IT Acceptable Use Statement

Version – v6 –March 2025

Procedure Author – IT Security and Customer Support Manager

Procedure Owner – Vice Principal (Finance and Infrastructure)

Parent Policy Statement – Information Services Policy Statement

Public Access or Staff Only Access – Public

Version – v6 –March 2025

Changes and Reason for Changes – Additional content added under Device Tracking.

IT ACCEPTABLE USE STATEMENT

INTRODUCTION

Information Technology plays a vital role in helping deliver efficient services and contributing towards the student experience. Staff will recognise the importance of maintaining good practice for IT to be effective. The purpose of this Statement is to support all users of University systems in understanding good practice, avoiding misuse of University facilities and behaving lawfully.

Everyone using UWS IT equipment or systems is responsible for the security of data on them. As such, all users must adhere to the requirements of this statement at all times. Should anyone be unclear on the statement or how it impacts them, they should contact the Information Services Helpdesk.

This Statement should be read in conjunction with the following UWS procedures and other documents that also apply to this context:

a) Data Protection Code of Practice
b) Dignity and Respect at Work Guidelines
c) Disciplinary Procedure
d) Equality, Diversity & Human Rights Code
e) IT Information Security Procedure
f) IT Software Licensing & Control Statement
g) IT Password Management Procedure
h) Records Management Protocol
i) Guidelines for the use of Social Media at UWS
j) University Regulation – Code of Discipline for Students
k) Guidance on use of USB devices
l) Acceptable Use Statement MS Teams
m) Guidance document for Staff - MS Teams
n) IT Hardware Asset Management Statement
o) UWS Bring Your Own Device Statement

The impact of this Statement will be monitored regularly to reflect the changing online environment and technologies. The Statement may also be amended where particular concerns are raised or where an incident has been recorded.

This Statement supersedes any written or oral policy previously issued concerning IT acceptable use in the University.

1. SCOPE OF STATEMENT

This Statement applies to all individuals issued with a UWS user ID and password (hereafter referred to as ‘user’).

This Statement covers the use of all UWS IT systems, equipment and networks whether accessed on or off campus. It applies to access gained through the wired or the wireless network or via a VPN connection. The statement also applies to personal equipment being used to conduct University business or connect to the University network for the purpose of accessing UWS applications or data.

2. OUR STATEMENT

Use of any UWS IT systems, equipment and network on or off campus implies acceptance of all terms and conditions within this and associated protocols and guidelines and of the consequences of inappropriate use.

2.1 Computer Access Control

Access to UWS IT systems is controlled by the use of a user ID and password using Multi-Factor Authentication. All user IDs are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on UWS IT systems and equipment by anyone who uses that ID. All those with a user ID must comply with the Password Management Procedure.

Individuals must not:

a) Allow anyone else to use the user ID allocated to them on any UWS system or equipment.

b) Allow any unauthorised person to use UWS devices

c) Leave user accounts logged in at an unattended and unlocked computer.

d) Use weak or easily guessable passwords. Where weak passwords are identified IT may disable access to the account if the service user is not contactable.

e) Use someone else's user ID and password to access UWS systems or equipment.

f) Leave passwords unprotected (for example written down in view of others).

g) Perform any unauthorised changes to UWS IT systems or information.

h) Install any unauthorised software on UWS equipment

i) Attempt to access data that they are not authorised to use or access.

j) Use a device infected with malware on the UWS network. Devices identified as 'infected' will be blocked from accessing the network until the issue can be confirmed as resolved. Attempts will be made to the user, however access will be blocked even if use is not contactable.

k) Exceed the limits of their authorisation or specific business need to interrogate the system or data.

l) Fail to return UWS IT equipment at the end of their contract of employment. Notification of equipment not returned by contract end date will be escalated to DPO/Legal as a potential data protection issue.

m) Gain or attempt to gain unauthorised access to accounts or passwords

n) Fail to return UWS equipment at the end of a loan period.

o) Take corporate laptops and other mobile devices outside of the UK without prior approval from Risk and Resilience. Loan devices must be booked from IT if a device is required to be taken to potential 'Risk' countries (including China).

p) Take UWS corporate IT devices on holiday. UWS IT laptop and other mobile phones are not covered under the organisation insurance policy during periods of annual leave.

q) Use USB storage devices which are not encrypted. Use of USB devices for storage should be by exception.

r) Respond to emails or anyone asking you to disclose your password. The Helpdesk will never ask you to tell them your password.

s) Engage in online discussions or forums that promote or sympathise with extremist ideologies.

t) Use encrypted platforms or hidden networks for accessing or sharing extremist content.

The security of UWS information and information systems is critical and all use and access to data must comply with the IT Information Security Procedure.

2.2 Internet Access

Access to the internet is provided primarily via the Janet network. Use of the internet should also comply with the Jisc Acceptable Use Policy:

Use of the internet via UWS equipment is intended for University use. Personal use is permitted but should be kept to a minimum so that it does not compromise a staff member's work or a

student's course related study. It should also not preclude others with work-related or course related needs from using the resources.

2.3 Email

University emails may require to be disclosed under the Freedom of Information (Scotland) Act 2002 or the Data Protection Act 2018. Therefore, users should be aware of the content and language used in e-mails and avoid emotive or subjective language.

Students must not send emails which make representations, contractual commitments or any other form of statement concerning the University unless they have specific authority to do so.

2.4 Social Media

Social media can be a useful tool to encourage student engagement and learning but can be far more informal in nature. Staff should be aware of this when communicating with students via social media and should never share information with students or interact with them in a way that they would not willingly or appropriately do in a University or other public setting. Staff should not communicate via social media in a way that may bring the University into disrepute e.g. using offensive or discriminatory language or posting inappropriate images/content.

Use of social media sites including Instagram, Facebook, Twitter, YouTube online blogs and wikis has increased the risk of inappropriate content being published. Users should be careful not to associate themselves with UWS on personal sites if the views or information on the site might cause conflict with the University.

Access to these sites is not controlled by the institution but users are expected to behave responsibly when using them, particularly when accessing them via the university's network and to comply with the Guidelines for the use of Social Media at UWS.

2.5 Personal Data

Under UK GDPR, personal data is any information which is related to an identified or identifiable natural person. Users must be familiar with the University's Data Protection Code of Practice. Personal data being sent outside the University must be encrypted. If personal data is being transferred outside of the European Economic Area (EU members states plus UK, Iceland, Norway and Liechtenstein), please contact the Legal Services team.

All users are accountable for their actions on the internet and when using email and social media. All institutional protocols and legislation restricting the disclosure of confidential or personal information must be maintained. Disciplinary action may be taken where this is not adhered to.

2.6 Unacceptable Use

Unless such use has been approved for an academic or research purpose, or pursuant to a formal University investigation, one or more of the following is considered unacceptable use for all users:

1. Installation of any software that is not provided by the University. Use of pirated software or illegal use of licensed software.
2. Use of software no longer receiving vendor security updates and not supported by a current maintenance agreement.
3. Modifying or circumventing the precautions taken by the University to prevent virus infection.
4. Using the facilities for monetary gain.
5. Preventing others from making legitimate, work-related use of the facilities.
6. Trying to gain unauthorised entry to other computer systems or files ('hacking').
7. Copying, deleting or making changes to any files, directories or folders other than those in connection with their work.

8. Tampering, adjusting, switching on/off or otherwise interfering with the equipment in open access labs and teaching labs other than normal usage.
9. Transmission of unsolicited commercial or advertising material, save where that material is embedded within, or is otherwise part of, a service to which the recipient has chosen to subscribe.
10. Creating, transmitting, transferring, downloading, browsing, viewing, reproducing or accessing any image, material or other data of any kind, which contains unacceptable content, including but not limited to:-
    a) Sexually explicit messages, images, films, video clips, cartoons, jokes or any other material of a sexual nature
    b) Any other content which may offend, harass, provoke, demean, degrade or threaten any other person (whether a fellow employee or a third party) whether on the grounds of age, disability, gender re-assignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation
    c) Any content that promotes violence, terrorism or extremism or contravenes current anti-terror legislation as per the Terrorism Act 2000 and UK Government Prevent Strategy
    d) Any content that is illegal, defamatory, malicious, libelous, derogatory or causes annoyance or needless anxiety
    e) Any inappropriate use of social networks, chat-rooms, newsrooms, bulletin boards, blogs or wikis, as defined by the Guidelines for the use of Social Media.
    f) Any content that deliberately introduces a virus, malware or spyware into the UWS network or systems or the network or systems of any other party, which is designed to corrupt or destroy the data of other users or in any other way compromise the integrity of those systems.
    g) Any content for private business purposes, or content that conflicts with the University's interests or policies.
    h) Any content that infringes or may infringe the intellectual property or rights of others or data protection rights.
    i) Content that discloses information that is confidential to the University or its employees.
    j) Creation of content that benefits any political organisation.
    k) Failure to return IT equipment at the end of UWS contract.
    l) Any content that may bring the University into disrepute.
    m) Any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us).
    n) Any content that breaches Dignity & Respect at Work Guidelines.

These restrictions apply to work, course related use and personal use. The University considers it important that all use is restricted in this way to avoid disruption in the workplace and the learning environment while reducing the likelihood of embarrassment, distress or offence to others. Any failure to comply may be dealt with under disciplinary procedures.

3. PROCEDURE

3.1 Monitoring and Compliance

The use of any University IT systems, equipment and network is monitored in order to ensure that this use is compliant with the law and with University rules.

All data that is created and stored on UWS computers remains the property of UWS. Only under certain circumstances will access to another user account or email be permitted. Any access requires to be authorised by the *IT Security and Customer Support Manager*, *Legal Team, People & Wellbeing* or *Dean of School* or *Head of Department*. Any access will only be given to an appropriate staff member subject to Data Protection laws and monitored by *People & Wellbeing*.

Personal data should not be stored on UWS equipment, network or cloud storage. Examples of this include but are not restricted to personal photographs, music, films and other media files. Network storage will be monitored for these files and may be deleted.

Inbound and outbound internet traffic is scanned for security threats. Access to categories of websites that are deemed unacceptable are blocked by Information Services from the University network.

Some staff and students may be involved in legitimate teaching or research that involves a blocked website. When this is the case, access should be requested via the Information Services Helpdesk. Authorisation will be required from the relevant Dean of School or Head of Department prior to this access being granted.

Investigations will be commenced where reasonable suspicion exists of a breach of this or any other relevant policy. The University may use an external agency to carry out appropriate technical investigations. Any suspected breach of this procedure must be reported immediately to the *IT Security and Customer Support Manager* or the *Information Services Helpdesk* to allow investigation of the incident prior to taking appropriate action.

All breaches will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with UWS disciplinary procedures for staff. Pending investigation of a suspected breach of the policy, IT services may be suspended for that individual.

User behaviour is subject to the laws of the land, even those that may not apparently relate to IT such as the laws on fraud, theft and harassment. Where investigation reveals activity that is considered to be in breach of current laws, the incident will be escalated to a senior member of staff. The matter may be reported to the appropriate authorities on the guidance of senior management. Relevant current legislation includes, but is not limited to, the following:

a) Communications Act 2003
b) Computer Misuse Act 1990
c) Copyright, Designs and Patents Act 1988
d) Criminal Justice and Public Order Act 1994
e) Data Protection Act 2018
f) Human Rights Act 1998
g) Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
h) Equality Act 2010
i) Regulation of Investigatory Powers Act 2000
j) Freedom of Information (Scotland) Act 2002
k) Counter Terrorism & Security Act 2015

3.2 Device Tracking

Device geolocation monitoring may be enabled on a corporate device where a theft of loss has been reported in order to identify the last known location of the device. Any UWS owned device not returned at end of employment will be categorised as a lost device and may be tracked.

Requests to track a device for any other reason will be rejected by IT/Legal unless there was a safety concern for the individual the device is allocated to.

3.3 Government Prevent Strategy

The University has a duty under the Counter Terrorism & Security Act 2015 to have *"due regard to the need to prevent people from being drawn into terrorism".*

One way in which people can become drawn into terrorism or extremism is via online material. This policy prohibits accessing, posting or contributing any material (whether at the University or otherwise) that promotes terrorism or extremism as defined in the Government's Prevent Strategy 2011:

"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. We also include in our definition of extremism calls for the death of members of our armed forces."

A secure web gateway provides UWS with web content categorisation. Website categories that would breach this policy are blocked by default. Some staff may be involved in legitimate teaching or research into blocked topics that are sensitive in nature. When this is the case:

1. Explicit approval must be obtained from the staff member's line manager.
2. Ethical approval must be obtained through the appropriate School Ethics Committee or University Ethics Committee.
3. Robust storage must be in place, so the material is only accessible by the relevant individual(s).

Should a member of staff become aware that a student or member of staff has been attempting to access terrorism or extremism related content, they should discuss this confidentially with their line manager or a senior member of staff. If necessary, the line manager or senior member of staff will then escalate this via prevent@uws.ac.uk.