IT Acceptable Use Policy
Student and other
3rd party users

Author:	Steve Violaris Head of Technical Services	**Reviewer:**	Fidelma Washington Chief Operating Officer
Date of Review:	April 2025	**Next Review:**	April 2027
Approved:	May 2025	**Date:**	June 2025

Putting Students First

Chronology of updates

September 2022	Reviewed – No updates required.
December 2023	Links updated, section 7 updated to include reference to unauthorised network connection, Section 8 updated to include Safeguarding
April 2025	Policy adapted to new template, expanded scope to apply to all non-staff members and 3rd parties, job titles updated

Contents

1 Introduction

This policy outlines the standards and expectations for the use of the college's information technology resources, including computers, networks, and internet access, on both college owned and personally owned devices. Our goal is to ensure that these resources are used responsibly, ethically, and in compliance with all relevant laws and regulations.
As a member of the college community, you are expected to use the college's IT resources to support and enhance the educational mission of the institution. This includes activities related to teaching, learning, administration, and communication. The policy aims to protect the integrity, security, and availability of our IT resources, while also safeguarding the privacy and rights of all users.
By adhering to this policy, you help maintain a safe and productive environment for everyone at the college. Please read the following guidelines carefully and ensure that your use of IT resources aligns with these principles.

2 Policy Statement

This policy provides a framework for using IT resources (e.g. all computing, telecommunication, and networking facilities) provided by the college. It should be interpreted such that it has the widest application, in particular references to IT services should, where appropriate, be taken to include departmental or other system managers responsible for the provision of an IT service. This policy should be interpreted so as to encompass new and developing technologies and uses, which may not be explicitly referred to.
Members of the college and all other users of the college's facilities are bound by the provisions of these policies in addition to this Acceptable Use Policy. They are also bound by such other policies as are published by the college. Users should also be aware that the college will monitor their use of its computer systems, devices and digital communications.

3 Scope

This policy applies to all non-staff users using college IT facilities (hardware, software, data, network access, telephony, services provided by licensed third parties, online cloud services or using college IT credentials) including students and third party individuals who have been given access for specific purposes. The term college IT facilities refers to all IT facilities. It is the responsibility of all users of the college’s IT facilities to read, understand and comply with this policy and any additional policies related to their activities, including other relevant information security policies.

4 Legal and Regulatory Framework

This policy is guided by relevant laws, regulations, and standards, including the General Data Protection Regulation (GDPR UK).

The user must comply with all relevant legislation and legal precedent, including the provisions of the following specifically related Acts of Parliament, or any re-enactment thereof:

- Computer Misuse Act 1990
  http://www.legislation.gov.uk/ukpga/1990/18/contents
- Data Protection Act 1998 – was this superseded by the one mentioned above i.e. 2018 (in green), please check. I would move the references to the GDPR and DPA into this bullet pointed list and remove them from the above introductory sentence.

  http://www.legislation.gov.uk/ukpga/1998/29/contents
- Counter-Terrorism and Security Act 2015
  http://www.legislation.gov.uk/ukpga/2015/6/contents/enacted
- Obscene Publications Act 1959
  http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
- Copyright, Designs and Patents Act 1988
  http://www.legislation.gov.uk/ukpga/1988/48/contents
- Regulation of Investigatory Powers Act 2000
  http://www.legislation.gov.uk/ukpga/2000/23/contents
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
  http://www.legislation.gov.uk/uksi/2000/2699/contents/made
- Malicious Communications Act 1988
  http://www.legislation.gov.uk/ukpga/1988/27/contents
- Communications Act 2003
  http://www.legislation.gov.uk/ukpga/2003/21/contents

5 Acceptable use

IT resources are provided primarily for academic and operational purposes to support learning and teaching, research, enterprise and other work of the college. Limited network services may also be provided to contractors and guests.

Whilst the principles of academic freedom will be fully respected, facilities must only be used responsibly, in accordance with the law and must not bring the college into disrepute.

College IT facilities may be accessed via college owned devices or via personally owned devices. However, this policy is applicable, regardless of the ownership of the device used. Personally-

owned devices, whether owned by students or 3rd parties, must be maintained with up to date anti-virus software (where appropriate), system patches and kept secure. It is the responsibility of the owner to ensure that there is a licence for all software installed on privately owned equipment. If plugging in any device to the college's mains electricity supply, users must abide by the college's inspection/testing of portable electrical appliances (PAT) policy. Devices provided by the college must also be kept secure in a similar manner.

College IT equipment should not be moved unless under guidance of the IT Team. No devices should be connected to or disconnected from the college wired network by unauthorised parties. Personal devices may only be connected to the college network through the appropriate wireless network.

Use of the facilities for personal activities is permitted, provided that it does not infringe the law or college policies, does not interfere with others' work? However, this is a privilege that may be withdrawn by the college, at any point, if such use is not in accordance with this policy.

Using college owned or managed services for commercial work for outside bodies that is being undertaken on a personal basis, solely for personal gain and not through college channels, requires explicit permission from the Head of IT & Learning Services.

College email addresses and associated systems must be used for all official college business, in order to facilitate auditability and institutional record keeping.

When using the college's IT facilities, you remain subject to all relevant laws and policies, and, when accessing services from another legal jurisdiction (for example accessing college services while abroad on holiday), you must abide by all relevant local laws, as well as those applicable to the location of the service. Following the requirements of this policy, and other college policies and procedures applicable to your activities, should normally ensure that you comply with the law. If you have any concerns about whether planned actions might be regarded as unlawful, please contact the IT helpdesk for further advice.

You must not infringe copyright or break the terms of licenses for software or other material.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. In the event that there is a genuine academic need to carry out an activity which might be interpreted as being in breach of the law (e.g. the deliberate viewing or accessing of sites or media which are specifically designed to promote terrorism or which are directly linked to a proscribed terrorist organisation) the college must be made aware of your plans in advance and prior permission to access must be obtained from the Head of IT and Learning Services or the Head of Student Advocacy and Safeguarding

Further details of what constitutes acceptable and unacceptable use is provided in the subsequent sections of this policy.

6 Keeping your IT credentials secure

You must take all reasonable precautions to safeguard your username, password and any other IT credentials issued to you. Advice is available on the choice of passwords. You must not allow anyone else to use your IT credentials. No one has the authority to ask you for your password, and you must not disclose it to anyone, including the IT helpdesk.

You will be held responsible for all activities undertaken using your IT credentials including while accessing systems by remote connection. You should only use the access to college systems provided to you for the purpose which that access was granted.

You must not attempt to obtain or use anyone else's credentials. You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

Do not leave a workstation logged in and unattended. You are advised to lock computers if you intend to take a short break. This prevents other users from accessing your account.

7 Behaviour

The conduct of students and 3rd parties when using the college's IT facilities should always be in line with the college's values, including the use of online and social networking platforms. When using college IT facilities, you must not:

- cause needless offence, concern or annoyance to others including posting of inappropriate comments about students or members of staff (genuine scholarly criticism and debate is acceptable)
- use the IT facilities in a way that interferes with others' valid use of them
- undertake any illegal activity including the downloading and storing of copyright information, except under a relevant licence, or with permission from the copyright owner
- view, store or print pornographic images or video
- retain or propagate sites or media which are specifically designed to promote terrorism or which are directly linked to a proscribed terrorist organisation, except in the course of recognised research or teaching that is permitted under UK and international law
- send spam (unsolicited bulk email), forge addresses, or use college mailing lists other than for legitimate purposes related to college activities
- deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, storage or consumables
- undertake any activity which jeopardises the security, integrity, performance or reliability of electronic devices, computer equipment, software, data and other stored information. This includes undertaking any unauthorised penetration testing or vulnerability scanning or the monitoring or interception of network traffic, without permission and connecting unauthorised devices to the network.
- deliberately or recklessly introduce malware or viruses
- attempt to disrupt or circumvent IT security measures.

8 Monitoring

The Isle of Wight College records and monitors the use of its IT facilities, under the Regulation of Investigatory Powers Act (2000) for the purposes of: This Act needs to be included in the bullet point list in the regulatory section if not already there.

- The effective and efficient planning and operation of the IT facilities
- Investigation, detection and prevention of infringement of the law
- Safeguarding
- Investigation of alleged misconduct by staff, students or 3rd parties.

The Isle of Wight College will comply with lawful requests for information from government and law enforcement agencies.

The college uses proactive monitoring, including keyword detection, to supplement both its filtering and the normal supervision of its users. This is intended to safeguard all users of college systems and meet the duty of care outlined by Ofsted and the Prevent duty guidance. Users should be aware that their use of the internet and college systems will be monitored and that inappropriate use will be dealt with through the normal college disciplinary procedures.

The college reserves the right to inspect any and all files stored on computers in all areas of the network in order to assure compliance with policy. The college may also review internet activity and analyse usage patterns where there is cause to suspect inappropriate use. Auditors (internal or external) have the right to access any computer files and systems in the performance of their duties.

Access to workspaces, email, and/or individual IT usage information will not normally be given to another member of staff unless authorised by the Head of IT, or nominee, who will use their discretion, normally in consultation with Human Resources. Where possible and appropriate, the Principal and CEO or COO and Deputy CEO will be informed, and consulted, prior to action being taken.

9 Implementation and enforcement of this policy

You must comply with any reasonable written or verbal instructions issued with delegated authority in support of the implementation of this policy. If you feel that any such instructions are unreasonable or are not in support of this policy, you may refer your concerns using the relevant student procedures.

If you believe this policy has been infringed, you should report the matter to IT services at the earliest opportunity. Follow up action will be considered carefully. Genuinely accidental infringement will be treated with understanding but any deliberate or willfully negligent infringement of this policy is likely to result in disciplinary action being taken. Penalties may include withdrawal of services. Offending material will be removed.

Information about deliberate infringement or illegal activities may be passed to appropriate law enforcement agencies, and any other organisations whose requirements may have been breached.

If a personally or college owned device is used to access or share college owned information, then the college reserves the right to remotely wipe the device in the event that it becomes damaged, lost or the college becomes concerned that the security of the information has been compromised.

3rd parties found to be in breach of this policy may have their access revoked as well as the access for all of the organisation responsible for them. Where activities may have been in breach of the law, the relevant authorities will be informed.

The Isle of Wight College reserves the right to recover from you any costs incurred as a result of your infringement.

10 Training and Awareness

All students are directed to this policy in the student handbook, updates will be published on the college intranet and all students will be notified of updates.

3rd parties should be advised that their access is dependent on their acceptance of this policy.