



### Version Control Statement

<b>ID Number:</b>	FW04 4	<b>Document Name:</b>	IT_Acceptable_Usage_Policy_V1.0.1	
<b>Approving Committee:</b>	Operations Team			
<b>Last Review:</b>	August 2025	<b>Next Review:</b>	Sep-27 to Nov-27	
<b>Owner:</b>	Vice Principal	<b>Review Lead:</b>	Facilities Manager	
<b>Amendments Since Approval:</b>	<b>Detail of Revision:</b>	<b>Date of Revision:</b>	<b>Revision Approved by:</b>	
	IT Acceptable Usage Policy replaced Internet usage policy	05/08/2021	Executive Committee	
	Executive Team changed to Operations Team as approving committee	10/09/24	Operations Team	
	Relevant UK Legislation and Futureworks policies updated	11/08/25	Operations Team	

If this document is required in an alternative format, please contact Futureworks on 0161 214 4600 or via email: [info@futureworks.ac.uk](mailto:info@futureworks.ac.uk)

#### IT Acceptable Usage Policy

This policy document details the acceptable usage and behaviour of users whilst using Futureworks IT facilities. IT facilities covered by this policy include the local computer network, internet access, computer hardware and all other IT services. This policy is enforced to ensure the safe, lawful and fair usage of IT Facilities at Futureworks to support a productive, inclusive and equitable learning environment.

#### **Acceptable Use**



Acceptable use includes all legal use that furthers the learning, teaching and other relevant activities of Futureworks students and staff that do not fall under unacceptable use as detailed in the following section.

### **Unacceptable Use**

To maintain safe, lawful and fair usage, the below activities are deemed as unacceptable use and are not authorised whilst using Futureworks IT Facilities.

1. Any use in contravention of law or other Futureworks policy or use that promotes the contravention of law or other Futureworks policy.
2. Access, transmission or storage of offensive, obscene or indecent images, data or other material.
3. Access, transmission or storage of unlawful material, including defamatory, discriminatory, threatening, extremist material or material which has the potential to radicalise.
4. Access, transmission or storage of material promoting discrimination on the basis of any protected or other characteristic.
5. Usage that promotes an offensive or threatening environment or that may constitute harassment.
6. Unauthorised downloading and installation of software.
7. Use of hardware for Cryptocurrency farming.
8. Transmission or storage of material in breach of copyright law and intellectual property rights.
9. Transmission or storage of material in breach of the privacy rights of a third party.
10. Nuisance behaviour that causes unnecessary annoyance, concern or offence to other members of the Futureworks community or public.
11. Impersonation or imitation of another person or their online accounts and services.
12. Transmission of spam email.
13. Intentional introduction of computer viruses, spyware or any other form of malware to Futureworks IT Facilities.
14. Attempting to gain unauthorised access to user data or areas of the network which are restricted.



### **Monitoring & Compliance**

Futureworks IT Facilities are under constant review and usage is subject to monitoring. Monitoring by IT staff is in place to ensure compliance with this policy and to ensure that safeguarding and prevent duty responsibilities are being fulfilled. Though Futureworks internet facilities are not filtered it is the expectation that staff and students will use this facility in good faith and in a manner promoting safe, lawful and fair use. Internet traffic will be monitored by IT staff and misuse flagged for investigation by Management. Failure to comply with this policy may lead to investigation and disciplinary procedures under the Regulations for the Conduct of Students which could ultimately lead to suspension or withdrawal from your course.

### **Additional information**

All staff and students will be briefed on this policy during induction by the Facilities Team. Queries regarding this policy can be sent to [it@futureworks.ac.uk](mailto:it@futureworks.ac.uk)

Relevant UK Legislation and Futureworks policies:

- Malicious Communications Act 1988
- Online Safety Act 2023
- Computer Misuse Act 1990
- Data Protection Act 2018
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Investigatory Powers Act 2016
- Communications Act 2003
- Counter-Terrorism and Border Security Act 2019
- Terrorism Prevention and Investigation Measures Act 2011 Copyright, Designs and Patents Act (1988)
- Digital Economy Act 2010
- [Student Harassment Policy and Sexual Misconduct Policy](#)
- [Safeguarding Policy and Procedure](#)
- Ethical Practice Policy (Academic)



- Student Social Media Policy
- [Data Security Policy](#)
- [Equality & Diversity Policy](#)