Digital Technology Acceptable Use Policy

Policy Reference IT001 V1.0
Effective Date: 16 October 2019
Last Revised: 16 October 2019
Review Interval: Annual
Review Date: September 2020
Approval Body: Senior Management Team

Policy Owner: Chief Operating Officer and Registrar
Policy Author: Chief Digital Officer

## 1. Introduction

This policy sets out the conditions of use of Swansea University's Digital Technology ("University Digital Technology"). The aim of this policy is to help ensure that University Digital Technology is used freely, but safely, securely, lawfully, equitably and with consideration for others.

All users of University Digital Technology are required to adhere to this policy.

## 2. Purpose

This policy defines the acceptable use of University Digital Technology.

## 3. Scope

This policy, its principles and obligations apply to:

- All users of University Digital Technology
- All University Digital Technology
- All devices making use of University Digital Technology
- Digital Technology administered on behalf of the University
- All electronic communications residing on, or distributed, sent or received using, University Digital Technology
- Internet access provided via University Digital Technology
- Social media operated on behalf of, or referring to, the University
- New University Digital Technology and uses, which may not yet be explicitly identified.

## 4. Exemptions

Where a legitimate academic use of University Digital Technology arises that might otherwise be deemed as unacceptable in this policy:

- Advice must be sought from Legal Services
- Advance approval must be obtained from the relevant College Ethics Committee
- Explicit authorisation must be given by the relevant Head of College
- Sufficient safeguards must be put in place to ensure that the use is contained strictly for the authorised purpose and is managed in such a way as to operate within the law, safeguard individuals, and ensure that University Digital Technology is not compromised
- The Chief Digital Officer should be notified to help minimise the constraints imposed by existing controls on the authorised use

For any other exemptions, advice should be sought from the Chief Digital Officer in the first instance.

**5. No Liability**

University Digital Technology is used entirely at the risk of the user. The University will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of any of University Digital Technology. Although every effort will be made to maintain services, facilities and the integrity of information and software, the University accepts no responsibility for the malfunction of any digital facilities and/or equipment, the loss of any data or software or the breach of any security mechanisms except to the extent that it obliged in law.

**6. Use in Professional Practice**

Use of University Digital Technology in pursuit of professional practice associated explicitly with a staff member or student's role and/or area of study is allowed, provided that there is no conflict of interest and such use is also allowed within the terms of all relevant contracts and licences.

**7. Private Use**

Whilst University Digital Technology is provided for the primary purpose of enabling students to pursue their studies and staff to carry out their work, personal use is permitted provided that:

- Use is proportionate
- It does not interfere with, conflict with or take priority over the performance of University duties
- It does not deny or impair the service to other users
- It does not risk bringing the University into disrepute

**8. Personal Commercial Use**

Using University Digital Technology for commercial work for outside bodies on a personal basis and not as part of University duties or related to relevant professional practice, requires advance and explicit permission from the Chief Operating Officer and Registrar.

**9. Representing the University on Social Media**

Users are required to use social media in line with the University's Social Media Guidelines.

**10. Internet Access via University Digital Technology**

The University has no control over information that can be accessed through the Internet and is not responsible for inadvertent exposure to potentially offensive material accessed by internet users using University Digital Technology.

**11. Acceptable Behaviour**

Users must use University Digital Technology in a way that is considerate of others, so that all users enjoy an atmosphere conducive to work and study. Users must behave in a manner which does not adversely affect or unduly impact upon others, or breach this or other University policies.

**12. Data Protection**

Users must ensure that personal data is handled appropriately and consistently within the provisions of prevailing Data Protection legislation and specific University Data Protection Policy, including cooperating with subject data access requests.

**13. Freedom of Information**

Users acting on behalf of the University shall ensure that University information is handled in a manner consistent with the provisions of prevailing Freedom of Information legislation, including cooperating with Freedom of Information requests.

**14. Responsibility for Security**

Users must ensure that devices making use of University Digital Technology:

- Are protected by a password or employ equivalent security features
- Are logged off or locked when unattended
- Have any encryption, remote location, remote lock, and remote wipe capabilities enabled

**15. User Accounts**

University User Accounts are provided for work and study purposes. They are not private. User accounts created by staff independently for the primary or substantial purpose of conducting University business are deemed to be University User Accounts. Staff are not permitted to use substantially private accounts to conduct University business.

All electronic communications using University User Accounts belong to the University (including their contents and attachments, subject to the University's Intellectual Property Policy (Staff) and Intellectual Property Policy (Students) policies) and are deemed to represent communications sent or received for and on behalf of the University.

Electronic messages may be disclosed in legal proceedings and may recovered even where a user has deleted them.

Users must:

- Take all reasonable precautions to safeguard University credentials (for example, a password, smart card or other security mechanism)
- Not allow anyone else to use their individual University credentials
- Avoid using University passwords for non-University websites, systems or services
- Not share passwords with anyone
- Change passwords if they might have been discovered by someone else

**16. Unauthorised Access**

Users must not use or access another person's account without proper authority. In particular:

- Unauthorised access (or attempted unauthorised access) to University Digital Technology is not permitted
- Allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to University Digital Technology is not permitted
- Users must seek approval from the Chief Digital Officer before adding or connecting new servers and network infrastructure to existing University digital infrastructure

**17. Authority to Access Accounts**

In exceptional circumstances, it might be necessary for the University to gain access to an individual user account. For example, sudden or unexpected absence, to address issues of legal compliance, or to progress a legitimate University need. Such access must be authorised by a member of SMT, Head of College, or Director of Professional Service Unit.

**18. Software Licences and Prevention of Piracy**

Users must ensure that the software they use is properly licensed.

Where a user installs centrally-provided software, the act of downloading indicates acceptance of the licensing conditions pertinent to that software. The user must comply with those conditions.

Similarly, where software has been installed from elsewhere, the act of installation indicates acceptance of the software's licensing conditions. Before installing such software, the user must ensure that the licensing conditions do not conflict with existing University software contracts, policies or interests.

All users must take reasonable care to prevent the illicit copying and use of software and documentation.

Users must not introduce software or other material requiring a license for which a valid licence is not in place.

The University reserves the right to audit devices for asset management purposes and to check that relevant licences are held.

Any unlicensed software or hardware or illicit copies of documentation will be removed.

**19. Monitoring**

The University may monitor the individual use of University Digital Technology where it is required by law or to protect its legitimate interests and those of others, including detection of criminal activity, cybersecurity breaches, asset management, business continuity, resolving problems, unacceptable use, and other legitimate purposes.

The University also reserves the right to inspect and/or remove any items of computer equipment connected to the network.

**20. Responsibility of Managers**

Managers have a specific responsibility to ensure the fair application of this policy.

**21. Consequences of Breaching This Policy**

Suspected breach of this Policy may be investigated under the University's Conduct and Disciplinary Proceedings Ordinance. The University may also take the following actions in response to a breach of this Policy:

- Withdrawal of access to University Digital Technology
- Disconnection and seizure of equipment
- Initiation of relevant conduct and/or disciplinary procedures for staff or students
- Referral to the police or other relevant authority

Where a breach of this policy results in a referral to the police of other relevant authority, the University will co-operate with the investigating authorities and disclose copies of any relevant data stored, appropriate logs and any hardware relevant to the investigation to such authorities in line with current legislation.

The Chief Operating Officer may authorise temporary suspension of a user's access to University Digital Technology where there are reasonable grounds to suspect that the user has breached this policy, pending an investigation.

The University reserves the right to block, disconnect, suspend, or otherwise prevent activities that it considers to be unacceptable use of University Digital Technology. Unacceptable use of University Digital Technology includes, but is not limited to:

- Being threatening, defamatory, indecent, obscene, offensive or harassing others
- Committing or promoting any unlawful act
- Disrespecting the dignity and privacy of others and not considering how their online behaviour may affect others
- Promoting activities likely to draw people into terrorism or extremist ideologies contrary to the University's PREVENT obligations and policy

- The creation or transmission of unlawful communications of any kind, including but not limited to threats of violence, obscenity, indecency, child pornography, or other illegal communications
- Promoting discrimination on the basis of age, sex, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, or sexual orientation, or any other protected characteristic
- Operating commercial ventures not authorised by the University or carrying out unauthorised or illegal personal, legal and business transactions
- Damaging the reputation of the University, its students or staff
- Physical damage to or unauthorised removal of any University Digital Technology
- Infringing copyright, distributing copyrighted materials, using unlicensed software, or accessing licensed products for which users are not authorised
- Denying or disrupting access to University Digital Technology for other users
- Unauthorised use of University Digital Technology
- Deliberately compromising security
- Spamming others
- Permitting and enabling others unauthorised access a University account other than their own
- Disproportionate personal use
- Impersonating or stealing the identity of another person

If users are in any doubt about what constitutes acceptable use, they should seek advice and guidance from their line manager.

**Policy History**

This policy sets out the conditions of use for Swansea University's Digital Technology and supersedes all existing University policy on this subject.

| Revision Date | Author | Description |
|---|---|---|
| 12 August 2019 | Chief Digital Officer | Draft |
| 16 October 2019 | Chief Digital Officer | Approved v1.0 |
| | | |

**Appendix 1**

| Term | Definition |
|---|---|
| University Digital Technology | University Digital Technology encompasses the widest definition of the University's digital, information technology, systems, applications, and infrastructure, including, but not limited to:<br>• Computing hardware, both fixed and portable, including personal computers, workstations, laptops, tablets, PDAs, mobile devices, smart phones, servers, printers, scanners, disc drives, monitors, keyboards and pointing devices<br>• Network infrastructure, including the physical infrastructure whether wired or wireless, network servers, firewalls, switches and routers<br>• Network services, including internet access, web services, broadband, email, wireless, messaging, network storage, telephony and fax services, CCTV, door and access control. This covers network connections in Halls of Residence, on-campus Wi-Fi, connectivity to the internet from University PCs<br>• Software and databases, including applications, web applications, virtual learning environments, video-conferencing, language laboratories, software tools, e-library services, electronic journals and eBooks<br>• Social networking media or services provided by the University<br>• Audio visual and teaching technologies<br>• Online services arranged by the University, such as Office 365, email, or any of the JISC online resources<br>• ICT credentials, such as the use of your University login, or any other token (email address, smartcard, dongle) issued by the University to identify yourself when using ICT facilities and / or equipment<br>• Digital technology bought on behalf of the University or used primarily or substantially for University purposes. |
| Mobile device | • Hand-held and other hand-portable computing equipment which is used for accessing, storing or processing University data, including (but not limited to) laptop PCs, tablets and mobile phones. This also includes audio visual and teaching technologies |
| Portable Storage Devices | • Readily-transportable items used to store data in electronic form (whether temporarily or long-term), including data sticks ("flash drives"), compact discs (CDs and DVDs), plug-in external drives and media players (mp3 players) |
| Social Media | • For the purposes of this policy, social media is defined as any online interactive communication tool, which encourages participation and exchanges. Current examples include Twitter, Snapchat, Facebook, YouTube, Skype, Instagram, Pinterest, Yammer and LinkedIn but the policy also includes the use of external internet message boards and chat rooms. Any social media platform hosted on the University's domain is within scope of this policy. |
| Users | Anyone using, or who has access to, University Digital Technology. In addition to staff and students this may include, but is not limited to:<br>• Visitors to the University's website, and people accessing the University's online services from off campus<br>• External partners, collaborators, contractors, agency workers, casual workers and agents based onsite, using the University's network, or based offsite accessing the University's systems |

| | |
|---|---|
| | • Tenants of the institution using the University's computers, servers or network<br>• Visitors using the University's Wi-Fi<br>• Students undertaking placements or work experience<br>• Users from other organisation using Eduroam or Govroam |
| University credentials | • Means of gaining access to University ICT Services, for example, a username and password, PIN, email address, smart card or other identity mechanism |