Acceptable Use of Technology Policy [IT01]

T:C Partnership
Training • Education • Careers

Change Control

Policy Name and Reference	Acceptable Use of Technology Policy [IT01]
Version	V1.5
Name of Responsible Committee	GLT
Job Title of Responsible Author	Group Executive Director of ICT
Date First Issued	May 2020
Date Current Version Issued	May 2025
Date of next Planned Review	May 2026

Revision History

Version	Date	Type of Amendment	Amendment Details
V1.0	May 2020	New	New Policy
V1.1	May 2021	Updated	
V1.2	May 2022	No changes	
V1.3	May 2023	No changes	
V1.4	May 2024	Updated	Table of contents / general restructuring of contents of policy, inclusion of sections 11, 4.2, reference to the JISC AUP in section 2, updating of email address and the IT Services phone number.
V1.5	June 2025	Update	Added a new section – 8. Utilizing Artificial Intelligence Technology and 13. Sign-Off and Acknowledgement. Included text referencing AI in the 'Purpose' section.

Table of Contents

1. Purpose

The Acceptable Use of Technologies Policy (AUTP) applies, without exception, to the use of TEC Partnership's IT facilities, equipment, network infrastructure and AI Technology. The purpose of this policy is to provide guidance on the use of network resources and services which includes the use of any TEC Partnership technology resources (internal or cloud based, the internet, email, instant messaging, social media, media publications, file transmission and voice/data communications).

2. Scope

This policy applies to anyone authorised to use TEC Partnership-owned computers or devices, as well as personal devices connected to the TEC Partnership network for accessing services such as email, internet, and other network resources—whether on-site or remotely. This includes all full-time and part-time staff, agency and casual workers, students, contractors, sub-contractors, individuals on work experience, visitors, and guests. All users are required to familiarise themselves with and adhere to the Acceptable Use of Technology Policy (AUTP). The policy is available on the TEC Partnership website and SharePoint, with printed copies available upon request.

3. Change

This policy is maintained by the TEC Partnership's IT Services department. Requests to change the policy should be made to the Group Executive Director of ICT, in writing, and approved by the Group Leadership Team.

4. Policy

All users must comply with all the relevant legislation listed in section 11 of this policy. Any breach of legislation or related policies is an offence and will be subject to the TEC Partnership' s disciplinary procedures.

For further information, please contact IT Services: itservices@tecpartnership.ac.uk

1. Authorisation

To use ICT facilities at the TEC Partnership, a person must have authorised access to the network. The use of facilities will be deemed an acceptance of this policy's terms and conditions. It is expected that all users will adhere to password guidelines and GDPR policies in addition to all relevant regulatory and legal requirements.

2. Definition of Acceptable Use

Users are encouraged to use all IT facilities, networks, systems, AI Technologies and services for work and study only.

Personal use is a privilege, not a right, with conditions:

- Study and work come first; ensure it does not interfere with productivity or security.
- Everything you do complies with all TEC Partnership policies. If in doubt, do not do it and seek advice.
- Always be respectful to other staff and students.
- Only authorised and licensed software should be used on company devices.
- All company devices accessing remotely shall do so using the secure and authorised VPN and personal devices are not permitted to corporate network.

3. Definition of Unacceptable Use

Unacceptable use of TEC Partnership's IT systems and network resources includes, but is not limited to, the following activities:

Inappropriate Content and Behaviour

- Accessing, creating, or sharing material that is fraudulent, illegal, obscene, or otherwise inappropriate.
- Engaging in harassment, bullying, or intimidation of staff or students, including discriminatory messages based on sex, race, disability, religion, sexual orientation, or age.
- Using profane, abusive, or hate-inciting language.
- Defaming individuals or groups (excluding legitimate academic critique).
- Infringing on intellectual property rights, including copyright and trademarks.

Misuse of Communication Tools

- Sending unsolicited messages or spam.
- Forging email addresses or impersonating others.
- Using ICT systems for personal commercial gain or trading.

System and Network Misuse

- Attempting to hack, damage, or gain unauthorized access to systems or data.
- Introducing or distributing malware or viruses.
- Connecting unauthorized hardware to the network.
- Circumventing network access controls or monitoring traffic without permission.
- Probing for system vulnerabilities (e.g., port scanning) without authorization.

Resource Misuse

- Excessive use of non-work-related websites or applications (e.g., social media).
- Generating heavy network traffic through non-academic activities.
- Using peer-to-peer applications (e.g., BitTorrent, uTorrent and Vuse) for non-educational purposes.
- Storing or distributing unlicensed software, music, or media.
- Copying website content or software without permission.
- Overusing shared resources (e.g., file storage) to the detriment of others.

Staff, learners, and visitors should consider the spirit of the TEC Partnership's Ethos when working on The TEC Partnership systems. Any conduct which may discredit or harm the TEC Partnership, its staff or the ICT facilities or can otherwise be considered intentionally unethical is deemed unacceptable.

Incidents of misuse will be dealt with by the TEC Partnership in accordance or be subject to the disciplinary procedures outlined in the terms and conditions of employment (staff) and admissions policy (learners). The appropriate level of sanctions will be applied as determined by the reported misuse.

4. TEC Partnership Network Use

The TEC Partnership network is not to be used for any of the following purposes:

Viewing, creating, storing, transmitting or deliberate receipt (other than for properly supervised and lawful research purposes) of any offensive, obscene, or indecent images (including pseudo images), data or other material, or any data capable of being resolved into obscene, unlawful, or indecent images or material.

Viewing, creating, storing, or transmitting material which causes, or is likely to cause annoyance, revulsion or needless anxiety to the TEC Partnership, its staff, learners, visitors or any third party.

Viewing, creation or transmission of defamatory abuse or other unlawful material in respect of the TEC Partnership, its staff, learners, visitors or any third party.

Viewing, storage or transmission of material in such a manner that it infringes the copyright of the TEC Partnership, another person or organisation or which discloses confidential or sensitive information or data relating to the TEC Partnership, its staff, learners, visitors or any third party.

a. transmission of unsolicited commercial or advertising material.
b. any other act which is considered unlawful in any country where the network is being accessed.
c. deliberate activities with any of the following characteristics:
    - wasting staff effort or networked resources, including the effort of staff involved in the support of these services, including but not limited to.
    - corrupting or destroying the TEC Partnership's or other users' data.
    - manipulating and altering assessments, grades, or transcripts.
    - accessing and copying files of other users to obtain an improper advantage.
    - violating the privacy of the TEC Partnership or other users.
d. disrupting the work of other users; using the TEC Partnership network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment).
e. continuing to use an item of networking software or hardware after a request that use cease because it is causing disruption to the correct functioning of the TEC Partnership network.
f. other misuse of TEC Partnership network or networked resources, such as the introduction of viruses, extracting material of others and passing it off as one's own, manipulating material of the TEC Partnership or others to one's own advantage, whether pecuniary or otherwise.

Where the TEC Partnership network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the TEC Partnership network.

All the provisions of the Acceptable Use Policy of the Joint Academic NETwork ("JANET") apply to users of the TEC Partnership network in addition to the provisions herein.

Users are not permitted to access the TEC Partnership network on behalf of third parties without prior written agreement of the TEC Partnership.

It is beyond the resources and ability of the TEC Partnership to monitor all activities. However, where there is a sound reason to suspect unacceptable use as defined above, the TEC Partnership reserves the right to inspect a user's material and use history, including email messages, and at its sole discretion block or edit such material as it sees fit. Furthermore, sometimes, the TEC Partnership may implement technical measures to monitor activity on the TEC Partnership network to ensure compliance with the requirements of this policy and to conduct tests for research purposes.

Acceptance of the right of the TEC Partnership to take steps to prevent suspected misuse is a condition of access to the TEC Partnership network.

Any external organisation having a direct link into the TEC Partnership network must take reasonable steps to ensure compliance with the requirements of this Policy and to ensure that unacceptable use of the TEC Partnership network does not occur. The external organisation must also accept responsibility for adequately informing its own users of the conditions of use of the TEC Partnership network.

Where necessary, and at the sole discretion of the TEC Partnership, access by an individual or organisation may be withdrawn, temporarily or indefinitely.

In the event of misuse of the TEC Partnership network, the TEC Partnership reserves the right to exclude access to any external organisation, or employee, or learner and in the case of:

1. misuse by an employee of the TEC Partnership, to proceed against that employee under the TEC Partnership's disciplinary procedures for employees and
2. misuse by a student, to proceed against that student in accordance with the TEC Partnership's Learner Disciplinary Procedures.

Individuals must not share the passwords for any of their TEC Partnership accounts. Account owners are held responsible for all activities and content associated with their accounts. Failure to conform to these requirements may lead to the suspension of account privileges or other actions as provided by the appropriate TEC Partnership policy. If an individual believes that someone else is accessing their account, they must report this immediately to the IT Services - **itservices@tecpartnership.ac.uk**

5. Device / Laptop Security Guidelines

This section provides recommendations for where laptop computers and other mobile devices are used. The policy is equally applicable to contractors, service providers and other organisations or agencies that use laptop computers to process TEC Partnership information in the performance of their duties.

Introduction

Mobile devices taken outside secure TEC Partnership environments are subject to special security risks: they may be lost or stolen and may be exposed to unauthorised access or tampering. Devices taken abroad may also be at risk, for example confiscated by police or customs officials.

Device loss will mean not only the loss of availability of the device and its data but may also lead to the disclosure of sensitive information – such as student assessment data. This loss of confidentiality, and potential integrity, will often be considered more serious than the loss of physical assets.

Where data should not be stored on the device but rather on the cloud and/or network storage systems provided.

If quantities of TEC Partnership data are held on a single device (or any other storage medium), risk assessment must consider the impacts of loss of all data. Note that deleted files should be assumed to persist on the device's hard drive.

Key Points:

Traditional password protection on a device offers limited defense against a determined attacker because the attacker has unconstrained access to the physical device. Modern complex password techniques offer more protection, which must therefore be used.

The physical security controls that are possible within the TEC Partnership buildings environment are not available outside of that environment; therefore, if procedural and personal controls of the device are breached the only effective technical measure that can be applied is encryption.

Unauthorised access and tampering to a device, particularly if there are repeated opportunities for access, may:

1. lead to continuing (and undetected) compromise of information on the device itself.
2. undermine security measures (including encryption); intended to protect information on the device in the event of loss or theft; and
3. lead to compromise systems to which the device is connected, for example, a networked system that is accessed from the laptop.
4. The impact of a breach of device security may therefore extend far more widely than the device itself.

6. Security of Equipment off-premises

Security should be applied to off-site equipment considering the different risks of working outside the organisation's premises.

Security risks, e.g., damage, theft, or eavesdropping, may vary between locations and should be considered in determining the most appropriate controls.

7. Mobile Devices and Communications

Appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

Care should be taken to ensure business information is not compromised. Users should take care and make themselves aware of the risks of working with mobile computing equipment in unprotected environments.

If lost or stolen the user must call IT Services immediately on 01472 315571. IT Services will arrange to block a SIM device. If the device is lost outside office hours, the end user should contact Vodafone Customer Services.

If damaged, then the user must return it to IT Services who will then arrange for the repair of the device and will also issue a standard replacement device (not a premium or optional handset) whilst the damage is in repair. It is up to the user's line manager to decide whether the user will have to financially contribute towards the cost of repair. It is at the line manager's discretion to decide whether the user will have to financially contribute towards the standard handset.

The equipment must be returned in the condition received by IT Services when the employee terminates employment.

Although they may be insured whilst in college, they are not insured elsewhere and therefore users must be aware that their department will need to pay for replacement if lost, damaged or stolen. It is at the department manager's discretion whether to ask for a contribution from the staff user towards the replacement of the equipment.

TEC Partnership reserves the right to recharge the individual concerned if high usage/costs are deemed unnecessary or not work related.

International travel is sometimes required for work purposes. Where this is required, the employee should email their mobile number and destination to services@tecpartnership.ac.uk and/or purchasing@tecpartnership.ac.uk before leaving the country. This will ensure that an appropriate tariff is selected. Personal use of mobile

phones abroad is not allowed, and any charges incurred due to personal use will be charged to the employee.

Staff are required to abide by the current legislation when using the device while driving. TEC Partnership takes no responsibility whatsoever for the consequences of unlawful behavior or any other malpractice.

TEC Partnership will review this policy at times or at the point of contract renewal with the mobile phone provider.

8. Utilizing AI Technology

TEC Partnership supports the responsible and ethical use of Artificial Intelligence (AI) technologies to enhance teaching, learning, and administrative processes. AI tools may be used to support personalized learning, automate routine tasks, and provide insights into student performance, provided their use aligns with institutional values and data protection regulations.

Users must ensure that any AI technology employed—whether for academic support, content generation, or decision-making—is used transparently and does not compromise academic integrity, privacy, or fairness. Students and staff are expected to critically evaluate AI-generated content and remain accountable for the originality and accuracy of their work.

The use of AI tools must comply with all relevant policies, including the Data Protection Policy, Information Security Policy, and Academic Integrity Policy. Any AI system that processes personal or sensitive data must be approved by the IT Services team and subject to appropriate risk assessments.

Misuse of AI technologies, including but not limited to plagiarism, data misuse, or unauthorized automation, may result in disciplinary action.

9. Security Measures

- Ensure that device(s) are not left unattended when working off-site.
- When travelling and not in use, ensure that device(s) are stored securely out of sight. For example, when traveling by car, ensure laptops are locked in the boot. Devices left on display and unattended will inevitably attract attention and are likely to be stolen.
- It is good practice to carry laptops in protective anonymous bags or cases (i.e., those without manufacturer logos on them) when not in use.
- Do not leave laptops or mobile devices unattended in car boots overnight.

- Do not leave device(s) unattended in insecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available.
- Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc. and on public transport e.g., buses and trains.
- When travelling, avoid placing device(s) in locations where they could be easily forgotten or left behind e.g., overhead racks and taxi boots.
- Be aware that using laptops in public places will draw the attention of those nearby. It is possible that information viewed on a laptop screen could lead to the unauthorised disclosure of that information being processed.

10. Privacy and Monitoring

The IT Services department reserves the right to monitor email, telephone, and any other electronically mediated communications, whether stored or in transit, in line with relevant legislation. The TEC Partnership, however, recognises that users' statutory rights to privacy are not affected by this policy.

Reasons for such monitoring include but are not exclusively the need to:

- Investigate or detect unauthorised use of TEC Partnership telecommunications systems and ensure compliance with this policy or other TEC Partnership policies.
- Ensure operational effectiveness of services (e.g., to detect viruses or other threats to the systems).
- Prevent breach of the law or investigate a suspected breach of the law, the TEC Partnership policy, or contracts.
- Monitor standards and ensure effective quality control.
- Compliance with Government's Prevent Duty.

Monitoring may involve (but not exclusively):

- Examining the number and frequency of emails.
- Viewing sent or received emails from a particular mailbox or stored on any server.
- Examining logs of ICT facility usage.
- Monitoring the amount of time spent on the Internet.
- Internet sites visited and downloaded information.
- Keywords typed into a web browser and or any locally installed applications.

Where abuse is suspected, a more detailed investigation involving further monitoring and examination of stored data may be undertaken.

Where disclosure of information is requested by the police (or another law enforcement authority) the request should be directed to the Executive Director of IT, Group Vice Principal of Corporate Services, Group Vice Principal of People & Culture or GDPR Officer.

Staff that have access to personal data, (as defined under the General Data Protection Regulations 2018) are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and manage this data is not compromised.

Staff found to be in breach of this policy may be subject to disciplinary action and/or legal action if a criminal offense has been committed.

11. Legal Constraints

Software may not be copied, installed, or used on the TEC Partnership's IT equipment except when and as permitted by the owner of the software and by law and with agreement from the TEC Partnership IT Services department. The department will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license It is up to the user to check the terms and conditions of any license for the use of the software or information and to abide by them.

Software provided by the TEC Partnership's IT Services department may only be used as part of the user's duties as an employee or student or for educational purposes. The user must abide by all the licensing agreements for software entered by the by the TEC Partnership with other parties, noting that the right to use any such software outside the TEC Partnership premises will cease when an individual leaves the institution. Any software on a privately-owned computer that has been licensed under the TEC Partnership's agreement must then be removed from it, as well as any TEC Partnership owned data.

T:C Partnership
Training • Education • Careers