PETROC™

European Union
European Social Fund
Investing in jobs and skills

IT and Mobile Devices Security Policy

1. Introduction

1.1 It is the responsibility of all Petroc IT system users to ensure they are familiar with the IT Security Policy. Student's must be made aware of the IT Security Policy at induction. Acceptance of this policy is acknowledged on all enrolment forms and is implicit within contracts of employment that are signed as part of any engagement with Petroc. The policy will be freely accessible at identified locations including the learning centres and is available online to staff.

1.2 Users will be reminded each time they log into any of the colleges systems of their obligations to this policy and will be reminded on screen to re-enforce this policy. This extends to the college wireless provision but not to mobiles and tablets that are not connected to the colleges system.

1.3 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.

1.4 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 unathorised 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 (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 which must be adhered.

2. Purpose of the Policy

2.1 The purpose of the Policy is to ensure that all users are aware of their responsibilities and compliance when using any aspect of the college IT System (this includes hardware, software, email and Apps etc). This extends to all user devices including Laptops, Tablets and mobile phones.

2.2 The policy aims to ensure that staff and students remain complaint with IT rules and regulations. That all necessary precautions are taken to ensure the security of staff/student data is not compromised.

3. General Principles/Procedures

3.1 Usage

3.1.1 Petroc maintains Services to the business such as Internet access, a voiceMail system, a telephone system (including Mobiles), 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. This extends to cloud services and that users are reminded that the content placed on them are still under the control of the college. As such, all content generated, messages created, sent, received or stored in the system , including Photos and videos, are and remain, the property of the college.

3.1.2 VoiceMail, eMail and instant messaging should not be used for the conduct of personal business as laid out in the email section below. This extends to the use of tablets and mobiles phone when used with Instant messaging, social media applications and photo and video software.

3.1.3 Petroc reserves the right to retrieve and review any message or Internet derived content composed, sent, or received. It should be noted 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 guaranteed to anyone.

While voicemail and eMail may accommodate the use of passwords for security confidentiality cannot be assured. Messages, Internet and any content on college devices may be reviewed by someone other than the intended recipient.

3.1.4 Whilst passwords must not normally be revealed to anyone, they may be made known to a College authority if required but will never be asked for via email or other non verbal method. Detailed information regarding passwords can be found below.

3.1.5 Internet content and communications may not contain content that may reasonably be considered offensive or disruptive to any employee or learner. 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 not only in accordance with legal requirements but also the philosophy of the college.

3.1.6 Excessive usage will be monitored on all services that are offered to users this extends to Mobile Phones as well as the general storage and bandwidth.

3.1.7 Damage to college assets accidentally or otherwise including laptops , tablets and or Mobile Phones will be reported to the Director of Resources immediately.

3.1.8 Use of college devices outside of normal operating practices is forbidden, this includes the use of mobiles, laptops and tablets. Devices should only be used whilst it is safe to do so (i.e not whilst driving) and should be used solely for the purpose of work.

3.1.9 All loses or damage are to be reported to IT Services immediately who will assess the costs and report directly to the Director of Resources.

3.1.10 IT Services will maintain an overall contract for use of IT and that no member of staff should make any formal contract without consulting IT Services first for anything IT related including mobile phone contracts.

3.1.11 Petroc has a standard disclaimer which must be included with all eMail communications (Disclaimer can be found in Appendix 1).

3.2 Email Usage/Storage (see appendix 2)

3.2.1 This section relates to the use of Petroc's email Services, for the purpose of sending or receiving email messages and attachments as part of delivering the aims and objectives of the college. This includes the use of any IT facilities, including hardware, software and networks, provided by Petroc in order to meet these aims and objectives.

3.2.2 The scope of this policy does not extend to the language and usage of email and or social media as a method of communication which is part of a wider communications and social media strategy. Users are asked to refer to the Social Media and Networking Policy for specific details regarding social media protocol.

3.2.3 Petroc has agreed that the maximum size limit for all users' email boxes aggregated together will be 400MB. This enables Petroc to maintain, monitor and ensure that there is no excessive burden on college resources – more storage space = more cost. In order to maintain this IT Services will ensure that:

- users will receive alerts when their total e-mail box size reaches 85% (348Mb) and 95% (389Mb) of the upper limits
- once the upper limit is breached all further incoming email will be returned to sender accompanied by the message "Your email could not be received by your intended recipient due to email box limitations" As soon as the mailbox is reduced within its size limits the bar is lifted. All returned e-mails will need to be re-sent if they are still relevant

3.2.4 Users are advised not to store excessive and unwanted emails within Outlook. This includes emails with attachments. These type of emails impact particularly on the email storage system and as a consequence further support services such as backup and recovery are also affected.

3.2.5 Users are advised to proactively delete or archive on a regular basis in order to keep the email systems working effectively and to work within the norms laid out above.

3.2.6 The email system is for Petroc business use only. The College has, in the past, allowed reasonable use of email for personal use if certain guidelines were adhered to. However, there are significant issues surround legal aspects of liability when using college emails for personal use. With this in mind the college will not support the use of college emails for personal use in the future.

3.2.7 Personal use is defined as email that does not have a direct relevance or need to the business. This includes the use of College email for registration to shopping sites, social networking sites and other sites that require an email for registration outside of business use.

3.2.8 If however, you need to buy online for Petroc as part of your work then please register with IT Services that you are doing so.

3.2.9 Petroc reserve the right to block any emails which are not related to the business of the college or are deemed a security risk in order to protect our systems for the majority of our users.

3.2.10 Petroc cannot support any issue relating to the use of email for personal use and will perform actions necessary to secure the college systems from malicious actions if deemed necessary. This may include the blocking of incoming email from certain destinations. Petroc will not accept liability for use of email accounts for anything other than business use.

3.2.11 IT Services continue to provide a secure filtered system which reduces the number of malicious emails arriving on our systems from outside of the college. These emails contain a variety of malicious attachments such as viruses, Malware and other known or unknown security attachments. The amount of emails arriving at the college email system continues to grow and IT Services will continue to proactively provide this service in order to protect the business from any denial of service or malicious activity and ensure the promotion of good Business Continuity.

3.2.12 Any email containing confidential information should be avoided. However, if the user must send the data by email then it is recommended that the information is secured by including it in a Microsoft Word or Excel file and protecting it with a password. Then provide the recipient with the password by means of other communication, for instance by telephone, in each case the user must adhere to strict Data Protection rules and policies and is advised to consult the colleges Data Protection officer.

3.2.13 Users must have no expectation of privacy in anything they create, store or receive on the College's computer system as it will be deemed for business purposes. Emails can be monitored without prior notification if Petroc deems this necessary or is directed by any government agency as part of an investigation. If there is evidence that a user is not adhering to the guidelines or laws set out in this policy, Petroc reserves the right to take disciplinary action, including termination and/or legal action.

3.3 User Agreement (Acceptable Use)

3.3.1 The *User Agreement* should 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. The following procedures/guidelines must be highlighted to all staff and students when using Petroc's IT systems:

- access to services which present material which might offend the public sense of decency, is considered an inappropriate use of college resources. Users are warned that such access is seen as a disciplinary offence and systems are in place to monitor any such activity

- 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. The 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, or put the college in a position if risk, 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 are obliged to notify IT Services 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,Mobile Phone use, 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 IT 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 either on the colleges network or via mobile communications where they are owned by the college
- users must acknowledge that in order for Petroc's IT 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 Petroc's Systems Administrator's Charter. A hard copy of this charter is available for users to view online. IT Services will always ask for permission to access a users directory and files or get approval from a senior manager

- Petroc's prohibition of derogatory and offensive comments also applies to messages communicated through these systems including mobile phone 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 IT 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
  An abbreviated version of the above can be found in Appendix 3 – it is suggested that this is issued to students prior to the use of college IT systems.

3.4 Software Piracy

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

3.4.2 Only software which has been purchased or licensed in some other way by the college, albeit through Petrocs normal purchasing arrangements, may be installed and used on Petroc's equipment.

3.4.3 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.

3.4.4 User's own software may not be loaded on to any of the college systems, this includes tablets and mobile phones.

3.4.5 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).

3.5 Password Guidelines/Procedure (See Appendix 4)

3.5.1 Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of a College's entire corporate network. As such, all College employees (including contractors and vendors with access to College systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. Students are advised to follow similar guidelines to secure and take responsibility for their own IT security both at the College and at Home. All users are advised to be aware of social engineering (the manipulation of people into divulging confidential information for the purpose of fraud or system access) and not to reveal any details to anyone via electronic and/or verbal communications which would compromise the college systems.

3.5.2 The aim of this section of the policy is to provide a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change of passwords as identified in the Colleges Audit Reports. The policy is, of course, based on the best "good practice" in Information Technology today.

3.5.3 The Policy applies to anyone who has or is responsible for an account (or any form of access that supports or requires a password) on any system that resides at any College facility, has access to the College network, or stores any non-public College information.

3.5.4 All system-level passwords (e.g., root, domain admin, application administration accounts i.e. Financial, Student Records, etc.) must be changed at least every 30 days.

- all user-level passwords (e.g. email, web, desktop computer, etc) must be changed every 30 days
- user accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password that is different from all other accounts held by that user

- users will be allowed a password history of 3. This means an allowance will be made to record 3 passwords that have previously been used and could be used again. This will be done automatically by the system
- password complexity is required and this is to be achieved through a combination of a minimum of 8 characters, using both uppercase and lowercase and 1 number
- the password minimum age will be set at 5 days. This, with the password history, means that the user is unable to go back to an original password for 15 days
- accounts will be locked after 4 failed attempts to access an account
- passwords must not be inserted into email messages or other forms of electronic communication.

3.5.5 Passwords are used for various purposes at College. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Everyone should be aware of how to select strong passwords.

3.5.6 Do not use the same password for College accounts as for other non-College access (e.g., personal ISP account, Bank Accounts etc.). Where possible, don't use the same password for various College access needs. For example, select one password for the financial systems and a separate password for IT and security systems. Do not share passwords with anyone, including administrative assistants. All passwords are to be treated as sensitive, confidential Business information.

3.5.7 Users are asked to refer anyone requesting their password to IT Services or refer the individual to this Policy (which stresses that an individual's password should not be given out). Do not use the "Remember Password" feature on applications (e.g., Internet Explorer, Outlook, Firefox or Safari).

3.5.8 Users are advised not to write passwords down and store them anywhere in the office. Do not store passwords in a file on ANY computer system (including ~~Palm Pilots~~ smart phones or similar devices such as tablets) without encryption.

3.5.9 The recommended change interval for passwords is every 30 Days as indicated above. Users will be informed when this is due by a message on the screen when they log in. If an account or password is suspected to have been compromised, report the incident to IT Services and change all passwords, including personal ones.

4. Monitoring and Review

4.1 The Director for Resources and Head of IT are responsible overall for the implementation of the Policy.

4.2 As a general rule the Policy will be reviewed every two years. However, Petroc reserves the right to amend the policy at its discretion and in accordance with the relevant legal regulations/laws.

4.3 The policy will be approved and monitored through SMT meetings.

Appendix 1

Email Disclaimer

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.

This message has been scanned for malware by Websense. www.websense.com

Appendix 2

Using Email Procedure - Best Practice

DO…

- always use the font Verdana and font size 10
- have a standard signature with your name, job title, contact details etc (this can be set up in the main screen of Outlook and clicking on Tools – Options – Mail Format – Signature)

  (full instructions can be found in the Marketing area of On-Campus – Petroc Templates)

BARNSTAPLE	**TIVERTON**
Name Job Title School/Directorate **Petroc** North Devon Campus Old Sticklepath Hill, Barnstaple, Devon, EX31 2BQ T +44 (0)1271 XXXXX F +44 (0)1271 338121 www.petroc.ac.uk	**Name** Job Title School/Directorate **Petroc** Mid Devon Campus Bolham Road, Tiverton, Devon, EX16 6SH T +44 (0)1884 XXXXX F +44 (0)1884 235262 www.petroc.ac.uk

- remember the recipients of emails are people and therefore your emails should be polite and courteous
- always include a "subject" when sending an email (short and descriptive)
- use an appropriate greeting to start your email i.e. "Hi" (internal use only), "Dear" or "Good morning/afternoon".
- use the spell checker
- state clearly what action you expect the recipient to take
- only mark the email as important if it is
- only copy staff in to an email when they need to take action – and let them know the action that they should take
- only forward emails when you expect the recipient to take action – and let them know the action to take
- attempt to reply to emails in a timely manner and if you cannot act on a request due to time constraints, send them a holding email
- regularly carry out housekeeping on your In-box, Deleted Items and Sent Items to ensure the size of your IT account is kept to a minimum
- remember to always use the Out of Office assistant when you are not going to be available to respond to emails for a period of time.

DO NOTS…

- use symbols and characters such as smileys
- write emails in capitals as it is considered as "shouting" and aggressive
- copy people in to an email unnecessarily.
- use a wallpaper on your email template
- use your Petroc account to send personal emails
- forward chain letters, junk mail and jokes
- use unnecessary abbreviations, jargon and slang
- send information by email that could be communicated via a different method – i.e. face-to-face, In the Know etc.

Appendix 3

Abbreviated IT Security Policy for Student Use

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 including issued laptops and tablets 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 Petroc's resources and may result in disciplinary action.
- 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 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.petroc.ac.uk/information/218/home_page.htm

Appendix 4

General Password "Do's and Don'ts"

DOs	DON'Ts
Ensure password is at least 8 characters long	Do not use single words contained in any dictionary, slang, dialect or jargon
Ensure the password contains mixed case and special characters or punctuation	Do no use any part of an account identifier (user ID)
Ensure the password is significantly different from previous passwords	Do not include any personal details when constructing the password
Change your password regularly (at least once every 30 days)	Do not let anybody observe you entering your password
Change your password upon suspecting it has been compromised	Do not display your password in your work area or any other visible place
Use several unrelated short words or take the first letter from a phrase	Do not reuse old passwords or words spelt backwards
Use a password with non-alphabetical characters e.g. digits or punctuation	Do not use simple passwords that can be easily guessed or easy to remember
Use a password that you can type quickly, without having to look at the keyboard	Do not use the same password on multiple accounts i.e. use a different password on each application you use
Deliberately misspell words	Do not e-mail, record electronically or write down your password
	Do not use a password of all digits, or the same letter
	Do not disclose passwords

Further advice may be sought from:
- IT Services
- Human Resources Department