Policy
Remote Access to Information and Information Systems

Document Approval and Version Control

Title	Name of Approvers	Date
Remote Access to Information and Information Systems	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

1   Document Overview

1.1   Purpose

The purpose of this policy is to ensure that staff, students or visitors accessing University information and University information systems from a remote location using a portable computer device, do not expose the University to increased legal or governance risk and understand the risks and responsibilities associated with remote working and restrict the distribution of personal and classified information.

1.2   Scope

This policy applies to all staff, students and visitors accessing University information or University information systems.

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.

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. For example laptop, USB, tablet, smart phone, external hard drive.

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

Remote working: Where a person works from a location other than the registered work place.

1.4   Supporting Documents

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

2   Policy

The University provides its staff, students and visitors with the facilities, technical infrastructure and opportunities to work remotely using portable computer devices. Any portable computer device used for remote working, which involves the use of storing information that is classified as confidential or highly confidential, must be owned by the University, be encrypted and protected by means of a password or personal identification number (PIN).

Any portable computer device used for remote administrative access to University information systems, by members of staff with elevated access privileges, must be owned by the University, be encrypted and protected by means of a password or PIN. Remote administrative access to University information systems must be protected by means of a password.

Personal computer devices must not be used to store information that is classified as confidential or highly confidential.

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

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