PETROC

IT Security Policy

Contents

Policy Name: IT Security Policy	Policy No: P04005
Approved Date: May 2023	Review Date: May 2025
Approved by: College Leadership Team	EqIA Completed: Yes
Author: Head of IT	Monitoring & Evaluation: College Leadership Team

1. Introduction

Petroc promotes responsible and lawful use of IT and digital platforms to support teaching, learning, and engagement. Academic freedom is respected within the bounds of this responsibility

1.1 This IT Security Policy is intended to provide a framework for such use of Petroc's IT resources and will be, in conjunction with Petroc's Information Security Management Stance, aligned to ISO27001. It applies to all computing, telecommunication, and networking facilities provided at all Campuses and mobile facilities. As such, it should be understood 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.

1.2 This policy is to be considered in parallel to the "Acceptable Use policy" published by JANET network operated by Jisc Services to which all users of the services provided by JANET must comply. In addition to this, when users are connected and using the 'Eduroam' service they must comply with the requirements set out in the Eduroam Policy.

1.3 National and International Law apply to activities carried out using computers and networks just as they do in any other sphere of life. The UK has a number of laws which apply particularly to computers. This policy is derived from and must be considered alongside these laws, in particular:

- the Computer Misuse Act (1990) creates offences of unauthorised access and unauthorised modification of computers and data
- the Regulation of Investigatory Powers Act (2000) controls the interception of traffic on networks. Interception for business purposes, for example the enforcement of acceptable use policies, is covered by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Other Statutory Instruments and Codes of Practice relating to these Acts and further information needed to support these areas may be found on the Home Office web page
- the Data Protection Act (2018) establishes requirements on anyone holding personal data on a computer or any other organised filing system
- the Anti-Terrorism, Crime and Security Act (2001) creates a code of practice for retention of communications data
- Under section 26 of the Counterterrorism and Security Act 2015 (the CTSA 2015) users must be aware that we have a duty in the exercise of our functions, to have "due regard to the need to prevent people from being drawn into terrorism (Prevent).

1.4 All European laws regarding computer misuse, electronic commerce, data protection, human rights and privacy etc. must also be adhered to.

2. Purpose of the Policy

2.1 Petroc's IT resources are provided primarily to facilitate a person's essential work as an employee or student or other role within the College. No use of any IT service should interfere with another person's duties or studies or any other person's use of IT systems, nor bring Petroc into disrepute, in any way.

2.3 Using Petroc's IT facilities, regardless of location accessed for non- work-related purposes, such as personal E-mail, shopping or recreational use including social networking sites is not considered an automatic or absolute entitlement or right. Whilst it is understood to enhance the overall experience of an employee or student priority access to such Petroc owned facilities will always be granted to those needing facilities for academic work or other essential College business. All users must act with caution and remain mindful of the risks internet use may pose to cyber security,

2.4 All users must correctly identify themselves at all times. A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources and the property of the college. In particular, passwords used must adhere to current password policy and practice. Advice on what constitutes a good password may be obtained from IT Services web pages. This advice must be followed: failure to do so may be regarded as a breach of this policy.

2.5 Personal Devices (Mobility)

2.5.1 Personal Device

Any Devices not managed by IT Services are defined as a Personal Device and users are required to follow some basic security requirements when connecting to the College Network:

1. Users must ensure that all the most recent operating system and application security related patches, fixes and updates have been installed on their personal devices prior to accessing the Petroc network.
2. Users are expected to install Antivirus software on all of their personal devices and to keep this up to date with the latest virus definitions.

2.5.2 Personal Use

Where a personal device is connected to the college network or where a college email or social media account is used; this shall be deemed to be college use not personal use and the IT security policy shall apply in full.

Use of Petroc email accounts should not, therefore, be used for registering on web sites that do not have a direct relevance or direct need to the business

e.g. (but not limited to) when buying for personal purposes from Amazon or EBay.

3. User Access Management

3.1 User accounts and access privileges shall be granted based on job responsibilities and documented business needs.

3.2 User account management shall follow the principles of least privilege, ensuring that users have access only to the resources necessary for their role.

3.3 User accounts must be protected with strong, unique passwords and enable multi-factor authentication where possible.

3.4 Multi-Factor Authentication (MFA), also known as Two-Factor Authentication (2FA), may require the use of an authenticator application installed on a mobile device. Reputable authenticator apps — such as those provided by Microsoft, Apple, or Google — are available free of charge from official app stores.Where a college-managed device is not provided for this purpose, it is a reasonable and secure expectation that personal mobile devices may be used to support MFA. Staff are reminded to maintain appropriate security controls on any personal device used for authentication, including the use of a strong passcode, regular software updates, and ensuring the device is not shared with others.

3.5 User accounts will be immediately revoked or disabled upon termination of employment or association with the college. Further details can be found in the Account Closure Policy.

4. Information Classification and Handling

4.1 All college information and data shall be classified based on its sensitivity and criticality.

4.2 Information owners shall be responsible for determining the appropriate classification, labelling, handling, and protection mechanisms for their respective data.

4.3 Access to sensitive and confidential information shall be restricted to authorised individuals with a legitimate need-to-know.

5. Network and System Security

5.1 Network devices, including firewalls and intrusion detection/prevention systems, shall be implemented to protect college networks from unauthorised access and malicious activities.

5.2 Operating systems, software applications, and network equipment shall be regularly patched and updated to address security vulnerabilities.

5.3 Critical and security patches must be applied to all supported devices and applications **within 14 days** of release.

5.4 Antivirus and anti-malware software must be installed and updated on all college-owned devices.

5.5 Wireless networks shall be secured with encryption, strong passwords, and access controls.

5.6 Remote access to college resources must be encrypted and authenticated through secure methods.

6. Privacy

6.1 It should be noted that systems staff, who have appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files and Web usage which may be stored on any computer which they manage. It is also occasionally necessary to intercept network traffic. In such circumstances appropriately privileged staff will take all reasonable steps to ensure the privacy of service users. Petroc fully reserves the right to monitor email, telephone and any other electronically mediated communications, whether stored or in transit, in line with its rights under the Regulation of Investigatory Powers Act (2000). Reasons for such monitoring may include the need to:

- ensure operational effectiveness of services
- prevent a breach of the law, this policy, or other Petroc's policy,
- investigate a suspected breach of the law, this policy, or other Petroc's policy
- monitor standards
- support the Government Prevent Strategy

6.2 Access to staff files, including electronic mail files, and/or individual IT usage information will not normally be given to another member of staff unless authorised by the Vice Principal or nominee, who will use their discretion, normally in consultation with the Head of People Services or other senior manager of Petroc. Where possible and appropriate, the Deputy Principal, Department Manager, or more senior line manager, will be informed and consulted prior to action being taken.

6.3 Petroc sees student privacy as desirable but not as an absolute right, hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff responsible for their academic work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the police or security services has been received, systems staff are also authorised to release the contents of a student's files, including electronic mail files, when required to by any member of staff who has a direct academic work-based reason for requiring such access.

6.4 The usage of Petroc's IT devices and the software installed on them, is automatically logged and monitored to ensure compliance with this policy and mitigate risks affecting the integrity of the network.

7. Leavers and closure of user accounts

7.1 After a student or member of staff leaves Petroc, files which are left behind on any computer system owned by, or managed on behalf of Petroc, including servers, and including electronic mail files, will be considered to be the property of Petroc.

7.2 When leaving Petroc, staff MUST make arrangements to transfer to colleagues any e-mail or other computer-based information held under their personal account, as this will be closed on their departure.

7.3 Student accounts will be disabled on leaving the college with accounts deleted within 180 days of end of their study programme, but not earlier than 30 days post end date, with access reviewed each academic year . Any funds held for print (considered resource fees) will also be closed and no refunds will be made.

8. Behaviour

8.1 No person shall jeopardise the integrity, performance or reliability of college systems, or those of our partners (including computer equipment, network, software, data and other stored information). The integrity of Petroc's computer systems is put at risk if users do not take adequate precautions against malicious software, such as computer viruses and associated malware.

8.2 Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene the Petroc College Code of Conduct. Staff Users of Petroc's computer systems must make themselves familiar with, and comply with the Staff Disciplinary policy and procedure ; student users must make themselves familiar with, and comply with the Learner Success Standards

8.3 No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.

8.4 Users of services external to Petroc's are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this IT Security Policy and be dealt with accordingly. This includes social networking sites, blog and wiki services, bookmarking services and any other externally hosted services. The use of Petroc's credentials to gain unauthorised access to the facilities of any other organisation is similarly prohibited.

8.5 Users shall refrain from engaging in activities that may disrupt or degrade network performance, compromise security, or violate any local or international laws.

8.6 The use of unauthorised software, unauthorised network devices, or circumvention of security controls is strictly prohibited.

8.7 Unacceptable use of Petroc's IT Resources may be summarised as:

- the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law; propagation will normally be considered to be a much more serious offence
- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights
- causing annoyance, inconvenience or needless anxiety to others, as specified in the Jisc (JANET) Acceptable Use Policy
- defamation (genuine scholarly criticism is permitted)
- unsolicited advertising, often referred to as "spamming"
- Impersonation; sending emails that purport to come from an individual other than the person actually sending the message using, e.g. a forged address
- attempts to break into or damage computer systems or data held thereon
- actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software
- attempts to access systems for which the individual is not authorised
-
- unauthorised resale of Petroc or Jisc services or information.
- excessive IT use during working hours that significantly interferes with a staff member's work, or that of other staff or students

8.8 These restrictions should be understood to mean that the following activities will normally be considered breaches of this policy. Any potential exceptions must be discussed and agreed with IT Services before the activity takes place. Examples include, but are not limited to:

- Downloading, uploading, distributing, or storing music, video, film, or other materials without a valid licence or other explicit permission from the copyright holder.
- Using peer-to-peer software or related applications to illegally download or share copyrighted material.
- Publishing unauthorised recordings (e.g., lectures) on external websites.
- Distributing or storing pirated software by any means.
- Connecting unauthorised devices to Petroc's network (i.e., devices not configured to comply with this policy or other

relevant regulations and guidelines, including those related to security, IT purchasing, and acceptable use). This includes network hubs, switches, and wireless access points not approved or managed by IT Services.
- Circumventing Network Access Control.
- Monitoring or intercepting network traffic without explicit permission.
- Probing or testing the security of systems (e.g., via port-scanning) without authorisation.
- Connecting devices to network access points, including wireless, without authorisation.
- Engaging in non-academic activities that generate heavy network traffic, interfere with others' legitimate use of IT services, or incur financial costs.
- Excessive use of resources (e.g., file storage) or actions that lead to a denial of service to others, including failure to respond to IT Services requests for remedial action (e.g., use of network stress-testing tools).
- Frivolous use of Petroc-owned computer laboratories, particularly where such activity interferes with others' legitimate use of IT facilities.
- Opening unsolicited email attachments, especially if not related to work or study.
- Deliberately viewing, accessing, or printing pornographic material.
- Forwarding or distributing electronic chain mail.
- Posting defamatory or inappropriate comments about staff or students on social media or networking sites.
- Creating or publishing web-based content that portrays official Petroc business without express authorisation or responsibility.
- Using Petroc business mailing lists for non-academic purposes.
- Using CDs, DVDs, USB drives, or other storage media to copy unlicensed software, music, or other copyrighted material.
- Copying website or other content without the express permission of the copyright holder.
- Committing plagiarism — the intentional use of another person's material without proper attribution.

8.9 It should be noted that individuals may be held responsible for the retention of attachment material that they have received, via e-mail that they have read. Similarly, opening an attachment, received via unsolicited e-mail, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in disciplinary action being taken. Disciplinary action may also be taken if casual or non-work-related activity results in significant problems being caused for I.T. systems or services, arising for example from browsing non-work-related websites or the downloading of software containing malicious content.

8.10 Acceptable uses may include:
- personal email and recreational use of Internet services, as long as

these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others
- advertising via electronic notice boards, intended for this purpose, or via other of Petroc's approved mechanisms

8.11 However, such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

9. Disciplinary

9.1 Staff who break this Acceptable Use Policy will find themselves subject to the Petroc staff Disciplinary Policy and procedures. The Director of People Services, as well as an individual's Senior Manager, may take such disciplinary action.

9.2 Students who break this Acceptable Use Policy will find themselves subject to the Petroc Learner Success Standards . The Director of Quality Improvement may take such disciplinary action.

9.3 Individuals may also be subject to criminal proceedings. Petroc reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

10. Incident Reporting and Response

10.1 All security incidents, including breaches, compromises, or suspected unauthorised activities, must be reported promptly to the IT department.

10.2 An incident response plan shall be established and regularly tested to ensure a timely and coordinated response to security incidents.

10.3 College employees and users shall cooperate fully with IT staff during investigations and provide accurate and timely information.

11. Training and Awareness

We are committed to maintaining a high level of cyber security awareness across all staff and students. Ongoing education and awareness are essential to reducing the risk of cyber threats and ensuring compliance with this policy and wider data protection obligations.

Mandatory Training

- All staff and students must complete **annual cyber security awareness training**.

- New staff and students must complete the training as part of their **induction process** before being granted full access to IT systems.

- Additional refresher training may be required following a security incident, policy change, or identification of increased cyber risk.

11. Monitoring and Review

11.1 The Vice Principal and the ICT Services Manager are responsible overall for the implementation of the Policy.

11.2 As a rule, the Policy will be reviewed every two years or after major incident or change in Cyber Essentials requirements. Petroc reserves the right to amend the policy at its discretion and in accordance with the relevant legal regulations/laws.

11.3 Annual self-assessment will be conducted against Cyber Essentials Controls.

11.4 The policy will be approved and monitored through CLT meetings.