

IT Acceptable Use Policy

|  |  |
| --- | --- |
| **POLICY TITLE** | IT Acceptable Use Policy |
| **DATE APPROVED** | 1 December 2021 |
| **APPROVING BODY** | Management Board |
| **VERSION** | 1.3 |
| **PREVIOUS REVIEW DATES** | This Policy was previously known as the Electronic Communications Policy (approved in 2016), which was reviewed and updated to create the Information Security Policy and IT Acceptable Use Policy |
| **NEXT REVIEW DATE** | September 2024 |
| **OUTCOME OF EQUALITY IMPACT ASSESSMENT** | No major change |
| **RELATED POLICIES / PROCEDURES / GUIDANCE** | The policy forms part of the Information Security Policy Framework and is related to:* Information Security policy
* Data Protection Policy
* Data Management and Governance Policy
* Janet/Jisc regulations: (https://community.jisc.ac.uk/library/acceptable-use-policy)
* Staff Disciplinary Policy
* Student Disciplinary Procedure
 |
| **IMPLEMENTATION DATE** | Immediate |
| **POLICY OWNER (JOB TITLE)** | User Support Services Manager |
| **UNIT / SERVICE** | Library and Information Services |
| **CONTACT EMAIL** | emtaylor@cardiffmet.ac.uk |

# Version Control

|  |  |  |
| --- | --- | --- |
| **VERSION** | **DATE** | **REASON FOR CHANGE** |
| 1.0 | September 2021 | Initial release for consultation |
| 1.2 | November 2021 | Feedback to section on bullying and harassment following consultation |
| 1.3 | 1.12.21 | Updated following feedback at Management Board on 1.12.21 |

**Mae'r ddogfen hon hefyd ar gael yn Gymraeg** / This document is also available in Welsh

Contents

[1 Introduction 3](#_Toc82764195)

[2 Purpose 3](#_Toc82764196)

[3 Scope 3](#_Toc82764197)

[4 Roles and Responsibilities 4](#_Toc82764198)

[5 Definitions 5](#_Toc82764199)

[6 IT Acceptable Use Policy Principles 6](#_Toc82764200)

[7 Expectations Upon Users 7](#_Toc82764201)

[8 Prohibited Activity 8](#_Toc82764202)

[9 Monitoring and Privacy 9](#_Toc82764203)

[10 Business Continuity and Exit Procedures 10](#_Toc82764204)

[11 Incident Reporting 11](#_Toc82764205)

[12 Related Policies and Procedures 11](#_Toc82764206)

[13 Review and Approval 11](#_Toc82764207)

# Introduction

## Information, in all its forms, is a primary asset of the University.  Its effective curation and security are critical to maintaining and supporting the University’s operations, its financial viability and reputation.

## This Policy sets out the responsibilities and required behaviours of all users of IT facilities provided by Cardiff Metropolitan University.

## It should be read in conjunction with the other policies and procedures that form part of the Information Security Policy Framework.  These are:

### *Information Security Policy*: This Policy sets out all the steps taken by the University to safeguard its information assets. It provides the overarching framework for information security at Cardiff Metropolitan University

### *Data Protection Policy*: This Policy sets out how the University complies with its legal obligations in relation to the processing of personal data as set out in the UK General Data Protection Regulations (UK GDPR)

### *Data Management and Governance Policy*: This Policy describes the arrangements the University puts in place to assure the integrity and quality of data across all its systems.

## All staff are expected to be aware of this policy and to comply with its provisions as is required by the Cardiff Met Code of Professional Conduct.

# Purpose

## The IT Acceptable Use Policy (IT AUP) is a statement of user responsibilities and expectations with respect to IT resources.

## The main purpose of the IT AUP is to ensure responsible and appropriate use of IT resources; to maximise the availability of IT resources for legitimate purposes; and to minimise exposure to misuse from inside or outside the University.

## University IT resources are provided on condition that they are used for acceptable, authorised purposes only, and therefore use of these resources is subject to compliance with the guidance within this policy.

## The University shall refer the matter to the appropriate law enforcement agencies, and any other organisations whose regulations may have been breached. The University accepts no liability where such steps are taken.

# Scope

## This policy applies to:

### The use of IT resources provided by Cardiff Metropolitan University

### The use of IT resources owned by other bodies, access to which has been provided by Cardiff Metropolitan University. In such cases, any regulations provided by either body applies. In the event of a conflict between regulations, the more restrictive takes precedence.

### All users of IT resources provided by Cardiff Metropolitan University, including staff, students, Governors and any agents or visitors granted access to such resources.

# Roles and Responsibilities

## The senior manager with overall responsibility for Information Security is the Director of Library and Information Services.

## The Head of Information Services has operational authority for the security of information within the University and develops policies and procedures that underpin the controls needed.

## The IT User Support Manager is the Policy Owner and has operational responsibility for user support services and implementation of this Policy.

## The Digital Strategy Committee (DSC) has executive oversight for information security within the University. DSC has responsibility for overseeing the management of the information security risks to the University's staff and students, its infrastructure and its information

## The Information Compliance Community of Practice includes representation from each School and Unit. Its members are expected to act as champions for good information security and governance in their areas and to support, guide and help to develop best practice.

## All staff, students and third parties with access to University IT resources should adhere to all policies, procedures and guidance relating to information security at the University as outlined in this Policy and undertake training as mandated.

## Breaches of the Acceptable Use Policy are regarded as serious and may result in disciplinary action, including possible charges of misconduct or gross misconduct. You must co-operate fully and truthfully in any security investigation irrespective of your status in the investigation e.g. the subject of the investigation or a witness. The University will co-operate fully with the police in any investigation relating to unlawful activities conducted using University ICT equipment or systems. We will notify the police as appropriate of acts we believe to be illegal and will disclose evidence to them where there is reasonable suspicion of criminal activity. If an investigation proves that you have accessed material that contravenes the categories set out in Section 8 - Prohibited Activity, without full disclosure to, and formal approval from, the University in advance, this could be considered gross misconduct. Disciplinary procedures will be initiated which may lead to sanctions up to and including summary dismissal.

## Questions about this Policy should be directed to Information Services (ithelpdesk@cardiffmet.ac.uk) or by accessing further guidance from <https://study.cardiffmet.ac.uk/IT/Pages/Home2.aspx>

# Definitions

## This policy uses terms that are defined below:

### *User/Users*: Any person or persons making use of the University’s IT resources. This includes but is not limited to:

* + - All Cardiff Metropolitan University staff and students
		- Authorised individuals, requiring access to IT resources for university business
		- Individuals accessing the institution’s online services
		- External partners and contractors using Cardiff Metropolitan University’s services
		- Halls residents
		- Visitors using University WiFi
		- Students and staff from other institutions using Eduroam on campus

### *Authorised System Administrator*: A member of staff who administers or has access to administer a Cardiff Metropolitan University IT system.

### *System Owner*: The individual responsible for a given systems’ provision.

### *Misuse of IT Resources:* Examples include but are not limited to:

* + - * Attempts to access or to facilitate access to computers, data, network equipment or information transmitted over the University network for which the individual is not authorised.
			* Unauthorised resale of Cardiff Metropolitan University data or services.
			* Attempts to damage or deny service to computer or network systems.
			* Attempts to monitor data on the University’s network
			* Deliberately scanning for or attempting to make use of any security bug or weakness.
			* Deliberately introducing malware into any IT resources, or taking action to circumvent precautions taken by the University to prevent this.
			* Use of University resources to bully, harass or cause distress to others.

### *Information Technology Resources (IT Resources)*: For the purposes of this Policy, University IT resources are defined as:

* + - * IT equipment (e.g. computers, printers, university network wired and wireless, multi-function devices, audio visual facilities)
			* Any information technology facilities or services provided by the university (e.g. computer rooms, the network, online services)
			* Software, whether locally installed or cloud based (e.g. Office365, Finance system, VLE)
			* Communication/storage of information and any operation involving the capture, manipulation, transmission or viewing of data by electronic means, within the University, within the UK or internationally.
			* The University telephone system.

# IT Acceptable Use Policy Principles

## University IT resources, including an IT account, are provided for staff to support their employment, students to support their university education, and for other authorised individuals to support University business.

## The University does not prohibit users from reasonably using IT resources for personal non-commercial use, subject to adhering to the principles of this policy. However, members of staff should not use a personal (non-University provided) email account to conduct University business and should maintain a personal email account for personal email correspondence.

## Where a potential user does not require access to IT resources for the purposes of their employment or studies there is no obligation on the University to provide access.

## University IT resources must be used in an approved, ethical and lawful manner to avoid loss or damage to University operations, reputation, or financial interests.

## Where University IT resources are being used to access other resources, any action deemed abuse by the regulations of that resource, or illegal under UK law, this will be regarded as misuse under this Policy and appropriate action will be taken.

## Use of IT facilities for non-institutional commercial purposes or for personal financial gain is not permitted.

## Cardiff Metropolitan University internet access is provided by the Joint Academic Network (JANET), and therefore this Policy is taken to include Acceptable Use Policy (AUP) for this Network.

## The terms of the various software and data licence schemes under which the University has agreed access also apply to the use of the relevant systems.

# Expectations Upon Users

## Access to Cardiff Metropolitan University IT resources is subject to users meeting the following responsibilities and expectations:

### Users handling, accessing or storing personal, confidential or sensitive information, must take all reasonable steps to safeguard it and must observe the University’s Data Protection Policy and related guidance. Where University or user owned mobile devices (e.g. laptops, tablets, smartphones, voice recorders) are used to store or access personal, sensitive or confidential data owned by the University, they must be encrypted and protected by appropriate security controls.

### All users of University IT resources must ensure that any personal computer or device, for which they have responsibility and which is attached to the University network (wireless or wired), is adequately protected against viruses, malware and other malicious software through the use of up-to-date antivirus software and ensuring that operating system patches are applied regularly.

### All individually assigned username and passwords and any other IT credentials are for the exclusive use of the individual to whom they are allocated. Passwords must not be divulged, even to authorised system administrators or system owners. Users who inadvertently disclose their IT account password must change their password immediately, and notify the IT Helpdesk on 029 20417000 to ensure action can be taken to limit the impact of such exposure.

### Users connecting to sensitive or confidential information from off campus must use an approved connection method that ensures adequate security. Guidance on remote working is provided on the Study website. <https://study.cardiffmet.ac.uk/IT/Flash/Pages/WorkingAwayFromCampus.aspx>

### Users must seek guidance or training where they do not feel confident in how to work with sensitive information or systems that contain sensitive information.

### Users must follow guidance and policies for the use of resources where available.

### Users must adhere to the terms and conditions of license agreements relating to IT resources. Observance of this Acceptable Use Policy will normally meet such requirements. Where software is procured by a user or department the provisions of the license must be complied with.

### Users should have regard to the intellectual property rights of third parties, particularly when downloading, forwarding and using materials that are copyrighted or contain branded materials, examples include logos, pictures, text, video files, and icons.

### When University owned IT equipment is no longer required, it must be returned to Information Services, to either be configured for re-use or disposed of. Data will be wiped before either configuring for a new use or disposing via a WEEE directive compliant process. Users must ensure all data of value is stored in a suitable location (e.g. University cloud storage) as any locally stored data will be destroyed.

### If users are provided with a loan machine, they should ensure that data is stored in University cloud storage and not locally on the device, as any such data will be destroyed following return.

### Users must adhere to Cardiff Metropolitan University Social Media Guidelines.

### Users should be aware that if they are using services that are hosted in a different part of the world, then they may also be subject to foreign laws and jurisdiction.

### Users shall ensure that sending of personal data is strictly necessary and in compliance with the University’s Data Protection Policy. In considering whether to store or send confidential or sensitive information using University IT resources, users should note the monitoring provisions in this policy, and also that all electronically stored information (including emails and chat) can be the subject of a Freedom of Information request.

### Where use of IT resources would contravene this Acceptable Use Policy but is required for legitimate university business, users should request a partial exemption of the relevant part of this policy. Requests should be made in writing detailing the reasons for the request. Requests related to academic research will need to be approved by the relevant ethics committee and other requests should be made through the line management structure with written approval given by the relevant Dean or Director of Service. Any request to access material that contravenes categories in Section 8 is required to detail the full extent and time-period needed. Contravention of this Policy without written approval and/or accesses attempted outside of the parameters of the approval given is likely to result in disciplinary action.

### Users should be aware that the University has a statutory duty to prevent people from being drawn into terrorism (under the Counter-Terrorism and Security Act 2015, known as the “Prevent Duty”). The Duty requires the University, in the exercise of its functions, to have due regard to the need to prevent people from being drawn into terrorism. Users must not carry out any acts which could incite or promote extremism including, but not limited to, accessing websites or sharing material that might be associated with extremist or terrorist organisations.

# Prohibited Activity

## Users of Cardiff Metropolitan University IT resources are prohibited from the following:

### Using IT resources in any way that is fraudulent, offensive, obscene, racist (see [Harassment and Bullying Policy](https://www.cardiffmet.ac.uk/about/policyhub/Documents/harassment-and-bullying-policy-statement-01-2021.docx)), malicious, defamatory, libellous, abusive, illegal pornography, or constitutes a criminal offence (directly or indirectly), or which promotes extremism / terrorism and / or could constitute grooming children or other crimes against minors.

### Using IT resources in a way that is designed or likely to cause harassment, bullying, annoyance, needless anxiety, unnecessary inconvenience, upset to another, or breaches confidentiality. [Harassment and Bullying Policy](https://www.cardiffmet.ac.uk/about/policyhub/Documents/harassment-and-bullying-policy-statement-01-2021.docx)

### Sending / posting unsolicited advertising, spam, or sending messages that purport to come from an individual other than the person sending the message.

### Breaching a third party’s intellectual property rights, including but not limited to licences, copyright, trademarks or music piracy.

### Any activity that may be described as “hacking”. Hacking is defined here as the intent to cause, or actions committed knowing they are likely to result in wrongful loss, damage or alteration to information, or action that attempts to gain or provide unauthorised access to an IT resource.

### Corrupting or destroying either University or third-party data or information with intent to cause damage or disruption. It is against the law to destroy information required for a Freedom of Information Act or the UK General Data Protection Regulation.

### Deliberately wasting staff time or IT resources (e.g. network bandwidth, processing power). Users shall take reasonable care to not disrupt the work of others and are prohibited from using IT resources in a way that denies service to other users.

### Installing or reconfiguring software on computers provided for student use without consultation with Information Services.

### Connecting any device that extends the university network – (e.g. wireless access points, routers,) without the consent of Information Services.

### Use of IT resources for private commercial use, including, but not limited to private/personal consultancy unless approved by Cardiff Metropolitan University.

### Disposal of IT equipment other than in line with University guidance.

### Users must not attempt to monitor the use of IT resources this would include monitoring or capture of network traffic, installation or use of key logging or screen capture software affecting other users, attempting to access system logs.

# Monitoring and Privacy

## The University is required to inform users about how it will protect the privacy of their communication and data. Users should be aware that to permit the detection and investigation of infringement of Universities policies and UK law, system administrators have access to information which includes but is not limited to the following:

* + - * Usage Logs for access to the University’s IT resources.
			* Network traffic
			* Data stored by users using University IT resources.
			* CCTV recordings
			* Geolocation data of University owned equipment.

## The University reserves the right to monitor and/or record communications and data as it deems appropriate under the following circumstances:

* + - * To establish the existence of facts to ascertain compliance with UK law or University regulations or procedures
			* In the interests of national or international security
			* To comply with lawful requests for information from government and law enforcement agencies
			* To prevent or detect a crime
			* To investigate or detect unauthorised use of systems, and, where necessary following the authorisation of a member of the University’s senior executive team report such unauthorised use to the police
			* To secure, or as an inherent part of, effective system operation.

## Any requests to monitor and/or record communications and data, will be referred to the University Secretary for permission to be granted. The University Secretary will seek guidance from the University’s Information and Data Compliance Officer, Director of People Services or Director of Registry Services as appropriate, and may seek legal advice, to inform the decision as to whether permission will be granted. In the absence of the University Secretary, the Head of Compliance will provide such permission. In cases where there might be a conflict of interest for the University Secretary, two members of the Vice-Chancellor’s Executive Group will provide the decision.

## Any monitoring shall be in accordance with the UK General Data Protection Regulation (UK GDPR) and relevant legislation as listed in [Annex 1](#_Relevant_Legislation:).

## System administrators or staff in Information Services may copy user data or lock accounts to preserve evidence until such time as approval for further investigation is granted.

# Business Continuity and Exit Procedures

## Where a user is unable to fulfil their duties at the University (for example on sick leave, maternity leave, annual leave, or if a user has left the university) the University reserves the right to access a user’s documents and email, in order to ensure continuity of University business. Such requests for access should be made by the relevant Dean or Director to the Director of People Services. In the absence of the Director of People Services, a member of the Vice-Chancellor’s Executive is required to approve such requests.

## Where access to a user’s data is approved for business continuity purposes, it may be appropriate to inform the user this has occurred.

## Users should not divulge their passwords but should ensure relevant data is appropriately shared in advance of any expected absence.

## When a member of staff leaves the University, access to their IT account will be disabled immediately. The account will be deleted after 12 months.

## When a student leaves the University, they will lose the ability to log in to University computers, and access to most systems. They will retain limited access to certain web resources for a period of one year.

## All users should ensure that before they leave the University that they return all University owned equipment.

# Incident Reporting

## Any suspected breaches of this Acceptable Use Policy should be reported immediately to Information Services.

## A user should not attempt to conceal a breach or suspected breach, doing so could lead to disciplinary action.

## The University has whistleblowing and complaints policies. This allows any individuals who have concerns over another person’s actions to raise these formally.

# Related Policies and Procedures

## This Policy should be read in conjunction with the following related University policies and procedures:

* + - Information Security Policy
		- Data Protection Policy
		- Data Management and Governance Policy
		- Staff Disciplinary Policy
		- Student Disciplinary Procedure
		- Cardiff Met Code of Professional Conduct

## Copies of all the University’s policies can be found via <https://www.cardiffmet.ac.uk/about/policyhub/>

# Review and Approval

## The policy will be reviewed and updated every three years unless legislative or statutory changes necessitate earlier review.

## The approval authority is the University's Management Board.

Annex 1

# Relevant Legislation:

## Legislation relevant to the use of IT resources in the UK includes, but is not limited to:

* Obscene Publications Act 1959 and 1964
* Protection of Children Act 1978
* Police and Criminal Evidence Act 1984
* Copyright, Designs and Patents Act 1988
* Criminal Justice and Immigration Act 2008
* Computer Misuse Act 1990
* Human Rights Act 1998
* UK General Data Protection Regulation
* Regulation of Investigatory Powers Act 2000
* Prevention of Terrorism Act 2005
* Terrorism Act 2006
* Counter-Terrorism and Security Act 2015
* Police and Justice Act 2006
* Freedom of Information Act 2000
* Equality Act 2010
* Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) Defamation Act 1996 and 2013