|  |
| --- |
| http://www.cardiff.ac.uk/identity/downloads/universitylogo-RGB-300.PNG**Document Control Table** |
| **Document Title:** | **UNIVERSITY ACCEPTABLE USE POLICY (IT FACILITIES)** |
| **Policy Owner:** | University IT |
| Version Number: | Version 3.1 |
| Document Status: | Approved |
| Date Approved: | 25 June 2019 |
| Approved By: | Data and Information Management Oversight Group |
| Effective Date: | 25 June 2019 |
| Superseded Version: | Version 3 |
| **Document History** |
| **Version** | **Date** | **Author** | **Notes on Revisions** |
| Version 1  | Approved Senate 13\_06\_2007  | Corporate Compliance Unit with Information Services | Substantive review  |
| Version 2 | Approved COO29\_09\_13 | Governance & Compliance Division with input from Information Services, Campus Services, Human Resources and Students Union President | Substantive review to include reference to RESLAN exceptions, inclusion of private use conditions and rationalisation of other clauses. Also replaces 2007 Guidance on Personal Use of Cardiff University IT Systems |
| V 2.1 | March 2013 | R Robertson, GOVRN | Minor update to reflect staff move in Note iv |
| V3 | Approved COO 24 November 2015 | Governance Services | Typographical amendments, enhancements related to, and addition of references to Prevent and Counter Terrorism and Security Act duties |
| V3.1 | 25 June 2019 | University IT | Included password requirements, other general updates |

**UNIVERSITY ACCEPTABLE USE POLICY (IT FACILITIES)**

This policy applies to **all** use of all IT facilities (as defined in the University IT Regulations) administered by Cardiff University.

1. All use must comply with the University IT Regulations and any breaches of this policy shall be investigated in accordance with the investigative provisions of those Regulations. ***See note i***
2. Users are encouraged to use the IT facilities to further the goals and objectives of their work, study or research and in accordance with the University’s Dignity at Work and Study policy. Subject to all of the following, the University permits private use of the IT facilities as a privilege, not a right.

3. Users shall not use the IT facilities inappropriately. ***See note ii***

4. The definition of inappropriate use includes all unlawful activity including use of the IT facilities for possession or retention of unlawful material. ***See notes iii and v***

5. Inappropriate use includes the following activities some of which may be unlawful in the certain circumstances:

5.1 the creation, download, storage, transmission or display of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material; ***see note iv***

5.2 the creation or transmission of material, which is designed, or likely, to be threatening or abusive, defamatory, invades another’s privacy, creates or maintains a hostile environment for others and/or causes other unwarranted damage or distress;

5.3 the creation, download, storage, transmission or display of material that promotes or incites racial or religious hatred, terrorist activities or hate crime; or instructional information about any illegal activities; ***see note v***

5.4 the creation, download, storage or transmission of material with the intent to defraud;

5.5 the creation, download, storage or transmission of material that infringes the copyright or licensing agreement of another person;

5.6 creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, except where it is authorised and relates to the academic or administrative activities of the University or the business of the Students Union, and/or where that material is embedded within or is otherwise part of a service to which the user has chosen to subscribe;

5.7 the representation of any views and opinions held personally by the user as the views of the University, unless the user is explicitly authorised to do so;

5.8 deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics including, but not limited to:

.1 wasting staff effort or IT facility resources

.2 corrupting or destroying other user’s data or violating their privacy

.3 any form of denial of service attack

.4 the introduction of viruses, worms, packet-sniffing or password detecting software

.5 port scanning

.6 vulnerability scanning

.7 attempting to disguise the identity of the sender/origin of an electronic communication

.8 unauthorised access of the network, unsecured or unattended equipment or restricted areas of the network

.9 exploiting equipment compromised by malicious code

.10 unauthorised use of another user’s logon credentials

.11 unauthorised remote access of any equipment by using, for example, Terminal Services, VNC, Telnet or SSH

.12 seeking to access data which is known, or reasonably ought to be known, to be confidential.

6. Hardware may only be connected to the network in accordance with the Permission to Connect procedure.

7. Passwords used to connect to Cardiff University IT Systems should be unique and substantially different to any other passwords used to connect to any other third party services and shall conform to the requirements of the Cardiff University [IT Systems Password Policy](http://sites.cardiff.ac.uk/isf/policies/cardiff-university-it-systems-password-policy/).

8. Users must employ such virus checking processes or procedures that are specified by the Chief Information Officer before files are transferred between computers or are copied over the network. The University provides virus protection software for home, laptop, student and campus systems as described here <https://intranet.cardiff.ac.uk/staff/services/technical-help-and-support/software>.

9. Vendor supplied security updates and critical updates are to be applied as soon as practicable to systems and applications. Fixes to a vulnerability with a severity the product vendor describes as ‘critical’ or ‘high risk’, shall be applied within 14 days of release;[[1]](#footnote-2)

10. Priority for use of University IT facilities shall be given to University business over and above private use and the University may re-proportion network resources including RESLAN (the IT network serving the student residences) as necessary to maintain proper functioning of the University.

11. Abuse of the private use privilege includes use that:

.1 Interferes with the performance of University duties

.2 Interferes with any teaching or assessment event or other University activity

.3 Significantly impedes or adversely affects network performance and/or IT resources

Such abuse may be considered under the relevant disciplinary processes.

12. The use of the IT facilities for private consultancy or commercial activities is governed by the University IT Regulations. In relation to RESLAN (the IT network serving the student residences), users are reminded that the Residences Agreement and associated Residential Terms & Conditions, prohibit the running of any commercial activity, business or trade or profession from the Room or any part of the Premises either online or otherwise.

13. Users should also be aware that there may be legal compliance issues in respect of private use of any of the University IT facilities where issues of registration of copyright, software licensing, and personal data processing rights are involved. Users may be personally liable for breaches of such legislation and should ensure that they are aware of the extent of their personal rights and liability in these fields.

**IMPORTANT NOTES:**

1. Users should be aware that logging of activity is carried out automatically by the University. The information logged includes (this list is non-exhaustive): websites visited, bandwidth usage and applications used. Further information is available in the IT Monitoring Notice.
2. Users should be aware that they are subject to any regulations applicable at a remote site when accessed, or to regulations governing the use of a specific application or service.
3. Many activities described in this policy have the potential to be regarded as a breach of criminal law including (but not limited to): the Protection of Children Act; the Protection from Harassment Act; the Counter Terrorism and Security Act; and the Computer Misuse Act. The University shall maintain a constructive relationship with the Police and other UK National Security bodies, shall co-operate in any Police enquiry, and shall report any matter which appears to constitute a serious criminal offence, or where otherwise the University thinks fit to do so, directly to the Police.
4. Where use of the system for what would otherwise be an inappropriate use is required for University related business (such as lawful research) the user should follow the requirements of the Security Sensitive Research Policy. Advice on the application of certain legislation as it applies to the use of IT can be sought from Assurance Services, Department of Strategic Planning and Governance.
5. Please note that Cardiff University has a statutory duty, under the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

**FURTHER INFORMATION AND GUIDANCE**

* IT Monitoring Notice - <http://www.cardiff.ac.uk/public-information/policies-and-procedures/it-regulations>
* University IT Regulations - http://www.cardiff.ac.uk/public-information/policies-and-procedures/it-regulations
* Dignity at Work and Study Policy - http://www.cardiff.ac.uk/public-information/freedom-of-information/publication-scheme/policies-and-procedures
* Guidance on the University’s duties under the Prevent programme and the Counter Terrorism and Security Act - <https://www.gov.uk/government/publications/prevent-duty-guidance>
* Guidance for Students on Use of University IT Facilities & RESLAN - <https://www.cardiff.ac.uk/new-students/when-you-arrive/it-services-and-digital-community/connecting-to-the-university-it-network>
* Cardiff University IT Service - <http://www.cardiff.ac.uk/study/student-life/learning-support/it-services>
* Security Sensitive Research Policy: <https://intranet.cardiff.ac.uk/staff/research-support/integrity-and-governance/security-sensitive-research>
1. \* 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)