



Policy Title	IT Security Policy
ID Number	P04001
Scope	All Users
Status	Policy
Reviewed By	Assistant Director of Facilities
Reviewed Date	January 2011
Last Reviewed	
Due for Review	January 2013
Impact Assessment Completed	Initial Assessment Completed

Policy Title: IT Security Policy

Policy Statement

To be issued to all users of the Petroc's IT Systems. To be highlighted at both staff and student induction. Acceptance of this policy is acknowledged on all enrolment forms and contracts of employment that are signed as part of any engagement with Petroc. This policy to be freely accessible at identified locations including the learning centres.

Users will be reminded each time they log into any of the colleges systems of their obligations to this policy by means of a pop up with a brief text relating to this policy.

This policy is to be considered in parallel to the [Joint Academic Network \(JANET\) "Acceptable Use Policy"](#) to which all users of the services provided by JANET must comply.

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. A draft [Amending Bill](#) has been published to extend the Act to cover denial of service attacks.
- 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 \(1998\)](#) 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.

There are also [European laws](#) regarding computer misuse, electronic commerce, data protection, human rights and privacy etc.

Electronic Communications

- Petroc maintains Internet access, a voiceMail system, a telephone system, Video Conferencing System, electronic-mail (eMail) system and supports other developing services to assist in the conduct of business within Petroc. These systems, including the equipment and the data stored in them, are and remain at all times, the property of Petroc. As such, all content generated, messages created, sent, received or stored in the system are and remain, the property of the College as laid out in Petrocs Email Policy and can be found under Petrocs Policy section online.
- VoiceMail , eMail and instant messaging should not be used for the conduct of personal business as laid out in the email policy.
- Petroc reserves the right to retrieve and review any message or Internet derived content composed, sent, or received. Please note that even when a message or Internet derived content is deleted or erased, it is still possible to recreate it; therefore, ultimate privacy of communications is not ensured to anyone. While voicemail and eMail may accommodate the use of passwords for security, confidentiality cannot be guaranteed. Messages and Internet content may be reviewed by someone other than the intended recipient.
- Whilst passwords must not normally be revealed to anyone, they may be made known to a College authority if required.

There is a password policy in force and can be found under Petrocs Policy section online.

- Internet content and communications may not contain content that may reasonably be considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments, or images, racial slurs, gender-specific comments, or any comments that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability. This is in support of Petrocs communications policies.
- The following disclaimer must be included with all eMail communications from Petroc.

The following disclaimer will be added to each outgoing email:

DISCLAIMER - Any opinions expressed in this communication are those of the individual and not necessarily Petroc. This communication and any files transmitted with it, including replies and forwarded copies (which may contain alterations) subsequently transmitted from the College are solely for the use of the intended recipient. It may contain material protected by attorney-client privilege. If you are not the intended recipient or the person responsible for delivering to the intended recipient, be advised that you have received this communication in error and that any use is strictly prohibited. If you have received this communication in error please notify the College by telephone on +44 (0)1271 345291 or via eMail to postbox@petroc.ac.uk, including a copy of this message. Please then destroy this eMail and any copies of it.

User Agreement (Acceptable Use) –

To be acknowledged on all enrolment forms/learning contracts, employment contracts and included in the Student Handbook, Staff Handbook and emphasised in Student and Staff Induction Programmes. At least the following statement

must be included in the standard document provided to each user of the Petroc IT systems.

- Access to services which present material, which might offend the public sense of decency, is considered an inappropriate use of this college's resources. Users are warned that such access is seen as a disciplinary offence.
- No communication is to be created or sent which may constitute intimidating, hostile or offensive material on the basis of race, colour, creed, religion, national origin, age, sex, marital status, lawful alien status, non job related physical or mental disability, veteran status, sexual orientation or other basis prohibited by law. This college's policy against sexual or other harassment applies fully to all communications, including same sex harassment.
- If you use the system in ways that are judged excessive, wasteful, or unauthorised, you may be subject to loss of access and appropriate disciplinary procedures.
- Employees learning of any misuse of the Internet, voice-mail, eMail or instant messaging systems or violations of this policy shall notify the *Principal* immediately.
- All users must acknowledge acceptance of these guidelines before their account is activated.
- Petroc's policies regarding Employee Standards of Conduct, Conflict of Interest, Equal Opportunity and Data Protection also apply to electronic messages, telephone messages including voice-mail, and other internal and external electronic communications, including, but not limited to, computer Bulletin Boards, Newsgroups, the Intranet, Internet and instant messaging.
- Transmitted communications are to be created, handled, distributed, and stored with the same care as any other business document. This includes complying with information-access rules, accessing information only for legitimate business purposes, and protecting information from access by unauthorised persons.
- Users must be aware that these systems, and the information stored within them, are the property of Petroc and are to be used only for Petroc-approved activities. Petroc maintains the right to monitor the operation of these systems, while respecting privacy, either in response to information about a specific threat, or generally because of a perceived situation
- Users are advised that Petroc may have a legal obligation to both obtain evidence and pass on information derived from the college's computer systems, as necessary in order to assist an investigation by a law enforcement agency
- Users of Petroc's computer systems must appreciate that confidentiality cannot be assured when transmitting information.
- Users must acknowledge that in order for Petroc's computer systems to be maintained and supported effectively, Systems Administrators will have access to individual user's directories, folders and files. Such access is regulated by the [Petroc's Systems Administrator's Charter](#). A hard copy of this charter is available for users to view online.
- The Petroc's prohibition of derogatory and offensive comments also applies to messages communicated through these systems. Special care should be given to ensure that the style and tone of messages are appropriate.

- Every effort should be made to send messages only to those who "need to know."
- Employees are responsible for using these systems appropriately. Inappropriate use could result in disciplinary action.
- Unauthorised access to, copying, alteration or interference with computers and computer programs or data is prohibited. Users must not make or use unauthorised copies of copyrighted software. (see footnote: software piracy)
- The use of one user's computer system account by another user is expressly forbidden!
- Misuse of this college's computer systems by a user which results in cost to this college will result in those costs being charged to the user. Such costs will be a minimum of £25.00 and have no upper limit.
- Users must never divulge any personal or college security information by email irrespective of who requests it.
- Users who are responsible for other staff, line managers for example, must never request personal security information of their staff by email.
- Users responding to web sites that request usernames and passwords must check carefully that the URL (address) is that of the web site they believe it to be.
- Users must only respond to trusted web sites with personal security information where the URL (address) is prefixed **https://** to ensure a secure transaction.

Abbreviated statement

The following is an abbreviated version of Petroc's IT Security Policy for issue to all student users:

Your Responsibilities when using Petroc's IT Systems:

Petroc has invested a considerable amount of money in the IT facilities available to students. Responsibility accompanies access to these facilities. On the enrolment form that you signed, you agreed to a number of responsibilities including: "I agree to take personal responsibility for computer security and use as set out in Petroc's IT Security Policy". Some of the key points of this policy are listed below:

- Petroc's computer systems are to be used only for college-approved activities.
- Users may not interfere with college computer systems in any way
- Passwords must not be disclosed to anyone other than a college authority
- The use of one user's computer system account by another user is expressly forbidden!
- All student user data will be removed from Petroc's computer system at the end of the academic year, unless a request in writing is made to IT Services.
- Access to services which present material which might offend the public sense of decency is considered an inappropriate use of this Petroc's resources.
- No communication is to be created or sent which may constitute intimidating, hostile or offensive material on the basis of race, colour,

creed, religion, national origin, age, sex, marital status, lawful alien status, non job related physical or mental disability, veteran status, sexual orientation or other basis prohibited by law.

- This college's policy against sexual or other harassment applies fully to electronic mail and instant messaging including same sex harassment.
- Misuse of this Petroc's computer systems by a user which results in cost to this college will result in those costs being charged to the user. Such costs will be a minimum of £25.00 and have no upper limit
- Monitoring of Petroc's systems will be carried out, therefore privacy and confidentiality is not guaranteed.
- Users are warned that a breach of this policy is a disciplinary offence.
- Unauthorised access to, copying, alteration or interference with computer programs or data is prohibited. Users must not make or use unauthorised copies of copyrighted software. (see footnote: software piracy)
- Petroc's IT Security Policy can be viewed on-line at:

<https://oncampus.ndevon.ac.uk/misc/SecurityPol.htm>

Software piracy

Software Piracy is the act of using illegally copied software without the permission of the copyright owners and contrary to their licensing arrangements.

Petroc's policy with regard to software is as follows:

- Only software which has been purchased or licensed in some other way by the college, albeit through Petroc's department's normal purchasing arrangements on behalf of the Petroc, may be installed and used on Petroc's equipment.
- Only software which meets the above criteria and which has been procured with a multi-user licence may be installed on Petroc's networks, multi-terminal mini computers or copied to be used by more than one user simultaneously.
- User's own software may not be loaded on to any of the college systems.
- Petroc's software may not be copied or moved from Petroc's computer media by any means, in any form other than for the purposes of security backups unless the college is licensed by the software licensor to permit such action. Users must obtain the permission of IT Services before making copies or moving software from Petroc's media. (In the case of security backups it is prudent to store backup media in a different location to the original i.e. another college room or building).