DRAFT

Document Title:	**Information Classification and Handling Policy**
Owner	Assurance Services, Department of Strategic Planning and Governance
Version Number:	3.4
Document Status:	Approved
Date Approved:	15 January 2019
Approved By:	Data & Information Management Oversight Group
Effective Date:	15 January 2019
Date of Next Review:	January 2021
Superseded Version:	3.3

Document History

Version	Date	Author/Consulted	Notes on Revisions
1	12 November 2013	ISF Steering Group	Approved subject to addition of Annex 2
2	12th March 2014	ISF Steering Group	Amendments to align with approved revised Information Classification (Annex 1) and addition of Annex 2 - handling guidelines Approved as handling guidelines
3	8th March 2016	ISF Team	Amendments to account for changes in policy and technology
3.3	22nd March 2016	Data & Information Management Oversight Group	Approved
3.4	15 January 2019	Data & Information Management Oversight Group	Updates include Security Sensitive Research in C1, inclusion of research data store and update to Online Collaboration Spaces

Information Classification and Handling Policy

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).

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 apply the appropriate handling rules to each category of information, and to seek clarification or advice from a line manager or the Information Security Team where they are unsure as to how to classify 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 IT Service Desk

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 constitute breach of contract.

Annex 1 – Information Classification v3

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*. • Security Sensitive research data	**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	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	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?

	recreate and how much resource would it require to recreate it?	be to recreate and how much resource would it require to recreate it?	

Annex 2 – Handling Procedures v3

General advice:

- **Always aim to keep Classified Information (C1 and C2) secure within the University's managed 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 11111**
- **Seek advice on secure disposal of equipment containing Classified Information via the IT Service Desk on 11111**
- **Use the Confidential Waste Service for disposal of paper and small electronic media Handling@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 Does information need to be shared with colleagues - if so enable folder sharing or move to shared drive	*Consider:* file password protection for most sensitive files Does information need to be shared with colleagues - if so enable folder sharing or move to shared drive	*Consider:* Does information need to be shared with colleagues - if so enable folder sharing or move to shared drive
 **Research Data Store**	Controlled access ✓ Shared space ? Central back-up ✓ *Service delivers high availability and resilience*	Grant access only to those who need it *Consider:* file password protection for most sensitive files	Grant access only to those who need it *Consider:* file password protection for most sensitive files	✓

INFORMATION HANDLING - Electronic/digital information storage

Location	Default Features	Classified *C1* Highly Confidential	Classified *C2* Confidential	NC Non –Classified
 **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 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 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 or password protect files Lock screen when unattended *Consider:* Any back-up requirements	Either encrypt drive or password protect files Lock screen when unattended *Consider:* Any back-up requirements	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 Lock screen when unattended
 **Personally owned (e.g. home) desktop PC hard drive C: or D:**	**Default Features:** 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. Encrypt drive* Do not download files to device Do not leave logged in and unattended	**No storage or creation permitted on device** *May be used for read only remote connection to access files if used in a private environment. Encrypt drive* Do not download files to device Do not leave logged in and unattended	**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

		Clear browser cache after read only use	Clear browser cache after read only use	

INFORMATION HANDLING - Electronic/digital information storage

	Classified *C1* **Highly Confidential**	**Classified *C2*** **Confidential**	***NC*** **Non -Classified**
 **University owned Laptop** **Default Features:** 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. MyFiles, CIFS) 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. MyFiles, CIFS) 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

INFORMATION HANDLING - Electronic/digital information storage

	Classified *C1* **Highly Confidential**	**Classified *C2*** **Confidential**	***NC*** **Non -Classified**
 **Personally owned Laptop** **Default Features:** 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. Encrypt Drive* 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. Encrypt Drive* 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
 **University owned Smartphone or tablet** **Default Features:** Controlled access ? Shared space × Central back-up ?	Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied Services to locate device and remote wipe in case of loss/theft to be enabled. Do not leave device unattended in public areas.	Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied 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 leave device unattended in public areas Do not share use of device with non-University staff *Consider:* Any back-up requirements

	Do not share use of device with non-University staff May be used for secure remote connection (e.g. MyFiles CIFS) to access files but do not work on highly confidential files in public areas *Consider:* Any back-up requirements	Do not share use of device with non-University staff May be used for secure remote connection (e.g. MyFiles, CIFS) to access files but do not work on confidential files in public areas *Consider:* Any back-up requirements	
	Classified *C1* **Highly Confidential**	**Classified *C2*** **Confidential**	**NC** **Non -Classified**
  **Personally owned Smartphone or tablet** **Default Features:** Controlled access ? Shared space × Central back-up ×	**Avoid storage or creation of highly confidential information on device.** Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied	**Avoid storage or creation of confidential information on device.** Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied	**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 Do not leave device unattended in public areas

  **University owned Smartphone or tablet** **Default Features:** Controlled access ? Shared space × Central back-up ?	Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied 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 May be used for secure remote connection (e.g. MyFiles CIFS) to access files but do not work on highly confidential files in public areas *Consider:* Any back-up requirements	Device must be configured to connect via Exchange Active Sync to ensure baseline security features (timeout, password, encryption) are applied 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 May be used for secure remote connection (e.g. MyFiles, CIFS) 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. MyFiles, CIFS) to access files with no download* If no alternative to use then encrypt* media – strong passcode Do not use to store master copy Treat as paper 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 Treat as paper 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
*device needs to implement FIPS 140-2 or FIPS 197 encryption standards				

INFORMATION HANDLING - Electronic Collaboration and Synchronisation

<table>
<tr><th></th><th>Default Features</th><th>Classified C1

Highly Confidential</th><th>Classified C2

Confidential</th><th>NC

Non-Classified</th></tr>
<tr><td rowspan="3">Office 365</td><td rowspan="3">Controlled access ✓

Shared Space ✓

Backed-up ✓</td><td>For Internal Sharing:

If restricted to authorised recipients</td><td>For Internal Sharing:

If restricted to authorised recipients</td><td rowspan="3">✓</td></tr>
<tr><td>For sharing with external parties:

If restricted to authorised recipients who are subject to existing sharing agreement

Files should be encrypted</td><td>For sharing with external parties:

If restricted to authorised recipients who are subject to existing sharing agreement</td></tr>
<tr><td colspan="2">Please be aware when syncing to other devices they need to meet the requirements set out in the ‘Saving and Storing files’ guidance</td></tr>
<tr><td>External ‘Cloud’ storage/file sync provider Non-University contract (e.g individual Dropbox account)</td><td>Controlled access ?

Shared Space ?

Central back-up ×</td><td>No storage permitted

Use University solutions (e.g. Office 365)</td><td>No storage permitted

Use University solutions (e.g. Office 365)</td><td>Do not use to store master copy</td></tr>
</table>

INFORMATION HANDLING - Electronic Transmission

	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 ✓	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 Autoforward to a personal email account from your University account not permitted *Consider whether sender or recipient may have delegated authority to others to access the account*	Marked confidential and double check recipient and get their permission to use that account Autoforward to a personal email account from your University account not permitted *Consider whether sender or recipient may have delegated authority to others to access the account*	✓ Autoforward to a personal email account from your University account not permitted
From: @xxx.com To: @xxx.xxx Sending from an externally provided personal email	Controlled access ✗ Shared space ? Central back-up ✗	University business must be conducted via your University email account	University business must be conducted via your University email account	University business must be conducted via your University email account

account (e.g. hotmail, gmail etc)		*Use University provided alternative to send message instead*	*Use University provided alternative to send message instead*	*Use University provided alternative to send message instead*

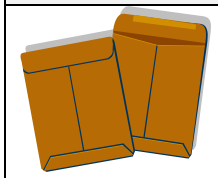
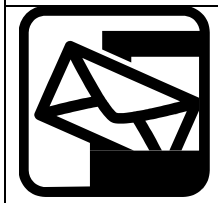
INFORMATION HANDLING - Electronic Transmission

	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

	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. MyFiles, CIFS) 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

	Classified *C1* **Highly Confidential**	**Classified *C2*** **Confidential**	***NC*** **Non -Classified**
 **Internal postal service**	***Requirement:*** In sealed envelope marked confidential and with sender details *Alternative:* Hand deliver ***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*	✓