissemination is normally prohibited except within strictly defined and limited circumstances. Such information is likely to include personal data, commercially sensitive or legally privileged information, or information currently under embargo. This information, if compromised, could: ○ cause damage or distress to individuals ○ breach undertakings to maintain the confidence of information provided by third parties ○ breach statutory restrictions on the use or disclosure of information or lead to a fine, e.g. for a breach of the Data Protection Act or Competition Law ○ breach contractual agreements ○ breach a duty of confidentiality or care ○ cause financial loss or loss of earning potential to the University ○ disadvantage the University in commercial or policy negotiations with others ○ prejudice the investigation or facilitate the commission of crime ○ undermine the proper management of the University and its operations	• Student personal details • Staff personal details • Exam papers (pre-examination or question banks that will be reused) • Student assessment results and feedback • Financial transactions • Internal reports • Completed commercial and research contracts/agreements including confidential information • Restricted research data • Legally privileged information • Information where release would result in breach of confidence • Reserved business of University committees • DRAFT commercial and research contracts/agreements (during negotiation) • Information concerning the prevention and detection of crime • Innovative research with the potential for IP protection
Highly Confidential	Information which is highly sensitive and high risk. Dissemination is only permitted on a 'need to know' basis. Actual harm to the University, its partners or suppliers, students, members of staff or other individuals will arise from its misuse. This information, if compromised, would: ○ cause damage or distress to individuals ○ breach undertakings to maintain the confidence of information provided by third parties ○ breach statutory restrictions on the use or disclosure of information or lead to a fine, e.g. for a breach of the Data Protection or Competition Law ○ breach a duty of confidentiality or care ○ cause very substantial financial loss to the University ○ prejudice the investigation or facilitate the commission of crime ○ severe impact on the management of the University	• Sensitive or special categories of personal data: ○ Race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health data; data concerning sex life or sexual orientation • Medical information including personal identifiers • Details of recent crimes or illegal activities (may be held for research purposes) • Sets of potentially offensive material • Sets of disciplinary records for staff and students • Information concerning national security

Qualifying descriptors may also be used to incorporate/map to protective markings from other classification schemes where necessary.

Guidance

Class	Description, Risk & Labelling	Storage & Encryption	Internal access and communication	External communication and collaboration	Disposal
Open	**Description:** University information that can be seen by anyone. **Risk:** Very little risk of harm to persons, the University or other organisations. **Label:** No requirement to label classification.	Electronic information should be stored using UoD provided IT facilities to ensure appropriate management, back-up and access.	Information can be shared via the web without requiring a UoD username. Electronic and hard copy information can be circulated freely subject to applicable laws and agreements e.g. copyright, contract, competition. Information can be exchanged via email, file sharing or portable media without encryption.	Information can be exchanged via email, file sharing or portable media without encryption.	Paper may be recycled using normal paper recycling services without shredding. Computer hardware, USB sticks and other portable media must always be disposed of by UoDIT as they are likely to contain information from multiple security classes.
Private	**Description:** Information where dissemination is restricted in some way e.g. information restricted to members of the University, a committee, project or partnership. **Risk:** Risk of harm to persons, the University or other organisations may arise from inappropriate disclosure. **Label:** May be labelled 'Private'.	Electronic and hard copy information must be stored using UoD owned facilities. Encrypted devices must be used for the temporary storage or transmission of this information. May be stored in a properly-permissioned Box folder.	May be viewed in originating systems and not downloaded (as far as possible). Where information is downloaded it should be held securely on encrypted devices. Not to be accessed in public places where information can be viewed by others. Should not be accessed or sent to non-University systems or services (personal email accounts, cloud storage products etc).	Information can be sent in unencrypted format via email to known recipients. Information can be shared using UoD IT facilities e.g. shared filestore. Information can be printed and circulated via the University mail service.	Paper must be shredded prior to disposal. Small volumes of paper may be shredded locally and disposed of in paper recycling. Larger volumnes of paper should be destroyed using the Estates and Campus Services 'white bag' process. Computer hardware, USB sticks and other portable media must always be disposed of by UoDIT.
Confidential	**Description:** Information which is sensitive in some way because it may be personal data, commercial or legal information, or be under embargo prior to wider release. Includes data about individuals, and data about the institution. May also include data provided to the University by other organisations eg research datasets. **Risk:** Significant risk of harm to persons, the University or other organisations is likely to arise from inappropriate disclosure of confidential information. **Label:** Should be labelled 'Confidential'.	Information must be stored using secure UoD facilities and will normally only be accessed via the core system. Portable devices must have full disk encryption. Unencrypted removable media (e.g. USB sticks) must not be used. May be stored in a properly-permissioned Box folder.	Whenever possible, information must be viewed in originating systems and not downloaded. Where information is downloaded it should be accessed, stored and/or transmitted in a secure manner. Not to be accessed in public places where information can be viewed by others. Must not be accessed or sent to non-University systems or services (personal email accounts, cloud storage products etc).	This information must be accessed, stored and/or transmitted in a secure manner. This will normally include encryption. Duplicate copies of confidential information must be avoided as far as possible.	Paper must be shredded prior to disposal. Small volumes of paper may be shredded locally and disposed of in paper recycling. Larger volumnes of paper should be destroyed using the Estates and Campus Services 'white bag' process. Computer hardware, USB sticks and other portable media must always be disposed of by UoDIT.
Highly Confidential	**Description:** Information which meets the highest standards of sensitivity and requires the greatest level of protection. It may be sensitive personal data, be commercially or legally sensitive information, or contain unprotected IP. This category may also include data provided to the University by other organisations eg law enforcement agencies. Information is only shared on a 'need to know' basis to the minimum number of authorised persons. Where any doubt exists concerning the sharing of information in this category, advice should be sought prior to transfer from the Director LLC&CI, the Director of Legal or the Head of Information Governance. **Risk:** Significant risk of harm to persons, the University or other organisations will arise from inappropriate disclosure of confidential information. **Label:** Should be labelled 'Highly Confidential'.	Information must be stored using secure UoD facilities and must be accessed using the relevant core system. Portable devices must have full disk encryption, secure authentication and never be left in an open, unattended state.. Unencrypted removable media (e.g. USB sticks) must not be used. Where use of an encrypted USB stick (or similar) is required, the data file must also be secured with a second unique 14 chr (minimum) password. May be stored in a properly-permissioned Box folder, but must have additional encryption - data files must be encrypted using a unique 14 chr password before being uploaded to Box.	Information must be viewed in originating systems and not downloaded. Any extraction of data from core systems must be properly authorised by the relevant Director/Dean. Where information is downloaded it should be accessed, stored and/or transmitted in a secure manner. Not to be accessed in public places where information can be viewed by others. Must not be accessed or sent to non-University systems or services (personal email accounts, cloud storage products etc).	This information must be accessed, stored and/or transmitted in a secure manner. This must include encryption. Duplicate copies of highly confidential information must be avoided as far as possible.	Paper must be shredded prior to disposal. Small volumes of paper may be shredded locally and disposed of in paper recycling. Larger volumnes of paper should be destroyed using the Estates and Campus Services 'white bag' process. Computer hardware, USB sticks and other portable media must always be disposed of by UoDIT.