Cardiff Metropolitan University | Prifysgol Metropolitan Caerdydd

Policy Owner - Director of Library and Information Services

Electronic Communications Policy

Established: April 2001
Version Number: 5.6c
Impact Assessed: TBC
Revised: June 2016

1. Introduction

1.1 This policy covers the use of all IT facilities and network connectivity administered by Cardiff Metropolitan University and any usage of Internet based services that may be done in connection with its business or learning. It covers usage from all locations, including from home, at other institutions or from the workplace and applies to staff and students, as well as any other third parties who may be granted access.

1.2 Breaches of this policy may be dealt with under the relevant disciplinary procedure and may, where an offence has occurred under any current law or regulation, be reported to the police, or other appropriate authority.

1.3 Any IT security related incidents and suspected weaknesses in the organisation's business operations and information processing systems should be reported by email to itsecurity@cardiffmet.ac.uk or to one of the Information Services Division Management team either directly or through IT Helpdesk.

2. Personal Use of Cardiff Metropolitan University IT Services

2.1 Although Internet and email access is intended to be used for institutional purposes, it is appreciated that there may be occasions when the system and/or the facilities need to be used for personal purposes. Any such usage must be carried out without contravention of this policy. Priority must always be granted to those needing to use open-access facilities for academic or other essential work.

2.2 Cardiff Metropolitan University business email addresses should not be used for sending and receiving personal communications and should not be used for registration on to any internet services unless these are to be used for business or academic purposes.

3. Monitoring and Investigation of IT Services

3.1 If there are grounds for suspecting that these regulations have been breached then full and unrestricted access to relevant data, email and computer files may be authorised. Further steps may also be taken such as immediate suspension of a user's authorisation to use the IT facilities and removal of any content, where this is necessary. Such actions will generally need to be authorised by a member of Vice-Chancellor's Board.

3.2 Cardiff Metropolitan University reserves the right to monitor its network and equipment usage and to access any material held on computer to check compliance with this policy. It shall be at the sole discretion of Vice-Chancellor's Board, which should be exercised reasonably, to decide whether or not material held or distributed is in breach of the conditions identified in this policy.

4. Disclaimers on Use of IT Services

4.1 Cardiff Metropolitan University makes no representations about the suitability of its IT services for any purpose. All warranties, terms and conditions with regard to this service, including all warranties, terms and conditions, implied by statute, or otherwise, of satisfactory quality, fitness for a particular purpose, and non-infringement are excluded to the fullest extent permitted by law.

4.2 Cardiff Metropolitan University shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of services, or with any delayed access to, or inability to use the services and whether arising in tort, contract, negligence, under statute or otherwise. Nothing in these terms excludes or limits liability for death or personal injury caused by the negligence of Cardiff Metropolitan University in providing the service.

5. Regulations

5.1 General

5.1.1 Any use of IT services and equipment in the UK is bound by the laws and legislation of the UK. Further information on relevant legislation is available on the IT Security page (Computer Legislation tab).

5.1.2 Whilst on-campus all parties must also adhere to any local regulations relevant to Learning Centres or departmental IT rooms and must respect the rights of others, conducting themselves in a quiet and orderly manner when using IT facilities.

5.1.3 Whilst using an individual IT or external Internet service all parties must adhere to any specific regulations for that service.

5.1.4 Users must not in any way cause any form of damage to the IT provision, nor should any equipment be moved or tampered with, without first consulting the IT Helpdesk.

5.1.5 All materials submitted to public areas on Cardiff Metropolitan University systems such as discussion forums, notice boards, web pages or shared file areas, chat rooms, email list or similar shall be legal, decent, honest and truthful. The right is reserved to delete, remove or edit any content that may be in contravention of this policy.

5.2 Access to Cardiff Metropolitan University IT Services

5.2.1 Use of Cardiff Metropolitan University IT services is granted by allocation of a User Name. Users must not use another person's User Name, nor allow any password issued to them to become known to any other person, nor, having logged in, leave IT facilities unattended and potentially usable by some other person.

5.2.2 When an employee resigns or is dismissed or suspended for gross misconduct then access to services will not be permitted. In addition an employee suspended, pending an investigation may also be denied access until that matter has been resolved. In these circumstances all IT and mobile equipment must be returned to relevant line management.

5.2.3 No equipment may be connected to Cardiff Metropolitan University's wired network without the prior agreement of the Head of Information Services (or nominee). Any equipment that is connected must have up-to-date Anti-Virus software and the latest levels of software patching.

5.3 **Unacceptable Use**

5.3.1 Any usage for the purposes listed below or any other use which brings Cardiff Metropolitan University into disrepute are a breach of these regulations. Any misuse such as those described below will be treated as a serious matter and may result in disciplinary action.

a) The Creation, transmission, distribution or posting of any material with the intent to cause harassment, defamation, annoyance, inconvenience or needless anxiety or with the intent to defraud.

b) The deliberate access and/or viewing or attempted viewing or distribution of any material that is obscene, vulgar, indecent or otherwise illegal.

c) The unauthorised transmission of unsolicited commercial or advertising material and in addition the creation or forwarding of chain emails, pyramid schemes or nuisance emails. It is also prohibited to attempt to conceal or falsify the authorship of an email or any other form of electronic communication.

d) In accordance with the Counter-Terrorism and Security Act 2015 access to inappropriate or illegal terrorist related material, is prohibited, unless relevant ethical approval has been granted and confirmed in writing by the Prevent Coordinator.

e) Gaining or attempting to gain unauthorised access, misuse of confidential information, corrupting or destroying data, violating privacy, disrupting the work of others or carrying out activities which deliberately denies, restricts or reduces service. This includes IT systems and resources that are internal to Cardiff Metropolitan University and also external systems on Internet.

f) Any deliberate activities which lead to disruption of communication services, wasting staff effort, IT resources or network bandwidth including time on end systems and the effort of staff involved in the support of those systems.

g) Unauthorised installation or modification of software or computer material, carried out on Cardiff Metropolitan University equipment,

including the deliberate erasure or corruption of programs or data, introduction of viruses and worms, modifying or destroying another user's file or system files, packet-sniffing, etc.

h) Unauthorised and/or illegal copying or use of software or other material that breaches or infringes any license, copyright, trademark or any other personal or proprietary right of any person.

i) The use of Peer-to-peer software (e.g. e-Donkey, Bit Torrent, Gnutella) for file-sharing applications or the transmission of content that breaches a third party's copyright or patent or deliberately discloses their confidential information.

j) In some cases software or services may be licensed or contracted specifically for academic usage. The use of IT services and Cardiff Metropolitan University licensed software for private commercial gain therefore requires specific permission.

k) Any use of social media must be conducted responsibly, appropriately and in accordance with Cardiff Metropolitan University's Social Media Guidance to Staff and/or Students at all times and without risk of Cardiff Metropolitan University being brought into disrepute. For further guidance please read the guidelines on responsible usage at the IT Security page (Social Media Guidance tab).

l) Any form of harassment, bullying, victimisation or defamation of members of staff or students whether through the use of Cardiff Metropolitan University IT services or Internet based forums such as social networking sites, blogs and wikis.

m) Email usage must be used in line with this policy. Further guidance on use of email is available on the E-Mail service page (Email Rules & Regulations tab).

6. Personal data

6.1 Any processing of personal data, whether electronically or as hard copy must be in accordance with the requirements of the Data Protection Act 1998. For further information please see the Data Protection Policy and the Data Protection Procedures and Guidance. Cardiff Metropolitan University has legal obligations with respect to the handling of personal data (information about identifiable living individuals) and any breach of the Act may represent a criminal offence for which Cardiff Metropolitan University and/or individual staff or students would be liable.

6.2 All staff are required to have undertaken the Information Security and Data Protection training (Available on the Staff Development site under ICT Skills). This will ensure they have awareness of the Data Protection Act and of best practices in information security.

6.3 Corporate IT systems have appropriate security controls, so if personal data needs to be processed outside of these systems, where it is at higher risk, it is essential that relevant encryption is used. For guidance on this please see the IT Security page (Securing Data tab).

6.4 Please note that if personal data is to be processed as hard copy, and particularly if it is to be processed outside Cardiff Metropolitan University, appropriate physical measures must be taken to protect the data.

6.5 Personal data should only be disclosed to other individuals, or to external third parties, or published to Cardiff Metropolitan University external websites, in accordance with the Data Protection Act.

6.6 Cardiff Metropolitan University has an Information Compliance Officer who is responsible for how we comply with the Data Protection Act. If you have any concerns about Data Protection, please contact dataprotection@cardiffmet.ac.uk.

7. Mobile and Portable Devices

7.1 Loss or theft of mobile and portable devices (such as Laptops, PDAs, USB Memory Sticks, Magnetic or Optical Media or External Hard Drives) could have serious legal implications. You should ensure that any confidential information is password protected and also refer to the section above if you intend to store personal data on such devices.

7.2 You are responsible for any mobile and portable devices that you use and should ensure that they are kept safe and secure at all times. You should take regular backups of any data that you store on them.

7.3 If you lose a mobile or portable device containing or having access to Cardiff Metropolitan University data then in addition to informing your line management you should contact IT Helpdesk to establish the extent of the loss as soon as possible. If any personal data has been compromised, you should also inform the Data Protection officer immediately by emailing dataprotection@cardiffmet.ac.uk.

8. Transfer of Data to External Companies and Systems

8.1 Should you intend to transfer any personal or confidential data to a 3rd party then you should consider the data protection implications of doing so. If you are transferring personal data, it is likely that a data sharing agreement should be signed between the University and the 3rd party committing them to comply with the Data Protection Act. Please contact the Data Protection Officer at dataprotection@cardiffmet.ac.uk for advice on this matter.

8.2 Following discussions with the Data Protection Officer you may then contact IT Helpdesk for advice on the most appropriate method of transfer. If you have an emergency requirement to transfer data at short notice, then you should alert IT Helpdesk at the same time as you contact the Data Protection Officer.

9. Use of Cloud Services

9.1 Before storing Cardiff Metropolitan University data or documents on cloud or internet based storage systems, such as Dropbox, you should carefully consider any risks associated with this. The general guidance is as follows.

i) DO NOT store any personal or confidential corporate information on non-Cardiff Met external storage systems and services.

ii) DO consider the risks carefully before storing any other data or documents on non-Cardiff Met storage. It is accepted that many work documents would not constitute a risk to persons or corporate sensitivities if lost, stolen or otherwise disclosed. As such staff members are expected to perform an assessment of the risks of storing any given document externally. Please refer to the IT Security page (Guidance on Use of Cloud Based Services tab) for further details.

10. Research involving sensitive material

10.1 Universities play a vital role in carrying out research on issues where security and sensitive material is relevant. Please see the advice on Security Sensitive Research Material in Cardiff Metropolitan University's Prevent Policy or contact the PREVENT Coordinator if you have any requirement to access, circulate or store any material that could be regarded as sensitive or require additional security. Any access to such material without the prior written authorisation of Cardiff Metropolitan University may lead to disciplinary action and where necessary will be passed on to the relevant authorities.

11. Publishing on to Corporate Web Sites

11.1 Any web site or service hosted on Cardiff Metropolitan University servers must conform to the Corporate Style unless otherwise approved by Communications, Marketing & Student Recruitment.

11.2 Content must support Cardiff Metropolitan University's interests rather than those of individuals and where personal material is posted then this should be limited to professional information such as staff profiles, research papers and reports.

11.3 The content management system (CMS) Approvers or relevant Head of Unit or Dean must ensure that published material is legal, does not breach copyright and is appropriate for Cardiff Metropolitan University's external audience**.**

12. Disposal of IT Equipment

12.1 Disposal of IT equipment, communications devices such as mobile phones and portable storage media must be done in line with the Equipment and Data Disposal procedures which are documented on the IT Security page.