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

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 necess4dieiis ade ofpnts to T016o urityt stafie

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

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. 5.00665(a)2.9n2crrap 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.

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

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.

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

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 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)