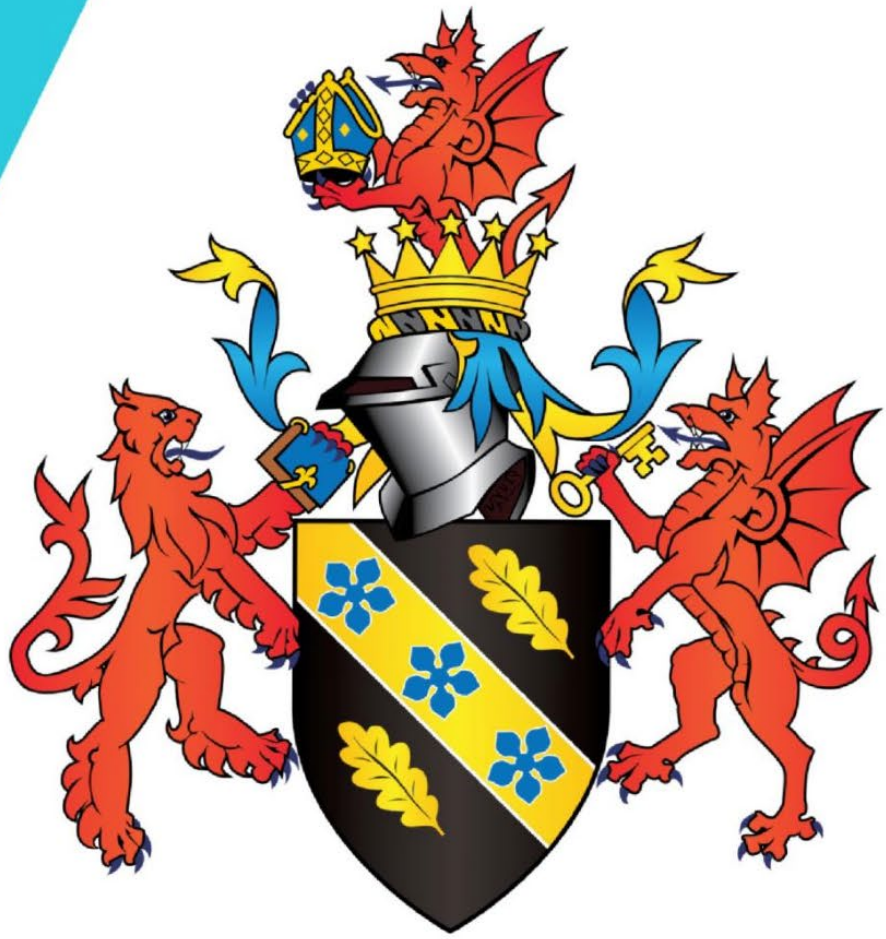
Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David



Information Technology Acceptable Use Policy V2.6

CONTENTS

1. Introduction

Information and Communication Technology permeates all aspects of the day-to-day running of the University of Wales Trinity Saint David. The University (which includes UWTSD and UoW for the purposes of this document) is committed to the appropriate use of information technology and services in support of its mission and the services that it provides. This document sets out the policy on the acceptable use of information technology & systems linked to the University of Wales Trinity Saint David. The University recognises that successful implementation of this Policy relies on having a well-briefed workforce combined with effective management procedures.

Staff and students using the University's Information Technology and Systems **must** ensure that they have read this Policy before using its information and communication technology. Failure to do so will not be accepted as a mitigating factor should a problem arise during employment or period of study.

The University reserves the right to audit and log all use of laptop computers for the purpose of ensuring the integrity, security and reliable operation of computer services. Breaches of this Policy will be treated as a disciplinary matter.

The University has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism under the PREVENT element of the Counter-Terrorism and Security Act (2015) and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material to University Management.

Note: The UK government has defined extremism as: 'vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs.'

This Policy has been subject to discussion and subsequent agreement with the recognised Trades Unions within the University and has been ratified by the Performance and Resources Committee of the University Council.

2. Scope

It is accepted that staff and students within the University will have differing levels of engagement with information technology. This Policy and all the procedures incorporated within the Policy covers:

- Users (academic, professional and support staff, students and others with access privileges) using either personal or University provided equipment connected locally or remotely to the network of the University. Throughout this policy, the word "user" will be used collectively to refer to all employees, individuals or groups.
- All Information Technology & Systems equipment connected (locally or remotely) to University servers.
- Information Technology & Systems owned by and/or administered by the Information Technology & Systems Department of the University.
- All electronic devices that can be connected to the University network, for instance, computers, phones and tablets.
- Connections made to external networks through the University network.
- All external entities that have an executed contractual agreement with the University.

Staff from other organisations operating under a protocol statement within their (respective) contract of employment and staff seconded into the University of Wales Trinity Saint David or University of Wales will be expected to abide by the terms of this Policy. Whilst the University will not have the contractual right to

take disciplinary action against these categories of staff, the Executive Head of IT Service Delivery or their delegated Senior Officer will have the authorisation to suspend access.

3. Purpose

Staff

Within their Contract of Employment all staff have a clause which relates to the appropriate use of the University's assets. This Policy sets out the criteria associated with the acceptable use of the University's Information Technology and recognises that the security of the systems and the management of risk to assets and users is paramount.

This Policy is underpinned by the principle of Dignity at Work and at Study and is designed to ensure fairness and consistency in its application.

Students

Within the "Student Guide to the Regulations" there is a specific paragraph with reference to this Acceptable Use Policy. This Policy sets out the criteria associated with the acceptable use of the University's information technology and systems for students and recognises that the security of the systems and the management of risk to assets and users is paramount.

In addition, the Policy and Procedural documents can be found on Moodle and the University's intranet. Each user is responsible for reading and adhering to the contents of these documents. Failure to observe any part could result in disciplinary and/or legal action being taken by the University against offenders.

3.1 Security

Security is the responsibility of all staff, students and other users of the University's Information Technology. Security can be defined as "the state of being free from unacceptable risk". The 'risk' relates to but is not exclusive to the following areas:

Confidentiality of Information

Confidentiality of information refers to the privacy of personal, student or business information associated with the University.

Integrity of Data

Integrity of data refers to the accuracy of data. Data integrity is of critical importance for informed decision making and for the collation of information and formulation of reports. Therefore, the risk of loss of data integrity, through accidental or malicious alteration, must be managed.

System Availability

System Availability is concerned with the full functioning of IT systems and their components at all times.

Information Technology Assets

Information Technology assets is concerned with physical assets (servers, PCs, Laptops, Smart Devices etc) contained within the unit's control.

Efficient and appropriate use of IT systems

Efficient and appropriate use of IT systems relates to users and their use of the systems available to them.

3.2 Threats

The term "threats" refers to the potential causes of losses to confidentiality, integrity or availability. Threats may be internal, external, human, non-human, natural, accidental or deliberate. The failure to maintain the confidentiality, integrity or availability of information technology and systems may have the potential to negatively impact the University. This Policy aims to set in place mechanisms to manage these threats and thereby to reduce the exposure that the University faces from these threats.

3.3 Reporting Security Incidents

All users of the University's information technology facilities have a responsibility to report immediately (to a member of the IT Service Delivery Team) any incidents which may have security significance to the University. If the incident is considered to be of a highly sensitive or confidential nature, then the report should be made directly to the Executive Head of IT Service Delivery or the Executive Director of Human Resources (copied in both cases to the University's Data Protection Officer)

Any issue relating to pornographic extremist or terror related material should be notified to the Executive Director of Human Resources or the Executive Head of IT Service Delivery immediately and **without delay**. If immediate accessibility to those members of staff proves difficult then you should elicit the support of the Vice-Chancellor's Personal Assistant who will be able to contact an appropriate individual and request that they contact, you. The matter should not be shared or discussed with any member of staff within your Department, Unit or School.

The University's Public Interest Disclosure Policy (Whistleblowing Policy) can be found in the University's Financial Regulations, Volume II, Appendix 19.

4. Roles and Responsibilities

4.1 UWTSD & UoW

The 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 extremism and terrorism.

4.2 Human Resources Department

It will be the responsibility of staff within the Human Resources Department to undertake Part One of the staff induction process. They will ensure that all new members are issued with this Policy and that they will confirm, in writing their acceptance of the terms of the Policy.

N.B. Before being allowed to logon and at each subsequent log in, all users (including students and external guest accounts) agree electronically to the terms of this Policy by logging into any University system.

4.3 Executive Heads of IT Departments

The Executive Head of IT Service Delivery & the Executive Head of IT Systems & Infrastructure will:

- Implement and oversee the effective use of security controls.
- Recommend appropriate measures for the protection of the University's Information Technology assets.
- Regularly (and at least annually) review this Policy and amend it as appropriate and direct it to the Executive Director of Human Resources and to the Associate Pro Vice-Chancellor of Corporate Governance so that changes can be submitted to the various University Committees.
- Regularly (and at least annually) review the internet security briefing content.

4.4 Information Technology Staff

Information Technology staff will: -

- Operate and manage the Information Technology in their custody in accordance with this Policy.
- Periodically reassess Information Technology security measures to ensure their effectiveness and respond to changes where appropriate.
- Ensure students are made aware of this Policy both electronically and during student inductions.

4.5 Individual users

Individual users of the University's Information Technology facilities will: -

- Act in accordance with the University's Information Technology security policies and procedures.
- Immediately report any known or suspected security incidents and breaches to the IT Service Delivery Department or the Executive Head of IT Service Delivery (copied to the University's Data Protection Officer).

5. Use of Internet Facility

Access to the internet is provided to users of the University Information Technology facilities in order to aid them in fulfilling their educational and working commitments.

The University also provides access to internal web enabled services including (but not restricted to) virtual learning environments (VLEs) and document sharing sites such as SharePoint.

This section outlines appropriate and inappropriate use of the University's internet and internal web enabled resources, including (but not restricted to) the use of browsers, electronic mail, instant messaging and file uploads and downloads. Use of these services is subject to the following conditions:

5.1 Appropriate Use

Users within the University are encouraged to use the internet as a tool for educational and working practices, but it must be noted that the University network may only be used for work which complies with the regulations as set out within JANET's Acceptable Use Policy (http://www.ja.net/services/publications/policy/aup.html).

The University recognises that social networking sites can be used as effective collaboration tools and the use of such sites for educational and for that reason professional development purposes is

encouraged. However, it should be noted that these sites may also pose an information security and privacy risk to the University and as such, when using such sites users should take care not to disclose any personal or University information that could result in any form of security breach. Care should be taken to limit the purely 'social' networking on University provided equipment. In particular staff should not engage in the 'social' elements during working hours. More detail is available in the Social Media Policy and Guidelines separate to this document.

The University recognises that users may undertake research activity which occasionally requires access to internet sites that would be considered unacceptable according to this policy. In all cases permission must be sought in writing, from the Ethics Committee, before undertaking the research. If approved the Executive Head of IT Service Delivery will be informed and additional monitoring, recording and reporting back of the users' internet activity will take place.

5.2 Inappropriate Use

Individual internet and internal web enabled resources use must not interfere with others productive use of resources. The list below attempts to provide a framework for activities which fall into the category of unacceptable use (this list is not exhaustive):

- Where the University's internet connection is being used to access another network, any abuse of the Acceptable Use Policy of that network will be regarded as a corresponding unacceptable use of the University's internet resources. Any breach of the Acceptable Use Policies of other networks that is likely to damage the reputation of the University may be regarded as a breach of this Acceptable Use Policy. For example SCONAL Library access. The internet and internal web enabled resources may not be used for the creation or transmission 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.
- The internet and internal web enabled resources may not be used for the creation or transmission of defamatory material.
- The internet and internal web enabled resources may not be used for deliberate unauthorised access to facilities or services accessible via the University's internet connection.
- The internet and internal web enabled resources may not be used for deliberate activities with any of the following characteristics:
- wasting networked resources, including time on end systems accessible via the University and the effort of Information Technology staff involved in the support of those systems;
- corrupting or destroying other users' data;
- violating the privacy of other users;
- disrupting the work of other users;
- using the internet in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- The internet and internal web enabled resources may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
- The internet and internal web enabled resources may not be used in any way that violates the University's policies, rules, or administrative directives. Use of the internet in a manner that is not consistent with the mission of the University or misrepresents the University is prohibited.
- Users should limit their personal use of the internet. The University allows limited personal use for independent learning, and public service. The University prohibits use for mass unsolicited mailings, access for non-employees to the University resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, gaming, competitive commercial activity unless pre- approved by the University, and the dissemination of chain letters.

If you are unsure that your actions will violate the above, you are advised not to continue with that course of action and consult the IT Service Delivery Department.

- Given the University's duty under the Counter-Terrorism and Security Act (2015), the University's internet and internal web enabled resources may not be used to create, access, transmit or download inappropriate extremist or terror related materials as governed by the Home Office under the PREVENT legislation or analogous legislation both in the United Kingdom or overseas
- Users may not establish University computers as participants in any peer-to-peer network such as torrent-based applications, services, or blockchain-based file sharing networks unless approved by the Executive Head of IT Service Delivery.
- Users must obtain approval from the IT Service Delivery Department before using any form of voice communication service over the internet other than University approved services.
- Users may under no circumstances attempt to circumvent or deliberately bypass the Information Technology security measures and controls that are in place.
- No user may use the University facilities to knowingly download or distribute illegal software or material.
- No user may use the University Information Technology facilities to deliberately propagate any virus.

Users should be aware that the University is able to monitor internet and internal web enabled resource traffic and identify individual users and all sites visited.

For security purposes, users may not share account or password information with another person. Accounts are to be used only by the authorised user for authorised purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the IT Service Delivery Department to obtain a password reset if they have reason to believe that any unauthorised person has accessed their account. Users must take all necessary precautions to prevent unauthorised access to their accounts.

6. Use of Electronic Mail

This Policy covers appropriate use of any email sent from the University email address and applies to all students, employees and agents operating on behalf of the University.

6.1 Microsoft 365 Email

The University uses Microsoft 365 mail as their cloud messaging service. All emails are stored off campus on Microsoft 365 servers, held within the UK. Microsoft 365 mail integrates seamlessly with other Microsoft 365 applications such as OneDrive for Business and Teams to provide improved user experience.

6.2 Electronic Mail Usage

All users are required to observe the following requirements when using electronic mail:

The University email system shall not be used for the creation or distribution of any disruptive, offensive or threatening messages, including (but not restricted to) offensive comments about any of the protected characteristics of the Equality Act 2010: -

- Disability
- Race
- Gender
- Age

- Gender reassignment
- Sexual orientation
- Religious beliefs and practice, political beliefs, or national origin
- Marriage & Civil partnership
- Pregnancy & Maternity

Given the University's duty under the Counter-Terrorism and Security Act (2015), the University email system must not be used to create, access, transmit or download inappropriate extremist or terror related materials as governed by the Home Office under the PREVENT legislation and or analogous legislation existing in the United Kingdom or overseas.

The Principle of Dignity at Work and Study and the characteristics relative to equality and diversity in the workplace should be observed at all times.

Users who receive any emails of this nature should report the matter immediately to the Executive Director of Human Resources or the Executive Head of IT Service Delivery.

Users may not accept or send any live examination data or examination paper material by email, unless authorised to do so by the Head of Quality Assurance Unit. If authorisation is given, data must be encrypted. Advice on how to encrypt data will be given by the IT Service Delivery Department if required.

Users are subject at all times to the University's Data Protection Policy. Users may not run any program received as an attachment to an email. Program files usually have the suffix .exe, but if unsure contact the IT Service Delivery Department before opening the file.

Users may only open application file attachments (such as word processed documents) received as an attachment to an electronic mail message if the message is expected and does not appear suspicious in any way. In the event of any concern whatsoever about an attachment the matter must be referred to the University's IT Service Delivery Department and must not be opened.

In the interest of maintaining network performance, the University's email system is configured to reject very large messages (over 50 Mb in size).

Please be aware that the University reserves the right to monitor and audit all incoming and outgoing emails without prior notice and as such users should have no expectation of privacy in anything they store, send, or receive on the University's email system.

Electronic Mail Retention

- This Policy is secondary to the University's Freedom of Information Policy and Records and Retention Schedule. Any email correspondence containing business information should therefore be retained in line with these policies.
- The primary intent of email backup is for the full recovery of the email system and not for the storage and restoration of old emails. The Information Technology Departments backup the email system solely for the purpose of restoring the service when it suffers a catastrophic system failure and the whole system has to be restored.
- Email correspondence containing business information should only be retained by the user for as long it is necessary for business purposes, in line with the University's Record and Retention Schedule.

6.3 Email Recovery

- Users should be aware that the Information Technology Departments do not recover individual deleted emails on request; other than following a RIPA request (Regulation of Investigatory Powers Act 2000) from the Police or in cases pending investigations. Requests for the recovery of such emails must be approved and authorised by the Vice-Chancellor or his nominee.
- Unless a user specifically requests a permanent deletion of an email then any mail items will be retained in the Deleted Items folder as per the deleted items retention policy period. As such, deleted emails can easily be recovered if they reside in the Deleted Items folder. If mail items are purged from Deleted Items or deleted by pressing 'shift+delete' they may still be retrievable for up to 90 days using the Recover Deleted Items feature. After that period, they will be permanently lost.

6.4 Quotas and Limits

- All users have access to the cloud-managed email service. All accounts have quota limits of 50GB per mailbox storage placed on them.
- Users receive an email notification when approaching their quota limit (49 GB) and are encouraged to follow the guidance in this to manage their account.
- Users will be prohibited from sending emails once their mailbox quote reaches 49.5 GB.
- Users will be prohibited from sending and receiving emails once their mailbox quote reaches or exceeds 50 GB.
- There are limits on the size of an email that can be received and transmitted. No Email greater than 50 Mbytes can be accepted for inward delivery to a University account. No email greater than 50 Mbytes can be accepted for external delivery by the email servers. The sender of oversized emails will be informed of the reason for delivery failure.

7. Anti–Virus & Anti-Malware Mechanisms

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable internet files, diskettes, CDs and removable storage devices. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user.

A virus infection can be very costly to the University in terms of lost data, lost productivity, and/or lost reputation. As a result, one of the goals of the University is to provide a computing network that is virus-free.

This section of the Policy provides instructions on measures that must be taken by the University to help achieve effective virus detection and prevention and applies to all computers that are connected to the University network via a standard network connection, wireless connection, modem connection, or virtual private network connection. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

7.1 Security Updates

Any device that connects to the University's network, regardless of operating system should be protected both from malicious code and hacking attacks which exploit software vulnerabilities, through the deployment and installation of operating system security

patches. All currently available security patches must be applied on a schedule appropriate to the severity of the risk they mitigate.

7.2 Responsibilities of the Information Technology Departments

The following activities are the responsibility of the University's Information Technology Departments:

- To keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.
- To apply any updates to the services it provides that are required to defend against threats from viruses.
- To install anti-virus software on all the University owned and installed desktop workstations, laptops, and servers.
- To take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, a suspect computer may need to be disconnected from the network or from an entire segment of the network.
- To notify users of the University systems of any credible virus threats via e-mail or telephone messages.
- To carry out regular scheduled virus-scanning of network data.
- To remove any virus-infected computer from the network until it is verified as virus-free.

7.3 Users' Responsibilities

- Users will not knowingly introduce a computer virus into the University's computing environment. Any activities undertaken by a User with the intention to create and/or distribute malicious programs (e.g. viruses, worms, Trojan horses etc) onto the University network are strictly prohibited and will result in disciplinary action by the University
- Users who use devices such as USB flash drives or similar devices are responsible for regularly scanning their approved media devices for viruses. If any infected files are identified as a result of these scans, the University's IT Service Delivery Department must be informed immediately.
- Any user who suspects that their workstation has been infected by any form of malicious software must inform a member of the IT Service Delivery Department immediately.
- Users who believe that their PC/Laptop/Mac may, due to a virus or malicious software, contain any inappropriate material (such as pornographic pictures or videos) should report the matter immediately to the Executive Director of Human resources or the Executive Head of IT Service Delivery. In circumstances where a user removes or quarantines an infected file, the IT Service Delivery Department must be informed immediately.
- Users must not attempt to either alter or disable anti-virus software installed on any computer attached to the University network.

8. Access and Passwords

All individuals who require access to system and information resources are properly identified by means of a unique personal identifier and password in addition to Multi-Factor Authentication (MFA). In order to protect the confidentiality and integrity of the University's information, access levels are restricted to those capabilities that are appropriate to each users' role. Only users authorised to access such resources are issued with these details (by the IT Service Delivery Department).

In the event of staff absence through sickness or leave, access to system and information resources can be granted to the individual's line manager, if required. A request for access must be made to Human

Resources in the first instance who will log a Service Desk ticket for access to be provided temporarily and will require Deputy Vice Chancellor approval.

All users must note: -

- UWTSD users will be required to change their password a minimum of every 410 days.
- Passwords must be of a minimum of 8 characters long and contain at least one capital letter and one numeric character.
- Shall be responsible for all computer transactions that are made with their user ID and password.
- Must not disclose passwords to others. For multi-user mailboxes, users must not disclose the password to any unauthorised personnel.
- Must change their password immediately if it is suspected that it has become known to another individual.
- Should always attempt to use passwords that will not be easily guessed by others. As guidance, it is recommended that when choosing a password, users should always **avoid**:-
    - Words found in the dictionary
    - Proper nouns
    - Regular words with numbers added to the end
    - Conventional words that are simply written backwards, such as ('nimda').
    - Instead try to pick acronyms, mnemonics, random letters, etc, or insert non- alphabetic characters in the middle of the word or replace letters with numbers ('0' to zero, I to 1, E to 3)
    - Sharing access of accounts with other individuals.
    - Using the same password on multiple accounts.

9. Physical Security

In order to protect computer hardware, software, data and documentation from misuse, theft, unauthorised access and environmental hazards, the Information Technology Departments will ensure that:

- Critical computer equipment (file servers) will be protected by an uninterruptible power supply.
- Critical computer equipment will reside within a secure, climate-controlled room. Only authorised personnel will have access to this room.

The following directives should also be followed by all users: -

- Disks and other portable storage devices should be stored securely when not in use. If they contain sensitive, personal or confidential data, they should be encrypted to AES-256 standard or equivalent and locked up when not in use. Such material must not be transferred by non-secure methods (for example, by regular mail).
- Disks, USB drives and other portable storage devices should be kept away from environmental hazards such as heat, direct sunlight and magnetic fields.
- Disks, USB drives and other portable storage devices (including mobile phones. Tablets and laptops) when taken offsite must be secured at all times. Such devices must be encrypted, or confidential documents contained within must be encrypted before being taken offsite. For advice on securing and encrypting these devices please contact the IT Service Delivery Department.
- The Information Technology Departments are responsible for all information technology equipment installations, relocations & modifications - users are not permitted to perform these activities.
- With the exception of laptops specifically allocated to a user, other users are not permitted to take Information Technology equipment off campus without formal permission from their line manager who will be responsible for keeping an audit of any equipment taken off campus.

Those who use equipment (including laptops, portable data projectors and conference phones) in meeting rooms are responsible for ensuring that the equipment is not left unsupervised at any time unless the room has been locked and is secure. Users of Information Technology equipment in these locations are not permitted to remove or disconnect any Information Technology equipment including peripherals.

10. Computer Usage

Users will be provided with Information Technology facilities to help them carry out the tasks required of them. Users should adhere to the following directives when utilising these facilities:-

- It is important that the Information Technology Departments are aware of all software that is installed on University owned computing devices. As such, the majority of users will not be able to install software on any University owned equipment. Users may request, via the Service Desk, installation of certain software or utilise the company portals to install software. The Information Technology Departments reserve the right to refuse installations of any software.
- Certain users may be granted permission via the Executive Head of IT Service Delivery or their nominee to install software themselves. This will be monitored by the Information Technology Departments.
- No equipment may be connected to the University network or a University computer without authorisation from a member of the Information Technology Departments.
- The University recognises that removable media devices (such as USB sticks, CD/DVD media) can greatly benefit our users who are often mobile. However, such devices are a well-known source of malware infections, and can result in the loss of sensitive University or personal information. As such, users should take care not to store sensitive or confidential University or personal information on such drives and operate the said devices with reference to the University's Data Protection Policy

10.1 Backup Procedure

The Information Technology Departments guarantees that all sensitive, valuable or critical information that resides on our file servers will be backed up on a nightly basis. A number of backups of all data will be stored off-site in order to protect against major damage occurring at the primary location (in accordance with the University's Business Continuity Policy).

In order to prevent the loss of any data, users are responsible for: -

- Ensuring that their work is saved to your University OneDrive, Teams or SharePoint sites. Alternatively, data can also be saved on a University network server in order to ensure that it will be backed up.
- Making their own arrangements to backup important work when using any non- networked computer or saving data (such as archiving emails) locally on their PC/Laptop.
- Ensuring that data kept on CD/DVD's/USB drives or other portable devices is backed up appropriately to limit effects of loss/damage to these devices.

10.2 Remote Access Procedure

The following directives only apply to those users who use remote access via Secure Virtual Private Network connections (SSL VPN), set up by the Information Technology Departments, to carry out work for the University.

Users with remote access privileges are responsible for ensuring that their remote access connection is given the same consideration as the users on site connection to the University network.

Remote connections to the University network are subject to the same rules and regulations, policies and practices outlined in this document and its supporting policies.

At no time should any users provide their remote-access login details to anyone else.

10.3 Laptop and Mobile Computing

Mobile computing devices such as laptops have become useful tools to meet the business and educational needs at the University. Such devices are particularly susceptible to loss, theft and hacking as they are easily portable and can be used anywhere outside of the University's network.

The purpose of this Policy is to establish the rules for the use of mobile computing devices (either staff or student loan laptops) that contain or access information resources at the University. These rules and guidelines are necessary to preserve the confidentiality, integrity and availability of the University information.

Encryption
Laptops and other portable devices should be kept physically secure, as well as being protected from unauthorised access. This is not only gaining access by a username and password, but by utilising an encryption service in the event the device is lost or stolen. Any USB storage devices being used for sensitive data must also be encrypted.

The IT Service Delivery Department will ensure that all university-owned portable devices and USB devices used for sensitive data are encrypted. You should contact the IT Service Delivery Department for further advice. All University owned Laptops and mobile devices will be enrolled with the University's Mobile Device Management systems for security purposes.

Any sensitive documents/data shared with third parties outside of UWTSD & UoW should always be encrypted. All UWTSD and the majority of UoW staff machines have 7-Zip installed for this purpose. Any UoW members of staff who require 7-ZIP installed should contact the IT Service Desk.

Data Storage and Backup Procedure
We strongly advise that you keep to a minimum the amount of confidential, personal, or sensitive University information stored on the laptop's hard drive (ensuring compliance with the University's Data Protection Policy and encryption protocols elsewhere in this document)

Users are responsible for ensuring that data stored on laptops or handheld devices is regularly backed up. IT Service Delivery staff can advise on the appropriate processes required to achieve this.

Software Installations
Users must not install software or change the configuration of the operating system without approval from the IT Service Delivery Department.

Personal Use
Users may not use a University laptop computer or handheld device for personal use (any purpose not specifically related to the University work) without the approval of their line manager.

Users should only use their laptop or handheld device to access systems and services for which they have been authorised.

Usage by a Third party
Users are responsible for ensuring that any use of a University computer by a third party is consistent with this Policy.

Use on Untrusted Networks
Users should only use untrusted networks such as a home broadband connection, hotel networks, or wireless access points provided they do not disable or remove the firewall and anti-virus software.

Users should report any suspicious activity whilst using such untrusted networks to the IT Service Delivery Department immediately.

When using untrusted networks users should ensure that they do not attempt to exchange any data considered to be confidential such as University financial, personnel or commercially sensitive data. For example, the exchange of information via home email messages or as attachments is particularly insecure. SSL VPN for remote access is considered to be a ***trusted*** network.

Theft, Loss, or Compromise
When left unattended, the University supplied portable computing devices must be physically secure and the device should be shut down or locked to prevent access. This means they should be locked in an office, room or locked in a desk drawer/filing cabinet when not in use.

If a user becomes aware of a theft, loss or compromise of any University laptop or handheld device, they must:
- Inform the local police immediately;
- Contact the University Insurance Officer in the Finance Department to report the loss to them;
- Contact the Service Desk Team to report the loss to them.

Auditing
The University reserves the right to audit and log all use of laptop computers for the purpose of ensuring the integrity, security and reliable operation of computer services. Breaches of this Policy will be treated as a disciplinary matter.

10.5 Microsoft OneDrive for Business

The University utilises OneDrive for Business and all users will be given access to this service. This is a convenient cloud-based storage service provided by Microsoft that allows a user to share files with colleagues and access them on multiple devices. OneDrive for Business as well as placing a copy of data on to the Microsoft cloud, will also sync the same data on to a user's device(s).

A user should consider the type of data that they intend to copy in terms of it being confidential and should also check with the data owner, institute, or department prior to copying confidential data to OneDrive for Business. If a user is unsure, they should request advice from the IT Service Delivery Department.

Files that are deleted in OneDrive are sent to the site Recycle Bin (also called the first-stage Recycle Bin) where you can restore them if you need to. Any files deleted from the recycle bin will be sent to the site collection Recycle Bin (also known as the second-stage Recycle Bin). OneDrive and

SharePoint files are retained for 93 days from the time you delete them from their original location. The files will remain in the site Recycle Bin for the entire duration unless they're deleted or the Recycle Bin is emptied. In that case, the items will go to the site collection Recycle Bin where they stay for the remainder of the 93 days. Once files are sent to the site collection Recycle Bin, only a SharePoint site collection administrator can restore the files. Once files have exceeded the retention time of 93 days they are permanently deleted. If a user requires assistance in recovering deleted files, they should contact the IT Service Delivery department for advice.

It's important that a user understands the process of sharing of files;

- Never share files or folders with everyone or the public but only with specific individuals
- Be careful when sharing links via email, make sure it is only sent to the intended recipient listed, to avoid sending sensitive data to the wrong person.

11. Data Protection

11.1 Monitoring of IT/Network Systems

The Regulation of Investigatory Powers Act 2000 does not allow the interception of communications by an employer unless the employer has "lawful authority".

11.2 Lawful authority by means of the RIPA

The RIPA allows universities to carry out the following interceptions without the consent of the sender or the receiver of the communication:

- the interception by or on behalf of the person running a service, for the purposes connected with the provision of the service – such as readdressing wrongly addressed email, or checking subject lines in email for viruses.
- The monitoring of system traffic to ensure effective performance – a possible example might be finding out the source to cut down spam.

11.3 Lawful authority by means of the Lawful Business Regulations

The Lawful Business Regulations at Section 3 provide the main source of lawful authority for interception of communications and permits the monitoring or keeping of a record of communications for certain purposes. These Regulations expand on the permitted interceptions provided for by the RIPA and were the result of a Department of Trade and Industry public consultation exercise following the concerns raised by many organisations as to the restrictive nature of the RIPA.

The purpose of the Lawful Business Regulations is to allow exceptions to the basic principle of non-interception as stated in the RIPA, and to allow interception without consent in certain instances.

Interception is permitted to:

- Establish the existence of facts. This is thought to mean to establish the existence of facts relating to ascertaining compliance with regulatory or self-regulatory practices or procedures.
- Ascertain compliance with regulatory or self-regulatory practices or procedures. A possible example might be HESA reporting.
- Ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system.
- Investigate or detect unauthorised use of the communications system.
- Prevent or detect crime, or in the interests of national security.

- Ensure the effective operation of the system.

Monitoring but not recording is also permissible in the following cases:

- To ascertain whether the communication is business or personal.
- To protect or support helpline staff.

There are also additional conditions:

- The interception must be made solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the system controller's business i.e. relevant to the business of the University;
- Every effort must be made to inform users that monitoring and recording may take place.

Consequently, the University reserves the right to monitor telephone use, internet use, email and other material on its computer systems from time to time, for the purposes indicated below:

- Compliance with University regulations and policies.
- Preventing or detecting crime.
- Investigating or detecting unauthorized use.
- Checking for viruses or other threats to the performance of the system.
- Investigating abnormal system behaviour.
- Resolving a user problem.
- Monitoring standards of service or training.
- Maintaining or carrying out University business.

Such monitoring will be kept to a reasonable minimum as stipulated in the legislation. Every care will be taken to comply with all applicable data protection and privacy legislation in respect of the confidentiality of any material that is monitored, in so far as this does not conflict with duties laid down in other legislation.

Any investigation, other than day-to-day monitoring, should be referred to the Executive Head of IT Service Delivery who will require the written authority of the Executive Director of Human Resources or nominee, in order to take place. The person who grants the authority should be satisfied there are reasonable grounds for this request.

12. Procedure for dealing with Staff Leavers

When staff leave the University there may be important data in their mailbox, home folders on the network, or stored on their PC. On departure access to email accounts and file stores is given to the line manager with the approval of a Deputy Vice-Chancellor. Information Technology equipment must also be returned to the IT Service Delivery Department.

12.1 Departing Staff Responsibility

- Prior to leaving employment all email contacts should be made aware that the email account should no longer be used, and that future e-mails may be automatically sent to another University employee.
- If required, email folders can be archived by submitting a request to the IT Service Delivery Department for permanent storage.
- Files of a personal nature should be removed, along with personal e-mails, as these will be examined after their departure to ensure no critical business information is lost.

- Laptops, Mobile phone, Tablets or any other equipment allocated to them should be returned to the IT Service Delivery Department or HR Department on or before the last day on-site before departure.

12.2 Line Manager Responsibility

- To undertake relevant leavers process and to meet with staff and obtaining relevant confirmation that all University IT equipment has/will be returned
- To inform the IT Service Delivery Department to access file store data if required.
- To inform the IT Service Delivery Department if emails of the departing employee should be forwarded to an alternative email address and the period for which this is required.

12.3 Information Technology Responsibility

- To delete data file stores and email accounts prior to one month at the request of the line manager or alternatively one month after they leave if no communication is received from their line manager.
- To remove e-mail forwarding after three months if relevant.

12.4 Human Resources Unit Responsibility

- To ensure that the correct end dates are inputted onto the HR System
- To create and maintain the relevant leavers process and ensure IT equipment return is included as part of the process

13. Halls of Residence Network

The Halls of Residence Network service, run by the IT Departments, provides wireless connections in all University accommodation blocks. Ethernet connections are also available in all Lampeter and Carmarthen halls of residence. The connections provide restricted access to services on the internet at large.

Personal equipment connected to the halls network must comply with certain standards which are available from the Service Desk on request. If you are unsure or fail to connect to the network, you should contact the Service Desk Team.

The following protocols are for University Network Administrators only. The majority of users will not have the technical knowledge to use them. For those who do have the capability, users must not run any of the following, to ensure security, bandwidth and traffic management, legal requirements or to protect the University and its reputation:

- DHCP servers
- DNS Servers
- Routing Protocols (such as OSPF, RIP etc)
- Network Discovery Protocols
- Internet Connection Sharing
- Port Scanners

Neither are they permitted to:

- Attempt DDNS (Dynamic DNS) updates.
- Set up network file shares that are writable without a password.
- Re-distribute access to others, nor any University resource made available.
- Configure any device attached with any IP (internet) address not specifically allocated to them.
- Connect any form of wireless access point, nor configure any computer with wireless capability such that the service can be accessed wirelessly.

- Download or distribute copyright material in breach of any license conditions.

- Run peer-to-peer network such as torrent-based applications, services, or blockchain-based file sharing networks unless approved by the Executive Head of IT Service Delivery..
- This list is not exhaustive and can be added to at any time.

Any personal computer connected to the service must have up to date anti-virus software installed. Virus risk management is an important priority and any personal computer not adequately protected under this provision will have its access disabled - until it is quarantined, inoculated and made safe.

14. Disclaimer

To the full extent allowed by applicable law, the University will not be liable to any user or any third party for any consequential or incidental damages (including but not limited to loss of revenue, loss of profits, loss of anticipated savings, wasted expenditure, loss of privacy and loss of data) or any other indirect, special or punitive damages whatsoever that arise out of or are related to use of the University network, or any of its information technology, systems or materials.

We encourage you to use your internet access responsibly. Should you have any questions regarding this Policy, feel free to contact the IT Service Delivery Department on ITServiceDesk@uwtsd.ac.uk (0300 500 5055 or internally on 5055).

15. Monitoring

Details of how the University will monitor the application of this Policy are detailed in previous sub sections.

16. Breach or Violation of the Information Technology Policy

The University recognises its responsibility for its students, staff and technological assets. Users who breach the terms of this Policy will be dealt with under the University's Disciplinary Policy. This could include temporary or indefinite withdrawal of access to the University's Information Technology. Where criminality is detected, the University will take relevant and appropriate action.

17. Links to other policies / procedures / relevant legislation:

This Policy is underpinned by the University of Wales Trinity Saint David Dignity at Work Statement.

Other relevant University Policy include:

- Bring Your Own Device (BYOD) Policy
- Strategic Equality Plan
- Disciplinary Policy
- Whistleblowing Policy
- Anti-Harassment and Anti-Bullying Policy
- Grievance Policy
- Records and Retention Schedule
- Data Protection Policy

(Please note that these policies are available on the UWTSD HR MyDay site, some of which are currently being drafted and/or updated – Please note that UoW staff currently do not have access to this site and so can request copies of relevant policies if required).

Relevant legislation to this Policy includes (but is not limited to):

- Computer Misuse Act (1990)
- Electronic Communications Act (2000)
- Obscene Publications Act (1964)
- The Safeguarding Vulnerable Groups Act (2006)
- The Safeguarding Vulnerable Groups Act 2006 (Controlled Activity) (Wales) Regulations (2010)
- Copyright (Computer Software) Amendment Act (1985)
- Malicious Communications Act (1988)
- Human Rights Act (1998)
- Data Protection Act, (2018)
- General Data Protection Regulation (2016) ("GDPR")
- Freedom of Information Act (2000)
- Equality Act (2010)
- Terrorism Act (2006)
- Copyright Designs and Patents Act (1998)
- Privacy and Electronic Communications Regulations (2003)
- Regulation of Investigatory Powers Act (2000)
- Data Retention and Investigatory Powers Act (2014)
- Lawful Business Practice Regulations (2000)
- Communications Act (2003)
- Defamation (Operators of Websites) Regulations (2013);
- Counter-Terrorism and Security Act (2015) - PREVENT

European legislation also needs to be complied with. In this context, that is primarily embodied in the Electronic Commerce (EC Directive) Regulations 2002 and GDPR: and includes but is not limited to;

- Liability for Publishing;
- Liability for Actions or Negligence

18. Resource Implications

Implication	Detail
Finance	This policy does not place an additional financial implication on the University. Proper application of this Policy should negate the requirement for unnecessary expansion of University archiving facilities.
Staff	The application of the Policy can be absorbed by current staffing.
Assets	It is not envisaged that implementation of this Policy will require any additional assets than has already been budgeted for within the general Information Technology and Systems departmental budget.

Partners	This Policy has implications for those accessing the University's Network. Therefore it is important that suppliers / contractors / partners accessing the network and its systems are made aware of this Policy. The Policy also outlines implications for utilising the JANET website and users are instructed to make themselves aware of their Acceptable Use Policy.
Timescales	There is no lead time envisaged in implementing this Policy. Once approved this Policy can be implemented immediately.
Leadership	The Executive Director of Human Resources, the Executive Head of IT Service Delivery and the Executive Head of Corporate Services have leadership responsibility for this Policy.

19. Impact Assessment

Implication	Impact Considered (Yes/No)	Impact Identified
Legal including a data protection audit	Yes	These are detailed in sections 17 and 18 above. This policy has been scrutinised and amended by the University's Data Protection Officer.
Contribution to the Strategic Plan	Yes	This Policy contributes to the University's defining characteristics set out in the Strategic Plan.
Risk Analysis	Yes	This Policy outlines how risks associated with utilising technology and systems are managed by implementing controls and monitoring the implementation of this Policy.
Equality	Yes	The provision of training and communication associated with this Policy will take into consideration those with specific access needs.
Welsh Language	Yes	Once approved the Policy will be made available bilingually.
Environmental and Sustainability	Yes	This Policy impacts positively on the sustainability agenda. Successful implementation of the Policy allows users to store, access and communicate electronically as an alternative to less sustainable means.

Communication/Media/ Marketing	Yes	Once approved the Policy will be communicated to staff through various means including staff induction, and staff bulletins. Access to it will be made available via the University website and Moodle. Communication to students will be undertaken as part of the student induction process. All users logging onto University equipment are asked to agree to the terms of this Policy before permission is given to allow them to proceed.

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

20. Document Version Control

Version No:	Reason for change:	Author:	Date of change:
	Original Policy Document		2014
	Submission to Senior Management		13 January 2015
	To JCC		4 February 2015
	Comments offered by Corporate Services	Claire Godden	12 Feb 2015
	Comments offered by JCC		
	To JCC		8 May 2015
v2.0	Comments offered by Chair of Resources Committee (Council)	Claire Godden	10 Sept 2015
	Date of Implementation		10 Sept 2015
v2.1	Addition of references to Counter-Terrorism and Security Act (2015) - PREVENT		2 May 2017
v2.2	GDPR and general formatting updates	James Cale/Paul Osbourne	10 October 2018
v2.3	Additional items around security added and changes to accommodate UoW	Ben Thorn	15 Feb 2019
v2.4	Updated post restructuring to reflect changes to roles and committee names	Ben Thorn	29 July 2019
v2.5	Updated roles and to incorporate Microsoft Teams usage.	Ben Thorn	16 July 2021
v2.6	Updated to incorporate MFA and password age duration change.	Ben Thorn	21 Oct 2022

Policy author(s): James Cale – Executive Head of Information Technology & Systems

Current status of Policy: Final

Is the Policy applicable to: HE

Date ratified: 06.06.17 Date effective from: 06.06.17 Policy review date: 06.06.23