

INFORMATION SECURITY ACCEPTABLE USE POLICY

January 2026

Document title	
Information Security Acceptable Use Policy	
Document author and department	
Ewa Kolaniak, Cyber Governance Risk and Compliance Manager, Information Security Team	
Approving body	
University Executive Board	
Date of approval	
26.01.2026	
Review date	
15.12.2025	
Edition no.	
4	
ID Code	
051	
Date of effect	
26 January 2026	
Document title	
For a) public access online internet or b) staff only intranet?	b)
<p>External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk</p> <p>If you need this document in an alternative format, please email corporate.communications@port.ac.uk</p> <p>The latest version of this document is always to be found at: https://policies.docstore.port.ac.uk/policy-051.pdf</p>	

Contents

Summary	4
What is this document about?	4
Who is this for?	4
Who can you contact if you have any queries about this document?.....	4
Executive summary	4
1. Purpose	5
2. Scope	5
3. Applicability	5
4. Risk	5
5. University Systems and Services	5
5.1 Acceptable Use:	5
5.2 Unacceptable use	6
6. Use of Email and Communication Tools	6
6.1 Acceptable Use:	6
6.2 Unacceptable Use:	7
7. Use of Mobile Devices and Remote Access	7
7.1 Acceptable Use:	7
7.2 Unacceptable Use:	7
8. Use of Artificial Intelligence	8
8.1 Acceptable Use:	8
8.2 Unacceptable Use:	8
9. Violations	8
10. Monitoring and Privacy	8
10.1 Monitoring is conducted to:	8
10.2 Key principles:	8
11. Policy Enforcement	9
12. Related Policies and References	9
13. Policy Review	9
Appendix A: Examples of Unacceptable Use of University	10
IT Facilities	10

Summary

What is this document about?

This Policy sets out what the University of Portsmouth regards as acceptable use and unacceptable use of its Information Technology facilities. The Policy ensures that all users understand the way in which the University's information technology systems and information should be used.

Who is this for?

This Policy applies to all staff, students and other users of University IT systems and technology, services and data.

How does the University check this is followed?

Subject to UK legislation, the University reserves the right to monitor, scan or otherwise probe its IT facilities, systems and networks, to detect potential problems, investigate security issues and maintain and protect an efficient service.

Monitoring will take place within the terms permitted under the Regulation of Investigatory Powers Act (RIPA) 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations) 2000 and the Investigatory Powers Act 2016.

The University also reserves the right to inspect any items of computer equipment connected to the University network. Any IT equipment connected to the University's network will be blocked if it is deemed to be in breach of this Policy or otherwise interfering or having the potential to interfere with the operation of the University network.

Who can you contact if you have any queries about this document?

Any questions or concerns relating to the terms or implementation details associated with this Policy should be addressed to the Information Security Team at cybersecurity@port.ac.uk.

Executive summary

The key elements of this Policy are as follows:

- University IT facilities, systems, services and data are provided to authorised individuals to support learning, teaching, research, administration and approved business activities of the University.
- The University reserves the right to take appropriate action against those using, or suspected of using, its IT facilities, systems, services and data in a manner it decides is unacceptable.
- Any misuse of the system may result in formal disciplinary action and, in some instances, the police or other enforcement authorities may be notified. If a user is subject to University disciplinary procedures or a police investigation, then their access to IT facilities and/or UoP data may be blocked.

1. Purpose

This Acceptable Use Policy (AUP) outlines the responsibilities for using the University's information systems, digital services, networks, and data. It requires all users to act lawfully, ethically, and securely when accessing University data and systems.

The policy aims to:

- a) Provide guidance on expected working practice
- b) Highlight issues affecting use
- c) Describe the standards that users must maintain
- d) State the actions that may be taken to monitor the effectiveness of this policy
- e) Warn users about the consequences of inappropriate use of the University's systems, services and data

2. Scope

This policy applies to the use of the University's IT facilities, digital services, data and networks. It covers all devices, accounts, software and services provided or supported by the University, regardless of location, and applies to the equipment that is used to access University systems, networks and applications. It also applies to digital communications (e.g. email, messaging platforms), online collaboration tools, cloud-based services, and any use of artificial intelligence (AI) tools that are used for University's activities.

3. Applicability

This policy applies to all systems, people and processes that constitute the organisation's information systems, including, governors, directors, employees, suppliers, students, contractors and other third parties who have access to University of Portsmouth systems and data.

4. Risk

This Acceptable Use Policy reduces risk of unlawful, unethical, and insecure use of University's resources. It also mitigates threats that could harm operations, reputation, or regulatory compliance.

5. University Systems and Services

University systems and services—including IT infrastructure, networks, software, communication tools, and digital platforms—are provided to support the University's mission in teaching, learning, research, and administration.

5.1 Acceptable Use:

- A. Use systems responsibly, lawfully, and in line with University's policies and applicable UK laws.
- B. Protect login credentials and do not share accounts or provide access to them to others.
- C. Access only data and resources for which you have authorised permission.
- D. Avoid any activity that could disrupt or damage University systems, including introducing malware, bypassing security controls or overloading networks.
- E. Use University digital tools primarily for University-related activities; limited personal use may be permitted but must not interfere with work or violate this or any other University policy.
- F. Seek explicit approval before using any external or cloud services that involve processing University data.

Access to offensive or sensitive material for valid reasons—such as in studies on racism—requires prior written approval from the Head of Department and the Departmental Ethics Committee.

5.2 Unacceptable use

- A. Bypass, disable or reduce the efficiency of security controls (e.g., antivirus, firewall, MFA)
- B. Share or reuse credentials
- C. Use unauthorised (not approved) software or hardware
- D. Access systems/data without proper authorisation
- E. Use University IT resources for illegal or unethical activity
- F. Attempt to gain unauthorised elevated privileges ("privilege escalation")
- G. Use anonymisation tools to hide activity (e.g. unapproved VPNs)
- H. Store sensitive data on unapproved platforms or personal devices
- I. Send confidential data unencrypted over email or external services
- J. Tamper with physical or environmental security (e.g. unlocking access doors)
- K. Excessive personal use that impacts performance/security
- L. Fail to report known security incidents or vulnerabilities
- M. Install or use unauthorised network scanning, sniffing, or attack tools
- N. Engage in cyberbullying, harassment, or sending offensive material
- O. Create, distribute, or facilitate the use of malware (e.g., viruses, worms, ransomware, trojans, spyware)
- P. Engage with or deliberately propagate phishing content including:
 - I. Knowingly clicking on suspicious or malicious links or attachments out of curiosity or with intent to investigate without authorisation.
 - II. Forwarding suspected phishing emails to others, except when reporting to the IS Service Desk or as requested by the cyber team.
 - III. Entering sensitive information into websites or forms which are known or suspected to be fraudulent.
- Q. Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive
- R. Utilise unapproved internet services that facilitate data exfiltration or that may introduce malicious software
- S. Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of unauthorised music, video or image files, using online gaming, betting sites or "money making" sites

Any staff member found to be using IT Systems, against acceptable usage, may be subjected to formal disciplinary action as detailed within the University of Portsmouth Disciplinary policy.

6. Use of Email and Communication Tools

University provided email accounts and communication tools (e.g. Microsoft Teams, Zoom) are essential for teaching, learning, research, and administration. These tools must be used in a respectful, secure, and professional manner.

6.1 Acceptable Use:

- A. Use University email and communication platforms primarily for University's related purposes.
- B. Communicate in a respectful and inclusive manner, avoiding language or behaviour that could be considered discriminatory, harassing, offensive, or threatening.

- C. Avoid using personal email accounts for University business, especially when handling personal or confidential data.
- D. Do not impersonate others, misrepresent the University, or conceal identity in communications.
- E. Be cautious when opening unexpected attachments or clicking links to avoid phishing or malware.
- F. Comply with legal requirements and University policies on data protection, confidentiality, and academic integrity.

6.2 Unacceptable Use:

- A. Use University systems to send spam, chain letters, or unsolicited bulk messages.
- B. Share inappropriate, offensive, or illegal content without relevant approvals.
- C. Use email or communication tools for personal business, political campaigning, or financial gain.
- D. Automatically forward University email to personal accounts without proper security controls.

7. Use of Mobile Devices and Remote Access

The University recognises the need for flexible and mobile working. Staff, students, and authorised third parties may use mobile devices (e.g. laptops, smartphones, tablets) and access University systems remotely to support academic, research and administrative activities, provided this use is secure and in line with University policies.

7.1 Acceptable Use:

- A. Ensure that any device used to access University systems and networks (including personal devices) is secured with up to date, supported operating systems, anti-malware protection, and screen lock/passcode security.
- B. Use strong passwords and, where required, multi-factor authentication (MFA) when connecting to University services.
- C. Access University systems remotely only via approved secure methods (e.g. VPN, virtual desktop environments, or authenticated cloud platforms).
- D. Immediately report any loss, theft, or compromise of devices used to access University systems or data to the Service Desk.
- E. Ensure that sensitive or confidential information is not stored locally on personal devices unless specifically authorised and encrypted.
- F. Keep devices physically secure and avoid using unsecured public networks (e.g. public Wi-Fi) for accessing University systems without using appropriate encryption measures.

7.2 Unacceptable Use:

- A. Disable security settings or bypass controls on University-managed or personal devices used for University purposes.
- B. Share mobile devices or credentials used to access University data or services.
- C. Leave devices unattended and unlocked in public or shared environments.
- D. Copy or synchronise sensitive University data to third-party apps or services that are not approved for use.

Remote working and mobile access must comply with the University's data protection obligations, information security policies, and any additional guidance issued by Library and Information Services or the Information Security Team and / or Corporate Governance.

While Staff may have access to work outside University core business hours, this is not an expectation of the University and any work undertaken outside of their core working hours should be discussed and agreed by their line manager.

8. Use of Artificial Intelligence

8.1 Acceptable Use:

Use of AI tools is permitted only when such use supports legitimate academic, research, or administrative purposes and is consistent with University policies and applicable laws (including UK GDPR). AI tools that process or generate content must be used in accordance with copyright and intellectual property laws and be approved by the University.

8.2 Unacceptable Use:

- A. Users must not upload confidential, sensitive, or personal data (e.g. student records, medical data, research data, passwords) to public AI tools (e.g. ChatGPT, Gemini, Copilot) without explicit approval and proper safeguards.
- B. AI tools must not be used to:
 - I. Plagiarise or falsify academic work.
 - II. Mislead or impersonate others (e.g. fake emails, AI voice cloning).
 - III. Generate or spread offensive, discriminatory, or deceptive content.
 - IV. Attempt to exploit security vulnerabilities.
 - V. Automate decision-making that impacts individuals without proper human oversight (UK GDPR Article 22).

9. Violations

Violations of this policy may result in disciplinary action, removal of access rights, or referral to legal authorities, as appropriate. Suspected misuse or information security incidents must be reported immediately to the University's **IT Service Desk** and / or **Information Security Team**.

10. Monitoring and Privacy

To maintain the security, integrity, and proper functioning of its information systems, the University reserves the right to monitor the use of its digital services and infrastructure. This includes activity on University networks, devices, email systems, storage platforms and other IT services.

10.1 Monitoring is conducted to:

- A. Protect University systems from misuse, data breaches, and cybersecurity threats.
- B. Ensure compliance with University policies, legal obligations, and information security standards.
- C. Investigate suspected breaches of policy, misconduct, or unlawful activity.
- D. Maintain operational performance and audit trails for accountability and service reliability.

10.2 Key principles:

- A. Monitoring is proportionate, lawful, and necessary.
- B. Data is only accessed by authorised personnel and handled in line with the University's Data Protection Policy and UK GDPR.

- C. Monitoring may include automated logging, traffic analysis, access auditing, and forensic investigation where justified.
- D. Personal privacy will be respected as far as possible; private use of IT systems is permitted within reasonable limits but not exempt from oversight.
- E. Users are responsible for all activity conducted under their accounts or using University provided or approved systems.

By using University IT systems, users give implicit consent to appropriate and lawful monitoring as outlined in this policy and related procedures.

11. Policy Enforcement

Compliance with this Acceptable Use Policy is mandatory for all users of University information systems, services, and data. Breaches of this policy—whether accidental, negligent, or intentional—will be taken seriously and may lead to disciplinary action and/or legal consequences.

12. Related Policies and References

This Acceptable Use Policy (AUP) supports the University's commitment to maintaining a secure, compliant, and responsible digital environment. Users should refer to the following related internal policies for further detail:

- A. Information Security Policy
- B. Disciplinary Policy

13. Policy Review

This Acceptable Use Policy is a controlled document and is subject to regular review to ensure continued relevance, legal compliance, and alignment with the University's operational needs and information security requirements.

Appendix A: Examples of Unacceptable Use of University

IT Facilities

The University reserves the right to block, restrict, investigate, or take disciplinary action in response to any use of its IT facilities that it deems unacceptable, inappropriate, or in breach of policy. The following examples, while not exhaustive, illustrate behaviours that are considered unacceptable.

1. Illegal or Unlawful Activity

Unacceptable use includes ***but is not restricted to*** any activity that contravenes UK law, such as the Computer Misuse Act 1990 or other applicable legislation:

- A. Gaining unauthorised access to systems, data, or user accounts (e.g. using someone else's login credentials).
- B. Modifying, deleting, copying, or accessing data without proper authorisation.
- C. Impersonating others using email, messaging, or online platforms.
- D. Publishing or distributing content that is threatening, defamatory, harassing, discriminatory, abusive, obscene, or otherwise unlawful.
- E. Engaging in activity that violates University policies or brings the institution into disrepute.
- F. Conducting unauthorised commercial activity or personal business using University IT resources.
- G. Entering into contracts on behalf of the University without appropriate authority.
- H. Using IT resources for work or services that directly compete with the University.
- I. Using systems in a way that disrupts operations, resources or denies access to others.
- J. Promoting, supporting, or encouraging acts of terrorism or extremism, including content that incites violence or intolerance.
- K. Unlawful discrimination or the promotion of discriminatory content.
- L. Breaching the University's Data Protection Policy or disclosing restricted or confidential information without authorisation.

2. Indecent or Offensive Content

The creation, access, storage, transmission, or hosting of material that may be considered offensive or inappropriate is prohibited.

- A. This includes obscene, pornographic, or otherwise indecent content.
- B. Linking to external sites that host such material is not allowed unless explicitly authorised for academic or research purposes by the Head of Department and relevant Ethics Committee, with notification to Information Services.

3. Unauthorised Access

- A. Access to systems and data must be explicitly granted and used only as intended.
- B. Attempting to access systems or resources without appropriate permissions.
- C. Encouraging or enabling others to gain unauthorised access.
- D. Connecting personal and / or unauthorised equipment (e.g. wireless access points, servers) to the University of Portsmouth networks without prior written approval from Information Services.
- E. Registering domain names that imply affiliation with the University without permission.

- F. Sharing restricted data via public platforms (e.g. forums, social media, emails) without proper authority.
- G. Using University IT facilities for external work or consultancy without explicit approval from the relevant Head of Department.

4. Copyright and Intellectual Property (IP) Infringement

Users must always respect copyright and IP laws.

- A. Do not install, copy, share, or distribute software, media, or content (including music, videos, games, or documents) without proper licensing or permission.
- B. Treat all internal information as confidential unless clearly marked for public dissemination.
- C. Refer to the University's Copyright Policy for further guidance.

5. Security Violations

The integrity, confidentiality, and availability of University IT systems must be maintained.

- A. Attempting to bypass or disable security controls, such as firewalls or anti-virus software.
- B. Modifying software, hardware configurations, or system settings without authorisation.
- C. Causing physical damage to IT equipment or tampering with installations.
- D. Using tools or software designed to monitor, disrupt, or damage IT infrastructure (e.g. keyloggers, malware, penetration testing tools without authorisation).

6. Disruption and Misuse

University IT facilities must be used responsibly and not to disrupt others.

- A. Causing intentional disruption or degradation of service to other users or institutions.
- B. Harassing, bullying, or intimidating individuals through any digital platform or communication method.
- C. Creating, displaying, or distributing content designed to distress or offend others.

7. Misuse of Email and Messaging Services

Email and electronic messaging should be used in a professional, respectful, and accountable manner.

- A. Sending anonymous, misleading messages, or using false identities.
- B. Sending spam, chain letters, hoaxes, or any unauthorised promotional content.
- C. Sharing sensitive information via email or other messaging platforms without proper safeguards or permissions.

8. Social Media Misconduct

Use of social media must reflect the values and expectations of the University community.

- A. Misrepresenting your affiliation with the University.
- B. Sharing confidential or sensitive University information on public platforms.
- C. Posting discriminatory, offensive, or harassing content linked to your role at the University.
- D. Engaging in activity that may damage the University's reputation.

Note: Breaches of this policy may result in suspension of access, disciplinary proceedings and/or referral to external authorities. Users are expected to exercise good judgment and seek clarification if unsure about acceptable use.