Resources for Chapter 7 – Information management

RESOURCES

- **Information Classification Scheme – University of York**
- **Development of an Information Classification and Handling Policy – Cardiff University, case study**
- **Information Classification and Handling Policy – Cardiff University**
- **University Guidance on Classification of Information – University of Oxford**

Information Classification Scheme – University of York

An information classification scheme for University information is being introduced to:

- protect information from accidental or deliberate compromise, which may lead to damage, and/or be a criminal offence
- help to meet legal, ethical and statutory obligations
- protect the interests of all those who have dealings with the University and about whom it may hold information (including its staff, students, alumni, funders, collaborators, business partners, supporters etc.)
- promote good practice in relation to information handling.

The classification scheme encompasses all data held by the University, in any format (electronic and hard-copy).

Level	Rationale	Examples
Public	This is information which does not require protection and is considered 'open' or 'unclassified' and which may be seen by anyone whether directly linked with the University or not.	Prospectus, programme and course information Press releases (not under embargo) Open content on the University web site Fliers and publicity leaflets Published information released under the Freedom of Information Act
Restricted	Non-confidential information where dissemination is restricted in some way eg to members of the University, partners, suppliers or affiliates Access to this information enhances University operations by facilitating communication and collaboration between staff, students and external partners, but access is restricted and governed by appropriate policies or contracts	Some committee minutes Departmental intranets University timetable On-line directory of contact details Teaching materials Procurement documents
Confidential	Information which is sensitive in some way because it might be personal data, commercially sensitive or legally privileged, or under embargo before being released at a particular time. It also includes information in a form that could not be disclosed under Freedom of Information legislation. Covers data about an individual, and data about the institution. 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 Press releases Financial transactions Internal reports Commercial contracts Research data

Information may also be marked with a descriptor, which identifies the reason why the classification is applied. The expiry date for the current level may also be given. For example:

- Confidential - personal
- Confidential - commercially sensitive
- Confidential - exams - expires 1 July 2013 and becomes public

Qualifying descriptors may also be used to incorporate/map to protective markings from other classification schemes, where staff are working with external partners, data and schemes (e.g. the Government Protective Marking Scheme). For example: Confidential - GPMS Secret

Class	Description	Storage	Dissemination and access	Exchange and collaboration	Disposal
Public	University information that can be seen by anyone.	Electronic information should be stored using UoY provided IT facilities to ensure appropriate management, back-up and access.	Information can be shared via the web without requiring a UoY username. Electronic and hard copy information can be circulated freely subject to applicable laws e.g. copyright, contract, competition May be accessed remotely and via portable and mobile devices without encryption.	Information can be exchanged via email or file sharing without needing encryption.	Electronic information should be deleted using normal file deletion processes in accordance with any retention schedule. Printed copy should be disposed of via the University paper recycling scheme and in accordance with any retention schedule.
Restricted	Non-confidential information where dissemination is restricted in some way e.g. information restricted to members of the University, a committee, project or partnership.	Electronic and paper-based Information must be stored using UoY provided facilities.	Information can be shared via the web but the user must provide UoY authentication. Electronic and hard copy information can be circulated on a need-to-know basis to University members subject to applicable laws (e.g. copyright) and University Regulations May be accessed remotely and via disk-encrypted portable and mobile devices without further encryption.	Information can be sent in unencrypted format via email. Information can be shared using UoY IT facilities e.g. wiki, shared filestore. Information can be printed and circulated via the University internal mail service.	Electronic equipment holding this information must be disposed of using the University secure IT waste disposal service and in accordance with any retention schedule. Printed copy should be disposed of via the University confidential waste scheme and in accordance with any retention schedule.

Class	Description	Storage	Dissemination and access	Exchange and collaboration	Disposal
Confidential	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 e.g. research datasets	Information must be stored using UoY IT facilities. Portable devices must have full disk encryption. Unencrypted removable media (e.g. USB sticks) must not be used. Encrypted removable media are not permitted without undertaking evaluation of other options.	Access to confidential data must be strictly controlled by the Data Owner who should conduct regular access reviews. Some types of confidential information may be shared with authorised users via UoY IT facilities, including remote access, subject to UoY authentication. For web access encryption must be used. Confidential data must not be extracted from University IT systems and stored on local IT systems. If a portable device (e.g. a laptop, tablet or phone) is used to access University confidential information, the device must be encrypted and require a password or PIN to access	The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed and an appropriate method selected. Confidential data must be encrypted prior to exchange. Exchange must be conducted using UoY provided facilities. Duplicate copies of confidential information must be avoided. Where copies are necessary the protective marking must be carried with the data. Where paper copies are required for circulation or sharing, secure delivery methods must be used. Paper and electronic copies must be marked 'Confidential' and the intended recipients clearly indicated. An optional descriptor, to state the reason for confidentiality, may be used.	Electronic equipment holding this information must be disposed of using the University secure IT waste disposal service and in accordance with any retention schedule. Printed copy should be disposed of in accordance with any retention schedule via the University confidential waste scheme or departmental shredding facilities. Large accumulations of data should not be downloaded or copied.

Examples of documents that may be marked PUBLIC

All documents that are published under the University's Freedom of Information Act Publication Scheme, for example the Annual Report and Financial Statements; policies once they are approved, minutes and papers of Court, Council and other committees. Note that documents marked 'Public' may not be re-classified to any other level, but that documents in the two other levels are likely, over time, to move into the 'Public' classification.

Examples of documents that may be marked RESTRICTED

Such documents might include internal briefing papers. The documents may be restricted to the University, or to a group in it, or to a group in the University and an external partner. Note that documents marked 'Restricted' might lose this marking over time.

Examples of documents that may be marked CONFIDENTIAL

This is the highest level of marking, and, for some documents, might persist for considerable periods of time. It is advisable to note clearly the group who may have access to such documents. Such documents might include papers relating to possible redundancies, patient-level research data, data that is commercially sensitive to a project or a company providing research funds, and data relating to living individuals, whether employees of this University or not.

Examples of documents that move through ALL THREE marking levels

Exam scripts start their life as 'Restricted'; once the exam has been held they might become 'Confidential' (to the University and its students, to protect intellectual property in module design and examination) for a period of years, and then become 'Public' as their sensitivity declines over time.

Development of an Information Classification and Handling Policy – Cardiff University, case study

Introduction

As part of the University-wide Information Security Framework Programme following ISO/IEC 27001 principles, we identified the need to establish an Information Classification, i.e. a University-wide system of categorising information in relation to its sensitivity and confidentiality, together with associated rules for the handling of each category of information in order to ensure the appropriate level of security (confidentiality, integrity and availability) could be applied.

Information Classification Development

A review of other universities' classification systems was undertaken as well as those of our key partners such as the NHS and government. Both the NHS and the government's classifications were under review at the time and what was in place could not for various reasons simply be transplanted to the University setting. Whilst a few universities had developed classifications with elements that we liked there was not one single scheme, at the time that we wished to follow in its entirety. Instead it was decided to develop our own classification looking to:

- keep it simple,
- make the labels intuitive and
- base it on impact of disclosure or loss and align this with our newly defined risk assessment impact scales.

We originally came up with a 4 point scale – with two categories relating to confidentiality ('Highly Confidential' and 'Confidential') and one category relating to criticality/integrity ('Protect'). The fourth category was Non-Classified. It became obvious after a short while however that the Protect category did not work in the same way as the other two classified categories so we decided to drop it as a category in itself and build in the relevant criticality/integrity policy considerations into each of the other categories.

A conscious decision was taken not to treat Personal Data or Sensitive Personal Data (as defined by the Data Protection Act) as a categories in themselves as the impact of disclosure did not always correlate. Some Sensitive Personal Data and much Personal Data is already public domain and not therefore 'sensitive' or confidential at all. We wanted to keep the focus of the categories on the scale of impact of inappropriate disclosure on the institution, groups or the individual. The definitions of the two classified categories (Highly Confidential and Confidential) were designed to include both confidential personal data (such as salaries) and confidential non-personal data (such as competitive business strategy, security codes, etc.).

Examples were given for each category. The short definitions of the categories are below:

- **C1 – Highly Confidential** - Has the potential to cause serious damage or distress to individuals or serious damage to the University's interests if disclosed inappropriately
- **C2 – Confidential** - Has the potential to cause a negative impact on individuals' or the University's interests (but not falling into C1)
- **NC – Not Classified** - Information not falling into either of the Classified categories

Policy

Having got the Programme Steering group to approve the Information Classification we then developed a handling rules and a supporting policy. It was determined that the scope of the policy would cover all information held by and on behalf of the University and the handling rules would apply to members of the University and to third parties handling University information. We also decided that where the University holds information on behalf of another organisation with its own information classification agreement shall be reached as to which set of handling rules shall apply – acknowledging that some data handling requirements from external organisations may be very stringent and require specific security arrangements to be put in place.

Handling Rules development

The Handling Rules were then drawn up to set out the aspirational policy in relation to the handling of University information depending upon whether that information is classified (Highly Confidential C1 or Confidential C2) or not, where and how (i.e. paper or electronic) it is held, and the environmental context. The rules attempt to address the variance in risks associated with the different combinations of information, format or device, and environment. As well as the University context, the document covers the rules around use of personal devices in respect of classified information as well as non-University owned applications that staff may wish to use to transfer or hold University information. The University is currently reviewing 'Bring Your Own Device' which is widely used by staff, so the draft Handling Rules had to attempt to introduce some level of security to the riskiest types of remote and mobile working without an outright ban on BYOD. The rules were drawn up with a view to the existing state of security controls at the time as well as known future improvements, so they contain statements such as 'avoid download' and 'read only' on personal devices where we know we can't currently stop this use but wish to discourage it. We tried to make the security controls consistent between paper and digital information so that Highly Confidential information was treated with equal concern whether it was in hard copy files or on a laptop. It was also important that the rules were presented in a user friendly format and work well on the web.

Consultation

The draft Handling Rules were developed by a small project team involving staff from both Governance and IT, then posted on an internal collaborative community which included senior representatives of the Colleges and Professional Services as well as School Managers and local IT representatives working closely with academics. Over 100 members of the community downloaded the file and 18 staff provided a total of over 50 comments. All comments were helpful and supportive of the aims of the document. A feedback table was compiled indicating what action had been taken in response to the comments received, and this was made available to the community.

Approval and Equality Impact Assessment

The draft Handling Rules were presented to the Steering Group and the University's Executive Board. It was noted that there would be some financial implications in terms of: a) future procurement of equipment that meets a minimum security specification and b) demands for University equipment to be purchased to replace personally owned equipment. In accordance with the Equality Act we also undertook an Equality Impact Assessment of the rules. This found a likely adverse impact on specific protected characteristic groups if they were currently using personally owned equipment to handle Classified (C1 or C2) information in the context of institutionally approved flexible working/reasonable adjustment. The proposed mitigation involves the prioritisation of provision of appropriate University owned equipment for those affected staff.

The draft Handling Rules are currently approved only as guidelines until such time as the programme has delivered some specific tools (such as enterprise encryption and a secure but user friendly file sync and share alternative) to support the more aspirational statements. Other tools may enable more differentiation between the rules relating to C1 and C2 information. In addition we will add in disposal and printing as handling processes that are currently not included and continue to gather feedback on the practical aspects of implementation. At this point the 'Handling Rules' will be reviewed, turned into enforceable policy and promoted through mandatory information security training. We will also develop a similar, but different document for contractors' use of University information.

The Information Classification policy and draft Handling Rules are available here: http://sites.cardiff.ac.uk/isf/handling/

Information Classification and Handling Policy – Cardiff University

1 Purpose

The purpose of this policy is to establish a University-wide system of categorising information in relation to its sensitivity and confidentiality, and to define associated rules for the handling of each category of information in order to ensure the appropriate level of security (confidentiality, integrity and availability) of that information.

2 Scope

This policy covers all information held by and on behalf of Cardiff University and the handling rules shall apply to members of the University and to third parties handling University information. Where the University holds information on behalf of another organisation with its own information classification agreement shall be reached as to which set of handling rules shall apply.

3 Relationship with existing policies

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy and all supporting policies.

4 Policy Statement

All members of Cardiff University and third parties who handle information on behalf of Cardiff University have a personal responsibility for ensuring that appropriate security controls are applied in respect of the information they are handling for the University. Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.

5 Policy

5.1 All information held by or on behalf of Cardiff University shall be categorised according to the Information Classification (Annex 1). The categorisation shall be determined by the originator of the information and all information falling into the classified categories shall be marked as such.

5.2 Information shall be handled in accordance with the Information Handling Rules (Annex 2) and where information falls within more than one category, the higher level of protection shall apply in each case

5.3 Where a third party will be responsible for handling information on behalf of Cardiff University, the third party shall be required by contract to adhere to this policy prior to the sharing of that information

5.4 Where the University holds information on behalf of another organisation with its own information classification, written agreement shall be reached as to which set of handling rules shall apply prior to the sharing of that information

6 Responsibilities

6.1 The Senior Information Risk Owner shall ensure that the Information Classification and associated Handling Rules are reviewed regularly to ensure they remain fit for purpose.

6.2 It shall be the responsibility of every individual handling information covered by this policy, to mark classified material as such, to apply the appropriate handling rules to each category of information, and to seek clarification or advice from a line manager or the Information Security Co-ordinator where they are unsure as to how to label or handle information.

6.3 All members of the University shall report issues of concern in relation to the application of this policy, including alleged non-compliance, to the Information Security Co-ordinator.

7 Compliance

Breaches of this policy may be treated as a disciplinary matter dealt with under the University's staff disciplinary policies or the Student Disciplinary Code as appropriate. Where third parties are involved breach of this policy may also constitute breach of contract.

Annex 1 – Information Classification v2

Category Title	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
Description	**Has the potential to cause serious damage or distress to individuals or serious damage to the University's interests if disclosed inappropriately** *Refer to Impact levels of 'high' or 'major' on the Risk Measurement Criteria* • Data contains highly sensitive private information about living individuals and it is possible to identify those individuals *e.g. Medical records, serious disciplinary matters* • Non-public data relates to business activity and has potential to seriously affect commercial interests and/ or the University's corporate reputation *e.g. REF strategy* • Non-public information that facilitates the protection of individuals' personal safety or the protection of critical functions and key assets *e.g. access codes for higher risk areas, University network passwords.*	**Has the potential to cause a negative impact on individuals' or the University's interests (but not falling into C1)** *Refer to Impact levels 'Minor' or 'Moderate' on the Risk Measurement Criteria* • Data contains private information about living individuals and it is possible to identify those individuals *e.g. individual's salaries, student assessment marks* • Non-public data relates to business activity and has potential to affect financial interests and/or elements of the University's reputation *e.g. tender bids prior to award of contract, exam questions prior to use* • Non-public information that facilitates the protection of the University's assets in general *e.g. access codes for lower risk areas*	**Information not falling into either of the Classified categories** e.g. Current courses, Key Information Sets, Annual Report and Financial Statements, Freedom of Information disclosures
Type of protection required	Key security requirements: **Confidentiality and integrity** This information requires significant security measures, strictly controlled and limited access and protection from corruption Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?	Key security requirements: **Confidentiality and integrity** This information requires security measures, controlled and limited access and protection from corruption Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?	Key security requirement: **Availability** This information should be accessible to the University whilst it is required for business purposes Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?

Annex 2 – Handling Guidelines v2

General advice:

- Always aim to keep Classified Information (C1 and C2) within the University's secure environment.
- Where this is not possible consider whether the information can be redacted or anonymised to remove confidential or highly confidential information, thereby converting it to Non-Classified Information (NC).
- Report any potential loss or unauthorised disclosure of Classified Information to the IT Service Desk on 74xxx
- Seek advice on secure disposal of equipment containing Classified Information via the IT Service Desk on 74xxx
- Use the Confidential Waste Service for disposal of paper and small electronic media xxx@cardiff.ac.uk

INFORMATION HANDLING - Electronic/digital information storage

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
Shared R: or S:	Controlled access ✓ Shared space ✓ Central back-up ✓ *Service delivers high availability and resilience*	Use restricted access folders *Consider*: file password protection for most sensitive files	Use restricted access folders or password protect files	✓
Home H:	Controlled access ✓ Shared space ✗ Central back-up ✓ *Service delivers high availability and resilience*	*Consider*: file password protection for most sensitive files	*Consider*: file password protection for most sensitive files	*Consider*: Does information need to be shared with colleagues - if so enable folder sharing or move to shared drive
School/Department based server	Controlled access ? Shared space ? Central back-up ?	Seek advice from local IT on default access rights, physical security of server and back-up **No storage or creation permitted unless** server environment is equivalent to IT Services server security environment) If yes then required to use restricted access mechanisms where online access is shared *Consider password protection for most sensitive files* *Consider:* Any back-up requirements	Seek advice from local IT on default access rights, physical security of server and back-up **No storage or creation permitted unless** server environment is equivalent to IT Services server security environment) If yes then required to use restricted access mechanisms where online access is shared *Consider*: Any back-up requirements	*Consider*: Any back-up requirements
Other IT Services maintained service (e.g. database)	Controlled access ✓ Shared space ? Central back-up ✓	Seek advice from IT Services on default access rights Use restricted access mechanisms where online access is shared	Seek advice from IT Services on default access rights Use restricted access mechanisms where online access is shared	✓

INFORMATION HANDLING - Electronic/digital information storage

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
University desktop PC hard drive C: or D:	In non-public areas: Controlled access ✓ Shared space ✗ Central back-up ✗	Encrypt drive Lock screen when unattended	Either encrypt drive or password protect files Lock screen when unattended	Lock screen when unattended *Consider*: Any back-up requirements
	In public areas (e.g. Open Access PCs): Controlled access ✗ Shared space ✗ Central back-up ✗	**Use not permitted** *High risk of incidental disclosure*	**Use not permitted** *High risk of incidental disclosure*	Consider: Any back-up requirements
Personally owned (e.g. home) desktop PC hard drive C: or D:	Controlled access ✗ Shared space ? Central back-up ✗	**No storage or creation permitted on device** *May be used for read only remote connection to access files if used in a private environment.* Do not download files to device. Do not leave logged in and unattended Clear browser cache after read only use.	**No storage or creation permitted on device** *May be used for read only remote connection to access files if used in a private environment.* Do not download files to device. Do not leave logged in and unattended Clear browser cache after read only use.	**No master copy storage permitted** *May be used for remote connection to access files* Do not leave logged in and unattended Created documents must be saved on University network or University owned device

INFORMATION HANDLING - Electronic/digital information storage

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
University owned Laptop	Controlled access ✘ Shared space ✘ Central back-up ✘	Encrypt device – use strong password with maximum of 10 minutes inactivity until device locks. Use secure remote connection (e.g. Cardiff Portal or WebDav) to access files and avoid download or storage Do not use to store master copy of vital records Do not work on files in public areas Do not leave logged in and unattended Do not share use of device with non-University staff *Consider*: Any back-up requirements	Encrypt device – use strong password with maximum of 10 minutes inactivity until device locks. Use secure remote connection (e.g. Cardiff Portal or WebDav) to access files and avoid download or storage Do not use to store master copy of vital records Do not work on files in public areas Do not leave logged in and unattended Do not share use of device with non-University staff *Consider*: Any back-up requirements	Do not use to store master copy of vital records Do not leave logged in and unattended Do not share use of device with non-University staff *Consider*: Any back-up requirements
Personally owned Laptop	Controlled access ✘ Shared space ✘ Central back-up ✘	**No storage or creation permitted on device** *May be used for read only remote connection to view files if used in a private environment* Do not download files to device. Do not leave logged in and unattended Clear browser cache after read only use.	**No storage or creation permitted on device** *May be used for read only remote connection to view files if used in a private environment* Do not download files to device. Do not leave logged in and unattended Clear browser cache after read only use.	**No master copy storage permitted** *May be used for remote connection to access files* Do not leave logged in and unattended Created documents must be saved on University network or University owned device

INFORMATION HANDLING - Electronic/digital information storage

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
Personally owned Smartphone or tablet	Controlled access ? Shared space ✘ Central back-up ✘	**No storage or creation permitted on device** *May be used for read only remote connection to access files if used in a private environment* Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks. Encryption setting to be enabled where available. Clear browser cache after read only use.	**No storage or creation permitted on device** *May be used for read only remote connection to access files if used in a private environment* Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks. Encryption setting to be enabled where available. Clear browser cache after read only use.	**No master copy storage permitted** *May be used for remote connection to access files* Created documents must be saved on University network or University owned device
University owned Smartphone or tablet	Controlled access ? Shared space ✘ Central back-up ?	Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks. Encryption setting to be enabled where available. Services to locate device and remote wipe in case of loss/theft to be enabled. Do not leave device unattended in public areas. Do not share use of device with non-University staff Avoid storage of highly confidential information on device. May be used for secure remote connection (e.g. Cardiff Portal or WebDav) to access files but do not work on highly confidential files in public areas *Consider*: Any back-up requirements	Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks. Encryption setting to be enabled where available. Services to locate device and remote wipe in case of loss/theft to be enabled. Do not leave device unattended in public areas. Do not share use of device with non-University staff Avoid storage of confidential information on device. May be used for secure remote connection (e.g. Cardiff Portal or WebDav) to access files but do not work on confidential files in public areas *Consider*: Any back-up requirements	Do not leave device unattended in public areas Do not share use of device with non-University staff *Consider*: Any back-up requirements

INFORMATION HANDLING - Electronic/digital information storage

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
Small capacity portable storage devices (e.g. USB, CD,)	Controlled access ✗ Shared space ✗ Central back-up ✗	**Avoid use where possible** *Consider alternative means of access instead e.g. use secure remote connection (e.g. Cardiff Portal or WebDav) to access files with no download* If no alternative to use then encrypt media – strong passcode Do not use to store master copy Keep in lockable cabinet/drawer which is locked when unattended.	Encrypt media - strong passcode Not suitable for long term storage Do not use to store master copy Keep in lockable cabinet/drawer which is locked when unattended.	Not suitable for long term storage Do not use to store master copy
Large capacity portable storage devices (i.e. external hard drive)	Controlled access ✗ Shared space ✗ Central back-up ✗	Encrypt device – strong passcode Do not use to store master copy Keep in lockable cabinet/drawer which is locked when unattended.	Encrypt device – strong passcode Do not use to store master copy Keep in lockable cabinet/drawer which is locked when unattended.	Do not use to store master copy

INFORMATION HANDLING - Electronic Collaboration and Synchronisation

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
University's virtual learning environment	Controlled access ✓ Shared space ✓ Central back-up ✓	**No storage permitted**	**Requirement:** Use restricted access folder	✓
University collaborative workplace (e.g. Connections, Quickr Teamplace)	Controlled access ✓ Shared space ✓ Central back-up ✓	**No storage permitted** *Use University solutions e.g. (Quickr or Filr where available) instead*	**No storage permitted** *Use University solutions e.g. Quickr (or Filr where available) instead*	Do not use to store master copy
External 'cloud' storage/ file sync provider non-University contract e.g personal Onedrive, individually set up Dropbox accounts	Controlled access ? Shared space ? Central back-up ✗	**No storage permitted** *Use University solutions e.g. (Quickr or Filr where available) instead*	**No storage permitted** *Use University solutions e.g. Quickr (or Filr where available) instead*	Do not use to store master copy

INFORMATION HANDLING - Electronic Transmission

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
From: @cardiff.ac.uk To: @cardiff.ac.uk Sending from University hosted email account to same	Controlled access ✓ Shared space ? Central back-up ✓	Only as password protected attachment, marked confidential and double check recipient *Consider whether sender or recipient may have delegated authority to others to access the account*	Marked confidential and double check recipient *Consider whether sender or recipient may have delegated authority to others to access the account*	✓
From: @cardiff.ac.uk To: @xxx.xxx Sending from University hosted email account to an external account	Controlled access ✓ Shared space ? Central back-up ✓	Only as password protected attachment, marked confidential, double check recipient and get their permission to use that account *Consider whether sender or recipient may have delegated authority to others to access the account*	As password protected attachment, marked confidential and double check recipient and get their permission to use that account *Consider whether sender or recipient may have delegated authority to others to access the account*	✓
From: @xxx.com To: @xxx.xxx Sending from an externally provided personal email account (e.g. hotmail, gmail etc)	Controlled access ✗ Shared space ? Central back-up ✗	**Not permitted - unless sending to @cardiff.ac.uk** Use University provided alternative to send message instead	**Not permitted- unless sending to @cardiff.ac.uk** Use University provided alternative to send message instead	**Not permitted- unless sending to @cardiff.ac.uk** Use University provided alternative to send message instead

INFORMATION HANDLING - Electronic Transmission

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
Fastfile - a secure web based file transfer	Controlled access ✓ Shared space ✓ Central back-up ✓	Only as password protected attachment, marked confidential and double check recipient *Consider whether sender or recipient may have delegated authority to others to access the account*	As password protected attachment, marked confidential and double check recipient *Consider whether sender or recipient may have delegated authority to others to access the account*	✓

INFORMATION HANDLING - Paper records and other records storage

Location	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
Paper copies	***Consider***: Protection from fire and flood damage In restricted access University areas: ***Requirement***: In lockable cabinet/drawer which is locked when not in active use. No papers left out unless being actively worked on. In **unrestricted** access University areas: ✗ **Not permitted** *Alternative: create as/convert to electronic documents and use secure remote connection with permitted device* Off-site working: ✗ **Not permitted** *Alternative: create as/convert to electronic documents and use secure remote connection (e.g. Cardiff Portal or WebDav) with permitted device*	***Consider***: Protection from fire and flood damage In restricted access University areas: ***Requirement***: In lockable cabinet/drawer which is locked when office is unattended. No papers left out when desk unattended. In **unrestricted** access University areas: ***Requirement***: In lockable cabinet/drawer which is locked when not in active use. No papers left out unless being actively worked on. Off-site working: ***Requirement***: If needed to be taken off site a back-up copy must be made beforehand. Not to be left unattended and to be locked away in secure building when not in use.	In restricted access University areas: ✓ In **unrestricted** access University areas: ✓ Off-site working: *Consider making a back-up copy before taking off site*

INFORMATION HANDLING - Paper and other media transmission

Location	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
Internal postal service	✗ **Not permitted** *Alternative*: request specific hand delivery instead ***Consider***: *Making a back-up copy before posting*	***Requirement***: In sealed envelope marked confidential and with sender details ***Consider***: *Making a back-up copy before posting*	✓ ***Consider***: *Making a back-up copy before posting*
External postal service	***Requirement***: Via tracked and delivery recorded service, double wrapped (2 envelopes) and marked confidential. ***Consider***: *Making a back-up copy before posting*	***Requirement***: Via tracked and delivery recorded service, and marked confidential. ***Consider***: *Making a back-up copy before posting*	✓ ***Consider***: *Making a back-up copy before posting*
Fax machine	***Requirement***: if recipient has verified security of receiving machine and is at machine awaiting receipt ***Consider***: *Converting to an electronic format and using secure electronic transfer method instead e.g. Fastfile*	***Requirement***: if recipient has verified security of receiving machine and is at machine awaiting receipt ***Consider***: *Converting to an electronic format and using secure electronic transfer method instead e.g. Fastfile*	✓

University Guidance on Classification of Information - University of Oxford

LABEL	DESCRIPTION	EXAMPLE CONTROLS
CONFIDENTIAL	• Confidential information should be available only to small, tightly restricted groups of authorised users. • Disclosure of such information will have a severe adverse impact on the business of the University, its reputation, or the safety or wellbeing of its staff/ members. • Unauthorised disclosure of such information may have a severe financial impact on the University. • The confidentiality of such assets will far outweigh the importance of their availability. • Information assets in this category would include highly sensitive personal information as well as those with a high financial value, legal requirements for confidentiality and information, which is critical to the business operation of the University.	• Information classified as CONFIDENTIAL should be stored in such a way as to ensure that only authorised persons may access the information. • Information should be stored in a physically secure manner with appropriate defence against unauthorised entry. Physical access should be monitored and appropriate audit trails of access should be maintained. • File or disk encryption may be considered as an additional layer of defence or where physical security is considered insufficient. • Copies of such information should be kept to an absolute minimum and an audit trail should be maintained and secured for all copies of the information. It is assumed that the confidentiality of such information outweighs the need for availability and loss or destruction of such information would be preferable to unauthorised disclosure. • Such information may be stored on machines that are isolated from the network. Where remote access is required this must be controlled via a well-defined access control policy and tight logical access controls designed to allow the minimum access necessary. • Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication. • All users accessing CONFIDENTIAL information must be authenticated and an audit trail of all access must be secured and maintained. This should be kept for a minimum of 6 months or longer where applicable. Authentication should be appropriate, but where passwords are used there clearly defined policies should be in place and implemented. Other forms of authentication should be considered in addition. • Preferably, such information should be kept on on-site systems and users should not be able to make local copies of such information. Where this is required the information must be encrypted in transit and in storage. • Strict policies and procedures must be in place for the secure disposal/destruction of such information. • Any users having access to this information should be vetted as appropriate. • All users must be made aware of their responsibilities for handling such information. Any breach of policy regarding such information will be investigated and disciplinary action is a likelihood. • Any breach of the confidentiality of such information must be reported to the owner of that information. Other parties such as OxCERT and the University Data Protection Officer should also be informed. • Any security incident relating to computers or users having access to such information must be reported to OxCERT and investigated.

LABEL	DESCRIPTION	EXAMPLE CONTROLS
SENSITIVE	Information classed as SENSITIVE should only be available to groups of users who require access as part of their role within the University. • Disclosure of such information may have an adverse effect on the business of the University, its reputation or may cause distress to its staff/members. • Unauthorised disclosure of such information may have a financial impact on the University. • Information assets in this category would include sensitive personal information and other personal information to which access is only required by a subset of users. The information may have a substantial financial value and it is highly likely there will be legal requirements for maintaining its confidentiality.	• Information classified as SENSITIVE should be stored in such a way as to ensure that only authorised persons may access the information. • Information should be stored in a physically secure manner with appropriate defence against unauthorised entry. Physical access should be monitored and appropriate audit trails of access should be maintained. • File or disk encryption may be considered where physical security is considered insufficient. • An audit trail should be maintained and secured documenting all copies of the information. • Remote access must be controlled via a well-defined access control policy and appropriate logical access controls. • Remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication. • All users accessing SENSITIVE information must be authenticated and an audit trail of all access must be secured and maintained. This should be kept for a minimum of 6 months or longer where applicable. • Authentication should be appropriate, but where passwords are used clearly defined policies should be in place and implemented. Other forms of authentication may be considered in addition. • Users may need to make local copies of such information in which case it is likely that encryption in transit and in storage would be required. • Policies and procedures should be in place for the secure disposal/destruction of such information. • Users should be made aware of their responsibilities for handling such information. Any breach of policy regarding such information will be investigated and disciplinary action is a possibility. • Any breach of the confidentiality of such information must be reported to the owner of that information. Other parties such as OxCERT and the University Data Protection Officer should also be informed where appropriate. • Any security incident relating to computers or users having access to such information must be reported to the IT support staff responsible for the information system. The local ITSS will then decide whether the incident should be reported to OxCERT.

LABEL	DESCRIPTION	EXAMPLE CONTROLS
RESTRICTED	• Information classed as RESTRICTED should only be available to staff/ members of the University, sub-groups within the University and/or specifically authorised third parties. • Disclosure of such information is unlikely to have an adverse effect on the business of the University or its reputation. However it may have a negative impact on smaller groups or individuals within the University. • Unauthorised disclosure of such information is unlikely to have a significant financial impact on the University. • Information assets in this category may include some personal information, which should be processed fairly and with the consent of the data subject. • Information in this category is unlikely to have a substantial financial value.	• Users accessing RESTRICTED information should be authenticated and an audit trail maintained. This should be kept for a minimum of 3 months or longer where applicable. • Users are likely to make local copies of such information though encryption is likely not to be necessary. • Restricted information should be deleted when it is no longer necessary for the task in hand. • Any breach of policy regarding such information may be investigated though disciplinary action is unlikely. • Breaches of the confidentiality of such information would be reported to the owner of that information where appropriate. • Security incidents relating to computers or users having access to such information should be reported to the IT support staff responsible for the information system. The local ITSS may report the incident to OxCERT.
UNRESTRICTED	This classification can be used to indicate positively that no protective marking is required. Such information is likely to already exist in the public domain. Its disclosure will have a negligible effect on the University or on any sub-group or individual within the University.	Information in this category should not need users to be authenticated to access it. Such information should be deleted when it is no longer needed.