City of Portsmouth College

IT Acceptable Use Policy (Students and Staff)

Document Control:

Version	V2
Document Created Date:	February 2023
Document Last Approval:	April 2023
Document Update History:	
Document Next Review:	2026
Document Approval Authority:	Trade Unions Senior Management Team (SMT)
Document Owner:	Director of IT

1. Purpose

The College recognises the opportunities that technology brings to teaching, learning, assessment and research, giving users the opportunities to create, collaborate and explore in a digital world, using multiple devices from multiple locations.

The College seeks to promote and facilitate the proper and extensive use of Information Technology (IT) for the sole purpose of supporting the teaching, learning, research and business activities of the College; and may be used for any legal activity that further the aims and policies of the College.

It is the responsibility of all Users of the College's IT services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

This Acceptable Use Policy is intended to provide a framework governing the use of all IT resources across all sites on which the College operates including any remote access to IT systems and services from outside of the college. It should be interpreted such that it has the widest application so as to include new and developing technologies and uses, which may not be explicitly referred to.

2. Scope

This policy applies to all Users including staff, students, visitors, contractors, partners, tenants and others, of the IT facilities provided by the College, are bound by the provisions of its policies in addition to this Acceptable Use Policy. It also addresses the use of the College's IT facilities accessed via resources not fully owned by the College, such as partner resources and the use of personal BYOD ('bring your own device') equipment.

The IT facilities include (but not limited to) hardware, software, data, storage, network access, telephony, printing, back office systems and services and service provided by third parties including online, Cloud and hosted services.

3. Policy

This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy (available from http://www.ja.net/documents/publications/policy/aup.pdf), and the JANET Security Policy published by JANET (UK), the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement, and the Eduserv General Terms of Service.

4. Definitions of Unacceptable Use

The College network is defined as all computing, telecommunication, and networking facilities provided by the College, with reference to all computing devices, either personal or College owned, connected to systems and services supplied on-premises or remotely.

The conduct of all Users when using the College's IT facilities should always be in line with the institution's values, including the use of online and social networking platforms.

Unacceptable use includes:

a. The purchasing and / or use of any Hardware / Software or Cloud services that has not been approved by the IT Department and recorded in the College IT service Catalogue. All

requests for additional software, hardware or services should be approved by the Change Advisory Board.

b. Only members of the IT team are authorised to add, remove, or move any IT equipment within the college. This includes, but is not limited to, desktops, Phones, docking stations, PDQ Machines, Printers, Networking equipment and monitors. It is expected that laptops will be moved but must not be connected to the wired network without express permission from the IT department.

c. Only College owned equipment may be connected to the college ethernet network. Only IT members of staff are allowed to connect devices to the ethernet network.

d. No external storage devices are to be used on college machines this includes USB memory sticks.

e. The sharing of passwords or accounts is prohibited.

f. Users are responsible for ensuring that any emails, links or web usage is safe and from trusted sources.

g. Users are responsible for maintaining data security and complying with the GDPR policy.

h. Creation or transmission, or causing the 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.

i. Creation or transmission of material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the College or a third party or which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation.

j. Creation or transmission of material with the intent to defraud or which is likely to deceive a third party or which advocates or promotes any unlawful act.

k. College data must not be stored on any device or service that is not a college system. It is permissible to send emails with data attachments where required for college business only.

l. Creating, coping or transmitting unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.

m. Unsolicited or bulk email (spam), forge addresses, or use mailing lists other than for legitimate purposes related to College's activities.

n. Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.

o. Material that brings the College into disrepute.

p. Deliberate unauthorised access to networked facilities or services or attempts to circumvent College security systems.

q. Pursuance of commercial activities for personal gain.

r. Failure to undertake any mandatory IT training including but not limited to Phishing training following a phishing simulation attack. Cyber Security training.

s. Deliberate activities having, with reasonable likelihood, any of the following characteristics:
   i. Wasting staff effort or time unnecessarily on IT management.
   ii. Corrupting or destroying other users' data.
   iii. Violating the privacy of other users.
   iv. Disrupting the work of other users.
   v. Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
   vi. Continuing to use an item of networking software or hardware after a request that use should cease because it is causing disruption to the correct functioning of the network.
   vii. Other misuse of network resources, such as the introduction of computer viruses, malware, or other harmful software.
   viii. Any breach of industry good practice that is likely to damage the reputation of the JANET network will also be regarded as unacceptable use of the College Network.
   ix. Introduce data-interception, password-detecting or similar software or devices to the College's Network.
   x. Any deliberate activity that could result in damage to systems or data (including data loss) whether deliberate or not

5. Monitoring

The College records and monitors the use of its IT facilities, under the Regulation of Investigatory Powers Act (2000) for the purposes of:

a. The effective and efficient planning and operation of the IT facilities.
b. Investigation, detection and prevention of infringement of the law, this policy or other College policies.
c. Investigation of alleged misconduct by staff or students.
d. The College will comply with lawful requests for information from government and law enforcement agencies.
e. Users must not attempt to monitor the use of the IT facilities without explicit authority to do so.
f. Access to an individual's IT usage information will not normally be given to another member of staff unless authorised by the Director of IT, or nominee, who will use their discretion, normally in consultation with the Director of People Strategy and Organisational Development, Line Manager or member of the ELT depending on the nature of the request.
g. Where there is a requirement to access the account of another member of staff, authorisation must be obtained in writing from the Director of People Strategy and Organisational Development or staff member's line manager in agreement with the Director of IT
h. If the request for access is related to an investigation under the Disciplinary Policy, this should be managed wholly through the People Partner who will work with IT if approved by the Director of People Strategy and Organisational Development or their nominee.
i. The college may monitor the use of IT facilities and services for the purposes of Safeguarding, Security, Prevention of radicalisation and any other such purpose as determined by the college.

j. The college may conduct activities to test the security of systems and staff responses this may include Penetration Testing, Phishing attack simulation and other security tests.

6. Consequences of Breach

In the event of any failure to comply with the conditions of this Acceptable Use Policy by a User, the College may in its sole discretion:

Restrict or terminate a user's right to use the College IT facilities.

Withdraw or remove any material uploaded by that User in contravention of this Policy.

Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the College's Disciplinary Policy.

7. Deviations from Policy

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall be reported to the Director of IT.

8. Other notes

The use of College IT systems and resources are subject to the following statutes and regulations:

- The Copyright, Designs and Patents Act 1988
- Computer, Copyright Software Amendment Act 1985
- The Computer Misuse Act 1990
- The Data Protection Act 1998
- General Data Protection Regulation (GDPR) (EU) 2016/679
- The Electronic Communications Act 2000
- The Freedom of Information Act 2002
- The Regulation of Investigatory Powers Act 2000
- Trademarks Act 1994
- Criminal Justice and Public Order Act 1994