



Policy

Encryption of Portable Computer Devices

Document Filename	Encryption of Portable Computer Devices Policy.docx
Version	1.2
Information Classification	Open
Status	Approved
Date	19 October 2017
Policy Owner	Brian Fitzsimmons
Policy Contact	b.fitzsimmons@gcu.ac.uk

Document Approval and Version Control

Title		Name of Approvers			Date
Encryption of Portable Computer Devices Policy		Glasgow Caledonian University Executive Board			19/10/2017
Revision	Status	Author (s)	Reviewed By	Approved By	Issue Date
1.0	Draft	Brian Fitzsimmons	Mark Johnston, Hazel Lauder, Information Management Forum		
1.1	Draft	Brian Fitzsimmons	Information Governance Committee		
1.2	Approved	Brian Fitzsimmons		Executive Board	19/10/2017

Contents

Section	Content	Page
1	Document Overview	3
1.1	<i>Purpose</i>	3
1.2	<i>Scope</i>	3
1.3	<i>Definitions</i>	3
1.4	<i>Supporting Documents</i>	3
2	Policy	4
3	Review	4
4	Breaches of Policy	4
5	Information	4
6	Policy Awareness	4
7	Guidance	4

1 Document Overview

1.1 Purpose

The purpose of this policy is to maintain the confidentiality, integrity, availability and value of the University's information assets when being sent or used out with the University's networks.

1.2 Scope

This policy applies to all staff, students and visitors' accessing, storing and transmitting University information classified as confidential or highly confidential.

1.3 Definitions

University: Glasgow Caledonian University is a Scottish Registered Charity, No. C021474 with its registered office at Cowcaddens Road, Glasgow G4 0BA, Scotland, UK.

Staff: Staff are salaried members of the University or individuals contracted by or to the University to provide a service.

Student: A person pursuing any course of study at the University.

Visitor: A visitor is anyone, not a member of staff or student, requiring access to University services or premises.

User: A member of staff, student or visitor who has been authorised by the University to use University IT Facilities and to gain access to University networks and information systems.

Information: The result of processing, manipulating, or organising of data. Examples including but not limited to, text, images, sounds, codes, computer programmes, software and databases.

Information System: Any information processing system procured by and licensed to the University for Use in any of its IT Facilities.

Encryption: The process of taking plain text and using a key to convert it into cipher text. Ciphers, algorithms, or schemes are used to encrypt data. All encryption algorithms require the use of a key, and must be able, with the proper key, to be reversed, converting the cipher text back into the original plain text.

Portable Computer Device: Any device, that has been purchased by and is owned by the University that can be easily transported and has the capability and capacity to store information digitally; for example laptop, USB, tablet, smart phone, external hard drive.

Personal Device: A device that has been purchased by and is owned by the member of staff, student or visitor, and not the University.

1.4 Supporting Documents

Information Classification and Handling Policy, Information Systems Policy, Encryption Procedure

Document Filename	Encryption of Portable Computer Devices Policy.docx
Version	1.2
Information Classification	Open
Status	Approved

2 Policy

It is University policy to encrypt all portable computer devices that are used to store University information which has been classified as confidential or highly confidential.

It is the University's policy to encrypt all information classified as confidential or highly confidential when it is transmitted out with University's networks.

Information which has been classified as confidential or highly confidential and is transmitted out with the University network to a third party, unencrypted, must be recorded as a risk in the departmental risk register.

3 Review

The Information Governance Committee is responsible for keeping this policy current. This policy will be reviewed annually or more frequently as required.

4 Breaches of Policy

A breach of University policies, rules or regulations is considered as an issue of potential misconduct, which will be dealt with as a disciplinary matter under the University's Conduct & Capability policy. If there is anything in this policy that you do not understand, please discuss it with your line manager.

5 Information

If you have any questions regarding this policy please contact the University's Information Security Team via the IT Service Desk.

6 Policy Awareness

All individual users of University IT Facilities and information systems must comply with the appropriate information security policies, regulations, code of conducts, guidelines and practises and procedures including any external accountability.

It is a condition of use of the IT Facilities that a user's activity may be logged and or monitored and that information in their IT account, including but not limited to, files, images, documents, audio, videos, browsing history, communication history, may be accessed and processed with or without their consent as outlined in the **Monitoring and Accessing Information policy**.

7 Guidance

For guidance and further information please go to

<https://www.gcu.ac.uk/staff/it/itregulationspolicies/>

