



## **Information Classification and Handling Policy**



<b>Document Title:</b>	<b>Information Classification and Handling Policy</b>		
<b>Author(s) (name, job title and Division):</b>	Jim Dunsmore		
<b>Version Number:</b>	V1.0		
<b>Document Status:</b>	Approved		
<b>Date Approved:</b>	28/7/15		
<b>Approved By:</b>	Executive Board		
<b>Effective Date:</b>	1 August 2015		
<b>Date of Next Review:</b>	1 August 2016		
<b>Related Documents:</b>	Information Systems Policy Information Security Incident Management Procedure Records Retention Schedule		
<b>Document History</b>			
<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Notes on Revisions</b>
V0.8	9.6.15	J Dunsmore	HL Amendments.
V1.0	28/7/15	J Dunsmore	

### **Acknowledgments**

This document is based on the Information Classification and Handling Policy kindly supplied to Glasgow Caledonian University by Cardiff University, with permission to use any or all content as necessary.

The assistance of the University of Cardiff, especially Mrs Ruth H Robertson (Information Security Framework Programme Manager & Deputy Director Governance & Compliance) and Dr Hugh Beedie (Chief Technology Officer) is gratefully acknowledged.

## **Information Classification and Handling Policy**

### **1 Purpose**

The Policy aims to ensure that information is handled according to the risk or impact to ensure the confidentiality, integrity and availability of data.

The purpose of this policy is to ensure the appropriate handling of all formats of information by establishing a University-wide system of categorising information in relation to its sensitivity and confidentiality, and to define rules for the handling of each category of information in order to ensure the appropriate level of security of that information.

### **2 Scope**

This policy covers all information held by and on behalf of Glasgow Caledonian University (GCU), whether digital or paper. The handling rules will apply to members of the University including staff and students and to third parties processing or handling University information where the University holds information on behalf of another organisation with its own information classification, agreement will be reached as to which set of handling rules will apply. This will be clearly stated within any contract or Service Level Agreement (SLA). A glossary of terminology can be found at Annex 3.

This policy applies to the learning, teaching, research, business activities and administration functions of GCU.

### **3 Relationship with existing policies**

This policy is part of the Information Management Framework. It should be read in conjunction with the Information Systems Policy.

### **4 Policy Statement**

All members of GCU and third parties who handle information on behalf of GCU 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 will be followed.

### **5 Policy**

5.1 All information held by or on behalf of GCU will be categorised according to the Information Classification (Annex 1). The categorisation will be determined by the originator or recipient of the information and all information falling into the classified categories will be marked as such. The originator or recipient will retain primary responsibility for the security, storage, access, distribution and destruction of the information.

5.2 Information will 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 will apply in each case with subsequent review to verify or amend if required.

- 5.3 Where a third party will be responsible for handling information on behalf of GCU, the third party will be required by contract to adhere to this policy prior to the University sharing of that information. Where appropriate, separate Data Sharing Agreements will be in place. Advice should be sought if there is any doubt about whether a Data Sharing Agreement is required.
- 5.4 Where the University holds information on behalf of another organisation with its own information classification, written agreement will be reached as to which set of handling rules will apply prior to the sharing of that information.
- 5.5 No classified data is to be stored on local hard drives. All classified data must be stored on Storage Area Network (SAN) or secure devices outlined at Annex 2 of this document. This is to ensure resilience and to retain the secure integrity of the data.

## **6 Responsibilities**

- 6.1 GCU Vice Chancellor has overall responsibility for, and ownership of, the Policy.
- 6.2 The Head of Information Security is responsible for implementation and management of the Policy and will ensure that the Policy is reviewed regularly to ensure that it remains fit for purpose.
- 6.3 Members of the Executive are Senior Information Risk Owners (SIRO's) with overall responsibility for managing information risks in their business area. Members of the Executive are also responsible for endorsing and supporting the Policy and any amendments and ensuring its adoption within their areas of responsibility.
- 6.4 Deans and Heads of Department are the Information Risk Owners for all of their respective schools and departments. Including any third party involved with those departments and schools that have access to, or share information.
- 6.5 Other roles and Departments within the University will support the management and security of information including Information Compliance, Archives and physical security.
- 6.6 Individual members of staff are responsible for ensuring that they manage information and records in line with University policy and guidelines. Advice should be sought from their respective Information Risk Owners if required.
- 6.7 It is 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 their line manager, Information Risk Owner or Head of Information Security or Head of Information Compliance, where they are unsure as to how to label or handle information.
- 6.8 All members of the University will report issues of concern in relation to the application of this policy, including alleged non-compliance, to Head of Information Security or the Head of Information Compliance.

6.9 Any information loss, unauthorised access or alteration will be reported in line with the University's Information Security Incident Management Procedure.

## **7 Training and Awareness**

7.1 Members of the University will be made aware of this Policy through communications, training and awareness events and promotion via the staff intranet.

## **8. Compliance**

8.1 Internal audit and external audit may carry out reviews relating to compliance with information and records management policies and guidelines.

8.2 Non-compliance with this policy by any member of staff may result in disciplinary action.

8.3 It is the originators' or recipients' responsibility to control classified information from conception to destruction including the distribution and any copies of the data or document that may be created.

8.4 Non-compliance with this policy by any third party may result in any contract or SLA being terminated.

## Annex 1 – Information Classification

Category Title	<b>Classified C1</b>  <b>HIGHLY CONFIDENTIAL</b>	<b>Classified C2</b>  <b>CONFIDENTIAL</b>	<b>NC</b>  <b>Non -Classified</b>
Description	<p><b>Has the potential to cause serious damage or distress to individuals or serious damage to the University’s interests if disclosed inappropriately</b></p> <p><i>Refer to Impact levels of ‘high’ or ‘major’ on the Risk Measurement Criteria</i></p> <ul style="list-style-type: none"> <li>• Data contains highly sensitive private information about living individuals and it is possible to identify those individuals <i>e.g. Medical records, serious disciplinary matters, sensitive personal data</i></li> <li>• Non-public data relates to business activity and has potential to seriously affect commercial interests and/or the University’s corporate reputation.</li> <li>• Non-public information that facilitates the protection of individuals’ personal safety or the protection of critical functions and key assets.</li> </ul>	<p><b>Has the potential to cause a negative impact on individuals’ or the University’s interests (but not falling into C1)</b></p> <p><i>Refer to Impact levels ‘Minor’ or ‘Moderate’ on the Risk Measurement Criteria</i></p> <ul style="list-style-type: none"> <li>• Data contains private information about living individuals and it is possible to identify those individuals <i>e.g. individual’s salaries, student assessment marks, personal data</i></li> <li>• Non-public data relates to business activity and has potential to affect financial interests and/or elements of the University’s reputation <i>e.g. tender bids prior to award of contract, exam questions prior to use</i></li> <li>• Non-public information that facilitates the protection of the University’s assets in general <i>e.g. access codes for lower risk areas</i></li> </ul>	<p><b>Information not falling into either of the Classified categories</b></p> <p><i>e.g. current courses, key information sets, annual report and financial statements, freedom of information disclosures, policies, learning and teaching material, data which is not personal data</i></p>
Type of protection required	<p>Key security requirements: <b>Confidentiality and integrity</b></p> <p>This information requires significant security measures, strictly controlled and limited access and protection from corruption</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the</p>	<p>Key security requirements: <b>Confidentiality and integrity</b></p> <p>This information requires security measures, controlled and limited access and protection from corruption</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the</p>	<p>Key security requirement: <b>Availability</b></p> <p>This information should be accessible to the University whilst it is required for business purposes</p> <p>Back up requirements will need to be considered in relation to the importance of the information:</p>

	master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?	master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?	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

### General advice:

- The guidelines apply to any format of information relating to learning, teaching, research and administration (University business records).
- Classified Information (C1 and C2) must be kept within the University’s secure electronic environment and secure paper file storage systems.
- Report any loss or unauthorised disclosure, access or alteration of Classified Information to the IT Service Desk on 1234 in line with the Information Security Incident Management Procedure
- Seek advice on secure disposal of equipment containing Classified Information via the IT Service Desk on 1234

Use the Confidential Waste Service for disposal of paper or departmental cross shredder which renders the documents so that they cannot be reconstructed. Requests for the destruction of small electronic media should be made via the IT Service Desk. Refer to the [Records Retention Schedule](#) for guidance on the length of time that paper and other formats of records should be retained and records that should be consigned to the University Archives for long term preservation.



### Information Handling - Electronic/digital information storage

Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
 <p>Storage Area Network (SAN) Data Centre (Central Data Storage)</p>	<p>Controlled access ✓ Shared space ✓ Central back-up ✓</p> <p>Service delivers high availability and resilience</p>	<p>Use restricted access folders</p> <p><b>Mandatory:</b> file password protection for sensitive files at document level</p>	<p><b>Mandatory:</b> Use restricted access folders or password protect files</p>	<p>Mandatory: storage on SAN due to risk of loss and availability or another secure and backed alternative storage system</p>
	<p>Controlled access x Shared space x Central back-up x</p>	<p>Mandatory: Storage of classified data NOT PERMITTED</p>	<p><b>Mandatory:</b> Storage of classified data NOT PERMITTED</p>	<p>Mandatory: Storage not permitted due to risk of data loss and not being available to authorised users.</p>





Local Storage				
---------------	--	--	--	--

**Information Handling - Electronic/digital information storage**


Location	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non –Classified
 <p>School/Department Server</p> <p>Must be located within a Data Centre.</p>	<p>Controlled access x Shared space x Central back-up x</p>	<p><b>No storage or creation permitted unless</b> server located within one of the Data Centres managed by IT Services).</p> <p><i>Mandatory:</i> <i>Password protection.</i></p> <p><i>Mandatory:</i> Must be part of standard backup policy.</p>	<p><b>No storage or creation permitted unless</b> server environment is located within one of the Data Centres managed by IT Services).</p> <p><i>Mandatory:</i> Password protection</p> <p><i>Mandatory:</i> Must be part of standard backup policy.</p>	<p><i>Consider:</i></p> <p>Back-up and availability requirements</p>
 <p>Hosted Services</p>	<p>Controlled access ✓ Shared space ✓ Central back-up ✓</p>	<p>Use restricted access mechanisms where online access is shared</p> <p>Classification must be as specified by GCU.</p> <p>Risk assessed by IT Services</p>	<p>Use restricted access mechanisms where online access is shared</p> <p>Classification must be as specified by GCU.</p> <p>Risk assessed by IT Services</p>	<p>Permitted</p>

**Information Handling - Electronic/digital information storage**



Location	Default Features	Classified C1 <b>HIGHLY CONFIDENTIAL</b>	Classified C2 <b>CONFIDENTIAL</b>	NC <b>Non –Classified</b>
 <p><b>University desktop PC hard drive C: or D:</b></p>	<p><b>In non-public areas:</b> Controlled access ✓ Shared space ✗ Central back-up ✗</p>	<p>Encrypt drive Lock screen when unattended Storage not permitted</p>	<p>Encrypt drive Lock screen when unattended Storage not permitted</p>	<p>Lock screen when unattended Storage not permitted</p>
	<p><b>In public areas (e.g. Open Access PCs):</b> Controlled access ✗ Shared space ✗ Central back-up ✗</p>	<p><b>Not permitted</b> High risk of incidental disclosure</p>	<p><b>Not permitted</b> High risk of incidental disclosure</p>	<p>Lock screen when unattended Not permitted</p>
 <p><b>Personally owned (e.g. home) desktop PC hard drive C: or D:</b></p>	<p><b>Default Features:</b> Controlled access ✗ Shared space? Central back-up ✗</p>	<p><b>No creation/editing/storage of classified material permitted on device</b>  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.</p>	<p><b>No creation/editing/storage of classified material permitted on device</b>  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.</p>	<p>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 such as encrypted USB device.  No university documents are permitted to be stored on this personal device.</p>



--	--	--	--	--

**Information Handling - Electronic/digital information storage**



	Classified C1  HIGHLY CONFIDENTIAL	Classified C2  CONFIDENTIAL	NC  Non -Classified
 <p><b>University owned Laptop</b></p> <p><b>Default Features:</b>  Controlled access ✘  Shared space ✘  Central back-up ✘</p>	<p>Encrypt device – use strong password with maximum of 10 minutes inactivity until device locks.</p> <p>Use secure remote connection (e.g. Glasgow Caledonian University Portal or WebDav) to access files and avoid download or storage</p> <p>Do not use to store master copy of vital records</p> <p>Do not work on files in public areas</p> <p>Do not leave logged in and unattended</p> <p>Do not share use of device with non-University staff</p> <p><b>Mandatory:</b> Discuss with IT services back-up requirements</p>	<p>Encrypt device – use strong password with maximum of 10 minutes inactivity until device locks.</p> <p>Use secure remote connection (e.g. Glasgow Caledonian University Portal or WebDav) to access files and avoid download or storage</p> <p>Do not use to store master copy of vital records</p> <p>Do not work on files in public areas</p> <p>Do not leave logged in and unattended</p> <p>Do not share use of device with non-University staff</p> <p><b>Mandatory:</b> Discuss with IT services back-up requirements</p>	<p>Do not use to store master copy of vital records</p> <p>Do not leave logged in and unattended</p> <p>Do not share use of device with non-University staff</p> <p><b>Consider:</b> Secure remote connection due to risk of data loss and procedure to save to SAN on return to GCU IT network.</p>

**Information Handling - Electronic/digital information storage**




	Classified C1  HIGHLY CONFIDENTIAL	Classified C2  CONFIDENTIAL	NC  Non -Classified
 <p><b>Personally owned Laptop</b></p> <p><b>Default Features:</b> Controlled access ✕ Shared space ✕ Central back-up ✕</p>	<p><b>No creation/editing/storage of classified material permitted on device</b></p> <p>May be used for read only remote connection to view files if used in a private environment</p> <p>Do not download files to device.</p> <p>Do not leave logged in and unattended</p> <p>Clear browser cache after read only use.</p>	<p><b>No creation/editing/storage of classified material permitted on device</b></p> <p>May be used for read only remote connection to view files if used in a private environment</p> <p>Do not download files to device.</p> <p>Do not leave logged in and unattended</p> <p>Clear browser cache after read only use.</p>	<p><b>No master copy storage permitted</b></p> <p>May be used for remote connection to access files</p> <p>Do not leave logged in and unattended</p> <p>Created documents must be saved on University network or University owned device. Cannot reside on personal laptop.</p>
 <p><b>Personally owned Smartphone or tablet</b></p> <p><b>Default Features:</b> Controlled access ✕ Shared space ✕ Central back-up ✕</p>	<p><b>No creation/editing/storage of classified material permitted on device</b></p> <p>May be used for read only remote connection to access files if used in a private environment</p> <p>Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks.</p> <p>Encryption setting to be enabled where available.</p> <p>Clear browser cache after read only use.</p>	<p><b>No creation/editing/storage of classified material permitted on device</b></p> <p>May be used for read only remote connection to access files if used in a private environment</p> <p>Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks.</p> <p>Encryption setting to be enabled where available.</p> <p>Clear browser cache after read only use.</p>	<p><b>No master copy storage permitted</b></p> <p>May be used for remote connection to access files</p> <p>Created documents must be saved on University network or University owned device. Cannot reside on personal smartphone or tablet.</p>

	<p style="text-align: center;"><b>Classified C1</b></p> <p style="text-align: center;"><b>HIGHLY CONFIDENTIAL</b></p>	<p style="text-align: center;"><b>Classified C2</b></p> <p style="text-align: center;"><b>CONFIDENTIAL</b></p>	<p style="text-align: center;"><b>NC</b></p> <p style="text-align: center;"><b>Non -Classified</b></p>
<div style="display: flex; flex-direction: column; align-items: center;">   <p>University owned Smartphone or tablet</p> <p><b>Default Features:</b> Controlled access x Shared space x Central back-up x</p> </div>	<p>Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks.</p> <p>Encryption setting to be enabled where available.</p> <p>Services to locate device and remote wipe in case of loss/theft to be enabled.</p> <p>Do not leave device unattended in public areas.</p> <p>Do not share use of device with non-University staff</p> <p>Avoid storage of highly confidential information on device.</p> <p>May be used for secure remote connection (e.g. GCU Portal or WebDav) to access files but do not work on highly confidential files in public areas</p> <p><b>Consider:</b> Any back-up requirements</p>	<p>Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks.</p> <p>Encryption setting to be enabled where available.</p> <p>Services to locate device and remote wipe in case of loss/theft to be enabled.</p> <p>Do not leave device unattended in public areas.</p> <p>Do not share use of device with non-University staff</p> <p>Avoid storage of confidential information on device.</p> <p>May be used for secure remote connection (e.g. Glasgow Caledonian University Portal or WebDav) to access files but do not work on confidential files in public areas</p> <p><b>Consider:</b> Any back-up requirements</p>	<p>Do not leave device unattended in public areas</p> <p>Do not share use of device with non-University staff</p> <p><b>Consider:</b> Any back-up requirements</p>

**Information Handling - Electronic/digital information storage**

Location	Default Features	Classified C1 <b>HIGHLY CONFIDENTIAL</b>	Classified C2 <b>CONFIDENTIAL</b>	NC <b>Non -Classified</b>
 <p>Small capacity portable storage devices (e.g. USB, CD,)</p>	<p>Controlled access ✕ Shared space ✕ Central back-up ✕</p>	<p><b>Avoid use where possible</b></p> <p>Consider alternative means of transfer/access instead e.g. use secure remote connection (e.g. Glasgow Caledonian University Portal or WebDav) to access files with no download</p> <p>Use encrypted USB drive. Ironkey drives are available from IT services</p> <p>Do not use to store master copy</p> <p>Keep in lockable cabinet/drawer which is locked when unattended.</p>	<p>Use encrypted USB drive. Ironkey drives are available from IT services</p> <p>Not suitable for long term storage</p> <p>Do not use to store master copy</p> <p>Keep in lockable cabinet/drawer which is locked when unattended.</p>	<p>Not suitable for long term storage</p> <p>Do not use to store master copy</p>
 <p>Large capacity portable storage devices (i.e. external hard drive)</p>	<p>Controlled access ✕ Shared space ✕ Central back-up ✕</p>	<p>Permitted in limited circumstances only. Device must be encrypted to IS approved algorithm and the Senior Information Risk Owner must accept the risks associated should the data be lost.</p>	<p>Not Permitted in limited circumstances only. Device must be encrypted to IS approved algorithm and the Senior Information Risk Owner must accept the risks associated should the data be lost.</p>	<p>If these are required, contact IT Service Desk</p>

**Information Handling - Electronic Collaboration and Synchronisation**


	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
 Blackboard  University's virtual learning environment	Controlled access ✓ Shared space ✓ Central back-up ✓	No storage permitted	Requirement: Use restricted access folder	✓
 University collaborative workplace	Controlled access ✓ Shared space ✓ Central back-up ✓	Only where specifically setup for this level of security and with restricted recipients	If restricted to authorised recipients	✓
 External 'cloud' storage/file sync provider non-University contract e.g personal Onedrive, individually set up Dropbox accounts	Controlled access x Shared space x Central back-up x	No storage permitted	No storage permitted	Do not use to store master copy



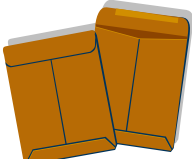
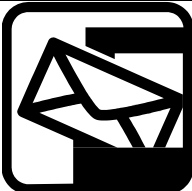

## Information Handling – Email

	Default Features	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
<p>From: @gcu.ac.uk To: @gcu.ac.uk</p> <p>Sending from University hosted email account to another internal email account</p>	<p>Controlled access ✓ Shared space x Central back-up ✓</p>	<p>Only as password protected attachment, marked confidential and double check recipient</p> <p>Consider whether sender or recipient may have delegated authority to others to access the account</p>	<p>Marked confidential and double check recipient</p> <p>Consider whether sender or recipient may have delegated authority to others to access the account</p>	<p>✓</p>
<p>From: @gcu.ac.uk To: @xxx.xxx</p> <p>Sending from University hosted email account to an external account</p>	<p>Controlled access ✓ Shared space? Central back-up ✓</p>	<p>Only as encrypted attachment, marked confidential, double check recipient and get their permission to use that account</p> <p>Consider whether sender or recipient may have delegated authority to others to access the account</p>	<p>As password protected attachment, marked confidential and double check recipient and get their permission to use that account</p> <p>Consider whether sender or recipient may have delegated authority to others to access the account</p>	<p>✓</p>
<p>From: @xxx.com To: @xxx.xxx</p> <p>Sending from an externally provided personal email account (e.g. hotmail, gmail etc)</p>	<p>Controlled access ✗ Shared space? Central back-up ✗</p>	<p>Not permitted</p>	<p>Not permitted</p>	<p>Not permitted- unless sending to @gcu.ac.uk</p> <p>Student information only to Caledonian.ac.uk</p>

**Information Handling - Paper records and other records storage**



	<p style="text-align: center;"><b>Classified C1</b></p> <p style="text-align: center;"><b>HIGHLY CONFIDENTIAL</b></p>	<p style="text-align: center;"><b>Classified C2</b></p> <p style="text-align: center;"><b>CONFIDENTIAL</b></p>	<p style="text-align: center;"><b>NC</b></p> <p style="text-align: center;"><b>Non -Classified</b></p>
 <p>Paper copies</p>	<p><b>Consider:</b> Protection from fire and flood damage</p> <p><b>In restricted access University areas:</b> <b>Requirement:</b> In lockable cabinet/drawer which is locked when not in active use. No papers left out unless being actively worked on. Segregate from routine files Consider sign out/in procedure</p> <p><b>In unrestricted access University areas:</b> <b>Not permitted</b></p> <p>Alternative: create as/convert to electronic documents and use secure remote connection with permitted device</p> <p><b>Off-site working:</b> <b>Not permitted</b></p> <p>Alternative: create as/convert to electronic documents and use secure remote connection.</p>	<p><b>Consider:</b> Protection from fire and flood damage</p> <p><b>In restricted access University areas:</b> <b>Requirement:</b> In lockable cabinet/drawer which is locked when office is unattended. No papers left out when desk unattended.</p> <p><b>In unrestricted access University areas:</b> <b>Requirement:</b> In lockable cabinet/drawer which is locked when not in active use. No papers left out unless being actively worked on.</p> <p><b>Off-site working:</b> <b>Requirement:</b> If needed to be taken off site a back-up copy must be made beforehand.</p> <p>Not to be left unattended and to be locked away in secure building when not in use.</p>	<p><b>In restricted access University areas:</b> ✓</p> <p><b>In unrestricted access University areas:</b> ✓</p> <p><b>Off-site working:</b> Consider making a back-up copy before taking off site</p>

**Information Handling - Paper and other media transmission**

	Classified C1  HIGHLY CONFIDENTIAL	Classified C2  CONFIDENTIAL	NC  Non -Classified
 Internal postal service	<p><b>Not permitted</b> In sealed envelope marked confidential and with full addressee and sender details. Hand deliver</p> <p><b>Consider:</b> Making a back-up copy before providing</p>	<p><b>Requirement:</b> In sealed envelope marked confidential and with full addressee and sender details. Consider hand delivering.</p> <p><b>Consider:</b> Making a back-up copy before posting</p>	<p>✓</p> <p><b>Consider:</b> Making a back-up copy before posting</p>
 External postal service	<p><b>Requirement:</b> Via tracked and delivery recorded service, double wrapped (2 envelopes) and marked confidential.</p> <p><b>Consider:</b> Making a back-up copy before posting</p>	<p><b>Requirement:</b> Via tracked and delivery recorded service, and marked confidential.</p> <p><b>Consider:</b> Making a back-up copy before posting</p>	<p>✓</p> <p><b>Consider:</b> Making a back-up copy before posting</p>
 Fax machine	<p><b>Requirement:</b> Ensure that the recipient has verified number and security of receiving machine and is at machine awaiting receipt</p> <p><b>Consider:</b> Converting to an electronic format and using secure electronic transfer method instead e.g. Fastfile Ensure that the Fax Cover Sheet includes: Name and contact Details of sender Mark Highly Confidential</p>	<p><b>Requirement:</b> Ensure that the recipient has verified number and security of receiving machine and is at machine awaiting receipt</p> <p><b>Consider:</b> Converting to an electronic format and using secure electronic transfer method instead e.g. Fastfile Ensure that the Fax Cover Sheet includes : Name and contact Details of sender Mark Confidential Address to a named individual</p>	<p>✓</p>

	Address to a named individual Remove from machine immediately after sending or receiving it and file	Remove from machine immediately after sending or receiving it and file	
--	---	--	--

**Information Handling – Scanning, printing/photocopying**

	Classified C1  HIGHLY CONFIDENTIAL	Classified C2  CONFIDENTIAL	NC  Non -Classified
 Any other reproduction	<p><b>Requirement:</b> Restrict the making of copies to only when it is not viable for people to access the master copy.</p> <p><b>Consider:</b> Control access to printing output on copier.</p> <p>Pro-actively protect against accidental compromise, for example don't leave in copiers, check all pages retrieved.</p>	<p><b>Requirement:</b> Restrict the making of copies to only when it is not viable for people to access the master copy.</p> <p><b>Consider:</b> Control access to printing output on copier.</p> <p>Pro-actively protect against accidental compromise, for example don't leave in copiers, check all pages retrieved</p>	<i>No Special Measures</i>
 Telephone conversations	<p><b>Requirement:</b> Ensure conversations cannot be overheard.</p> <p>Manage calls to ensure only authorised individual present.</p>	<p><b>Requirement:</b> Ensure conversations cannot be overheard.</p> <p>Manage calls to ensure only authorised individual present.</p>	No Special Measures

### **Annex 3**

#### **Glossary of terms used in Information Classification and Handling Policy Document**

Classified Data	Sensitive or Personally Identifiable data.
Data Sharing Agreement/Data Processing Agreement	An agreement in place where the University transfers personal data to a third party which outlines the data being processed, the purposes and the arrangements.
Default Features	Settings that are factory set or settings that are the basic settings for any system or function.
Desktop e.g. My Documents, C Drive	Hard Drive disks located within individual desktop machines.
Double Check Recipient	Confirm recipient is as intended.
Encryption	Codify data by using a digital algorithm, thereby making the data only readable by a device that has been given the same key to the algorithm.
Hard Drive	The data storage device contained within an individual workstation or laptop.
Hosted Service	A software system provided by an external company. The system will be located off campus within the external company's premises.
Information classification	Degrees of classification that indicate the sensitivity/risk associated with the data.
Information Asset Owner	The responsible manager leading the relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is moved and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used. Sometimes called the Information Risk Owner.
Ironkey Drives	The encrypted USB drive provided by GCU to allow the secure transportation of data.
Master Copy	The original document in any series of documents.
Non-Public Data	Data that does not originate from the public domain i.e. the internet.
Originator	The primary author of any document or data, responsible for initial classification
Personal Data	Data relating to any living individual, who can be identified from that data.
Recipient	The first recipient of any document or data within the University, who assigns a

	classification.
Restricted Access Mechanisms	Mechanisms that prevent the unauthorised access to any prescribed data. Such as password protection on shared drives or on individual documents.
Sensitive Personal Data	Personal data consisting of information as to: (a) the racial or ethnic origin (b) political opinions (c) religious beliefs or other beliefs of a similar nature (d) membership of a trade union (e) physical or mental health or condition (f) sexual life (g) the commission or alleged commission of any offence or (h) any proceedings for any offence committed or alleged to have been committed.
Service Level Agreement (SLA)	A contract of expected performance between two discrete departments or companies.
Senior Information Risk Owner	Executive Member with responsibility for that area of university function with responsibility for: The risk profile of the area. Identifying all risks. Making sure that appropriate mitigations are in place so that risks can be accepted.
Storage Area Network (SAN)	A large storage server with multiple drives that is connected via fibre optic cables to the network that provides very fast and secure access.
Third Party	A provider or contractor who is not part of GCU.
University's Secure Environment	Physical: Data centres located within GCU which are strictly controlled. Digital: Controlled access via permissions.