|  |
| --- |
| http://www.cardiff.ac.uk/identity/downloads/universitylogo-RGB-300.PNG**Document Control Table** |
| **Document Title:** | **IT Regulations** |
| **Owner:** | IT Services |
| Version Number: | Version 5.1 When approved |
| Document Status: | Approved |
| Date Approved: | 25 June 2019 |
| Approved By: | Data and Information Management Oversight Group |
| Effective Date: | 25 June 2019 |
| Date of Next Review: | June 2021 |
| Superseded Version: | Version 5 |
| **Document History** |
| **Version** | **Date** | **Author** | **Notes on Revisions** |
| Version 1  | Approved Senate 13\_06\_2007  | Corporate Compliance Unit with Information Services | Substantive review and updates. Introduces specified investigation roles and outcomes. |
| Version 2 | Approved Governance Committee 24\_04\_2012 | Governance & Compliance Division with Information Services and Human Resources | Substantive review and updates. |
| Version 3 | Approved COO29\_09\_2013 | Governance & Compliance Division with Information Services and Human Resources | Updates to reflect changes to University structure. Inclusion of explicit right to not reconnect virus infected machines until confirmed clean. |
| Version 4 | Approved COO 09\_03\_2015 | Governance & Compliance Division with Information Services and Human Resources | Updates to reflect changes to University structure and minor edits. |
| Version 5 | Approved DIMOGNovember 2016 | Strategic Planning & Governance | Updates to reflect position regarding powers and:* access to users’ accounts and information, including that held on personally owned IT assets;
* access to, and liability for, personal information held on University-owned IT facilities;
* access to information and devices/facilities in the event of a security incident or other investigation
* Other minor clarifications
 |
| Version 5.1 | June 2019 | Strategic Planning and Governance and University  | Minor updates to reflect legislation change and practice. Inclusion of patching requirements at section 6 |
| Version 5.1.1 | August 2023 | University IT | Minor update to remove invalid reference. |

**UNIVERSITY IT REGULATIONS**

Cardiff University has adopted an Information Security Policy. In accordance with that policy the University has agreed a set of Regulations covering the use of all its IT facilities and services, by staff, workers, honorary title holders, visiting academics, students and any other persons authorised to use them.

**Regulations covering the use of IT Facilities and Services**

**Introduction and Definitions**

These Regulations cover the use of all IT facilities and services administered by Cardiff University.

As well as these Regulations, users must abide by other policies or codes as relevant, including internal Cardiff University codes such as:

* Acceptable Use Policy
* Information Security Policy
* University IT Systems Password Policy
* Student Disciplinary Code
* the relevant staff disciplinary policy
* Safeguarding Children and Vulnerable Adults Policy
* Data Protection Policy
* Records Management Policy
* Dignity at Work and Study policy, and related documents
* Research Integrity and Governance Code of Practice

And external codes such as:

* the Acceptable Use Policy of the Joint Academic Network (JANET) available on the Web at https://community.jisc.ac.uk/library/acceptable-use-policy
* the user obligations under the Combined Higher Education Software Team (CHEST) available at https://www.chest.ac.uk/agreements
* the IT Regulations or similar codes imposed by remote sites, where their IT facilities or services are accessed or used by Cardiff University users

It is not the intention of Cardiff University that these Regulations should be used unreasonably to limit recognised academic freedom[[1]](#footnote-1), as defined in the University’s Statute XV.

**Definitions in these Regulations:**

"**IT facilities and services**" includes:

* Core services as provided by Cardiff University IT Services;
* Cardiff University College, School or Professional Services computers, computing equipment and mobile devices;
* personally owned computers, mobile devices and peripherals when connected to, or accessed from or via Cardiff University-owned IT facilities and services;
* use of remote networks and services, when accessed from or via Cardiff University IT facilities and services;
* all programmable equipment; any associated software and data, including data created by persons other than users, and the networking elements which link IT facilities and services.

"**users**" include staff, workers, honorary title holders, visiting academics***,*** students and any other person authorised to use IT facilities and services;

***“*connected to*”*** means connected either physically or virtually

"**files**" include data and software but do not include manual files.

“**Chief Information Officer” and “Director of Human Resources”** includes any officer with authorisation to act on his/her behalf.

**1. Breaches of Regulations**
Breach of these Regulations is a disciplinary offence and may be dealt with under the appropriate disciplinary policy and its related procedures. Where an offence has occurred under UK law, it may also be reported to the police or other appropriate authority. The manner in which breaches or suspected breaches shall be investigated is outlined in Regulations7 and 8 below.

**2. Private and inappropriate use of IT facilities and services**
IT facilities and services are provided solely for use by staff in accordance with their normal duties of employment, and by students in connection with their University education. All other use is private.

Private use is allowed, as a privilege and not a right, but if abused will be treated as a breach of these Regulations. Private use for academic consultancy or commercial purposes shall also comply with Regulation 10.

Any information or data for private use held on University-owned IT facilities and services is held at the user’s own risk. In addition to the right of access set out in Section 5 and Section 7 and the exclusions on liability referred to in Section 9, the University does not accept any responsibility for the integrity or availability of information or data held for private use and Users will not have any right of access to that information or data in the event that they are no longer able to access University-owned IT facilities and services.

All use, including private use, must comply with the University’s Acceptable Use Policy. Any use which does not breach any other Regulation herein, but nonetheless brings the University into disrepute, may also be treated as a breach of these Regulations.

See also the IT Monitoring Notices and the Process for Access to a User’s IT Account. Both are available here: <http://www.cardiff.ac.uk/public-information/policies-and-procedures/it-regulations>

**3. Compliance with UK civil and criminal law**
Users must comply with the provisions of any current UK law, including but not restricted to:

* the Computer Misuse Act 1990 and Police and Justice Act 2006 amendments (Part 5)
* the Copyright Design and Patents Act 1988 and amendments;
* the Defamation Act 1996;
* the Data Protection Act 2018;
* the Terrorism Act 2006; and
* the Regulation of Investigatory Powers Act 2000.

**4. Software Licence Compliance**

Users shall comply with the terms of any licence agreement between Cardiff University and a third party which governs the use of hardware, software, services or access to data.

Cardiff University may deploy the use of manual or automatic searches in order to ascertain compliance with software licensing as well as terms and conditions relating to software usage. Users connecting University-owned IT equipment in both the physical and virtual environment shall be required to download and install software asset management software as directed by the University.

**5. Integrity of IT facilities and services**

No person shall, unless appropriately authorised, take any action which damages, restricts, or undermines the security*,* performance, usability or accessibility of IT facilities and services; "taking action" may include neglect, where action might reasonably have been expected as part of a user's duties.

All connections of equipment to the IT facilities and services must be conducted in accordance with the University’s Permission to Connect procedure. Where viruses or other potentially harmful malware are discovered, IT Services may disconnect any physical or virtual IT system that is considered to present a risk to the integrity of the IT facilities and services or the security of information within those facilities and services. IT Services may deny permission to reconnect until it can be evidenced that the risk has been mitigated.

Any apparently unauthorised access, removal or modification of IT facilities and services shall be reported as soon as practicable to the IT Service Desk.

Users shall comply with an instruction from the Chief Information Officer which is issued in respect of a suspected, or actual breach of network security, or a reported breach of the University IT Regulations***.***

Cardiff University shall have powers to take all steps which it may deem reasonable to remove or prevent distribution of any material that is threatening the integrity of the network, or to preserve information or the state of the IT facilities and services which may include removal of any IT facilities or services.

**6. Security, confidentiality and passwords**
Users shall take all reasonable care to maintain the security of IT facilities, services and files to which they have been given access. All use and allocation of passwords must be in accordance with the University IT Systems Password Policy. In particular, users shall not transfer passwords, or rights to access or use IT facilities or services, without appropriate authority from the relevant Head of School/ Professional Services Department or nominee or authorised officer.

Users shall ensure that any installed software is appropriately patched and updated. Software (Operating System and Applications) of Internet facing assets must be patched within 14 days of an update being released, where the patch fixes a vulnerability with a severity the product vendor describes as ‘critical’ or ‘high risk’[[2]](#footnote-2).

The access to and use of all personally identifying data originating from Cardiff University systems must comply with the University’s Data Protection Policy and users are under an obligation to maintain the confidentiality, integrity and security of such data. See also Process for Accessing a User’s IT Account <http://www.cardiff.ac.uk/public-information/policies-and-procedures/it-regulations>

**7. Investigation of breaches of University policy or regulations**
The Chief Information Officer may immediately suspend a user's access to IT facilities and services pending an investigation under University procedures by an Authorised Officer or nominee of the University. The Director of Human Resources shall be informed of this action where the user is a member of staff, worker or honorary title holder. The Academic Registrar shall be informed where the user is a student.

Where no disciplinary code applies the Chief Information Officer shall have the authority to suspend a user’s account in support of, or in order to conduct, an investigation. In cases where the user’s account is suspended pending investigation Cardiff University reserves the right to notify the user’s employer (including employment agency) or academic institution of this fact with immediate effect.

Cardiff University shall have powers to access all relevant IT facilities, services and files and to take all steps which it may deem reasonable to remove or prevent distribution of any material which is in breach of any University policy or regulation, or to preserve information or the state of the IT facilities or services for the purposes of an investigation, which may include removal of any IT facilities or services.

As part of investigatory action, Cardiff University reserves the right to require access to any files held on IT facilities or services. It may also require that any encrypted data is made available in human-readable form.

Any such investigatory action shall not prejudice any final determination of whether a breach has occurred.

**8. Investigation of alleged breaches of the IT regulations**

8.1 Illegal Material Relating to Children

These allegations will always be treated as non-minor breaches. All allegations relating to use of the University’s IT facilities and services in connection with the possession of indecent images of children, or other illegal material in connection with children, shall be reported to the Designated Officer under the Safeguarding Children and Vulnerable Adults Policy. [[3]](#footnote-3)

8.2 Minor Breaches (all categories of users)

A preliminary investigation into alleged minor breaches of these regulations shall be conducted by the Chief Information Officer or nominee.

Following that investigation the Chief Information Officer shall have the authority to dismiss the complaint, issue an informal warning or take further action as provided for in section 8.3, 8.4 or 8.5.

8.3 Alleged Breaches by Staff

Where the alleged perpetrator of a suspected or actual non-minor breach is known to be a Cardiff University member of staff, worker or honorary title holder this shall be reported to, as appropriate, the Head of School/College Registrar/Director of Professional Services Department, and Director of Human Resources and considered in accordance with the applicable staff disciplinary procedure.

8.4 Alleged Breaches by Students

Where the alleged perpetrator of a suspected or actual non-minor breach is known to be a Cardiff University student and the matter is more serious (including repeat occurrences of minor breaches) the Chief Information Officer shall refer the matter to the Academic Registrar under the Student Disciplinary Code.

8.5 Other Categories of User

Where the matter is more serious (including repeat occurrences of minor breaches) and no relevant disciplinary procedure applies, the Chief Information Officer shall take appropriate and proportionate action which may include permanent withdrawal of service from the user and/or recommendation that the University take legal action.

8.6 Right of Appeal

The disciplinary procedures for staff and students contain appeal processes for matters dealt with under those procedures.

An individual may appeal against the outcome of an investigation conducted under these regulations by writing to the Chief Operating Officer, setting out the reasons for the appeal.

In cases where the user under investigation is not a member of staff at Cardiff University, nor a student, Cardiff University reserves the right to notify the user’s employer (including an employment agency) or academic institution of the outcome of any investigation at its conclusion.

**9. Liability**
By using the IT facilities and services each user agrees that Cardiff University shall have no liability for:

* loss or corruption of any, file or files or data, contained therein;
* loss or damage (excluding any liability for personal injury or death) to users or to third parties, or their equipment, operating systems or other assets resulting from the use of Cardiff University-owned IT facilities and services or any withdrawal of the use of said facilities and services at any time by Cardiff University.

Each user agrees that Cardiff University has the right to take legal action against individuals who cause it to suffer loss or damage, including damage to its reputation, or be involved in legal proceedings as a result of their breach of these Regulations, and to seek reimbursement of such loss, or any associated costs including the costs of legal proceedings.

**10. Academic Consultancy and Commercial Purposes**

Users may access the University's computers and networks for academic consultancy or commercial purposes only through compliance with the conditions described below and with reference to the Policy for University Services and Private Outside Work[[4]](#footnote-4)

Users applying for external research grants or contracts must abide by University procedures for obtaining funds for any IT element in their work. All external funds intended to pay for IT facilities or services must be declared to the Chief Information Officer and all charges paid promptly.

Software supplied through the University is normally licensed for academic use only; this will exclude consultancy and commercial purposes but will often also exclude internal use for, for example, administrative work. Any user engaged in academic consultancy or other private or commercial work must pay for all computer use and purchase any software licences necessary for this work.

No computer programs developed on the facilities and services provided may be licensed or sold without the prior authorisation of the Chief Information Officer or without reference to the Director of the Research and Innovation Services.

Reasonable precautions will be taken to ensure the reliability of the service, but no guarantee of the correct functioning of program or equipment is given. Where external work involving IT is undertaken this point must be drawn to the attention of the sponsors, unless independent verification of the results of the work has been undertaken.

Any advertising material disseminated via the University's IT facilities and services will be subject to the JANET Acceptable Use and Connections Policies. The University's IT facilities and services must not be used for placing or distributing commercial advertisements relating to any type of business unless expressly permitted by the Chief Information Officer. This may necessitate a separate 'proxy' licence being obtained by the user to distinguish it from the academic and research JANET service provided by IT Services for the University.

1. Education Reform Act 1988 s202 [↑](#footnote-ref-1)
2. \* As defined in the Common Vulnerability Scoring System (CVSS).  ‘critical’ or ‘high risk’ vulnerabilities are those with the following values:
·     attack vector: network only
·     attack complexity: low only
·     privileges required: none only
·     user interaction: none only
·     exploit code maturity: functional or high
·     report confidence: confirmed or high [↑](#footnote-ref-2)
3. https://www.cardiff.ac.uk/public-information/policies-and-procedures/safeguarding [↑](#footnote-ref-3)
4. https://intranet.cardiff.ac.uk/staff/research-support/commercialise-your-research-and-expertise/providing-consultancy-and-services [↑](#footnote-ref-4)