



## Policy

### Monitoring and Accessing Information

Document Filename	Monitoring and Accessing Information.docx
Version	1.1
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
Monitoring and Accessing Information		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		
1.0	Draft	Brian Fitzsimmons	Information Governance Committee		
1.1	Approved	Brian Fitzsimmons		Executive Board	19/10/2017

## Contents

Section	Content	Page
<b>1</b>	<b>Document Overview</b>	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>	4
<b>2</b>	<b>Policy</b>	5
<b>3</b>	<b>Review</b>	5
<b>4</b>	<b>Breaches of Policy</b>	5
<b>5</b>	<b>Information</b>	5
<b>6</b>	<b>Policy Awareness</b>	6
<b>7</b>	<b>Guidance</b>	6

## 1 Document Overview

### 1.1 Purpose

This policy outlines the circumstances in which it is permissible for the University to monitor the use of IT Facilities including internet use and or to gain access to information stored in a user's IT account with or without the users consent.

### 1.2 Scope

This policy applies to staff, students and visitors, in all registered University locations, who have been authorised by the University to use University IT Facilities to gain access to University information and information systems.

This policy applies to all University information regardless of type, location of storage and the device used for storage.

This policy applies to any other information that is transmitted using University or JISC communications networks.

### 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.

**IT Account:** An account issued by the University to users which allows the user access to University networks and information systems to process and store information on 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 digitally; for example laptop, USB, tablet, smart phone, external hard drive.

**Fixed Computer Device:** Any device, that has been purchased by and is owned by the University that is fixed to a location and has the capability and capacity to store information digitally; for example a desktop PC, a desktop workstation, a computer server.

**University IT Facilities:** All University owned or leased accommodation which houses computer hardware or software which in turn is owned, leased or licensed to and operated by the University. This includes;

- Computer hardware and software owned by, leased or licensed to the University and connected to the University network (s) by whatever means
- Computer hardware and software owned by, leased or licensed to the University and not connected to the University network (s)
- All networking, data processing and information and communications systems, including connections to external computers or networks including systems accessed through commercial or other arrangements

#### **1.4 Supporting Documents**

***Information Classification and Handling Policy, Acceptable Use of IT Facilities Policy.***

## 2 Policy

The University will not undertake monitoring of the use of IT Facilities of a specific user or provide access to information in a user's IT account except for those purposes identified in this policy. As University policy allows personal use of IT Facilities, subject to certain conditions, users need to be aware that personal information could be inadvertently accessed, without their consent, as per the circumstances outlined in this policy.

Monitoring of and or accessing a user's information or browsing history via their IT account or the University web filter will be made in accordance with legislation; this includes the Data Protection Act 1998 and the Telecommunications (Lawful Business Practice) (Interceptions of Communications) Regulations 2000.

Monitoring of and or accessing a user's information or browsing history via their IT account or University web filter without their consent will only take place under the following circumstances;

- To prevent, detect or assist in resolving crime
- To prevent or detect an illegal act from taking place
- In the interests of national security
- To ensure business continuity; for example, in cases of unplanned staff absence or when staff leave the University
- To establish the existence of facts relevant to the University business
- To investigate or detect unauthorised use of the University's information systems
- When the University is required by law to disclose information; for example a Subject Access Request or Court Order
- To confirm compliance with regulatory or self-regulatory practices or procedures relevant to University business
- To ascertain or demonstrate standards which are achieved or ought to be achieved by persons using the system in the course of their duties

## 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 this policy.

## **7 Guidance**

For guidance and further information please go to

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