Internet, Social Media and Email Policy

Revision: 1.0
Issued: 27th July 2021

TABLE OF CONTENTS

1. REVISION HISTORY AND APPROVAL

Revision	Nature of change	Approval	Date
1.0	First Issue	JL	27/07/21

2. USE OF SOCIAL NETWORKING SITES AND THE INTERNET

2.1. Use of the internet is now an accepted part of education and study, therefore, some safeguards and policies must be in place to clearly describe the expections, limitations and boundaries inherent in the use of this technology resource.

2.2. Learners: learners must comply with appropriate use of internet resources as per service provider and legal requirements this extends to the appropriate use of the PCI College Portal and related platforms. Inappropriate, offensive or similar material must not be posted to college platforms.

2.3. Staff and Associate lecturers: must only use internet resources provided by PCI College for the purpose of the work of PCI College and not for personal or other purposes. Inappropriate, offensive or similar material must not be posted to college platforms.

2.4. Failure to comply with this policy may result in progression and/or employment sanctions.

2.5. As Social Media has become a major aspect of modern living and whilst PCI College understands the use of social media platforms e.g. WhatsApp, Facebook etc. for private/personal/professional use, it is imperative that all stakeholders understand that confidentiality policies extend onto these platforms whilst associate with PCI College.

2.6. All stakeholders using social media platforms must carefully consider the implications for confidentiality before posting materials which may in fact breach confidentiality.

3. EMAIL

3.1. PCI College provide a secure email address with Multi Factor Authentication to all staff, Associate Lecturers and learners.

3.2. PCI College email addresses should only be used for the purpose of study and the conduct of PCI College business.

3.3. Email addresses may not be used for personal communication, registering with websites or platforms not directly related to PCI College business.

3.4. All incoming email should be validated to ensure you do not click on links or access resources which may be attempst at phishing etc.

3.5. Login credentials to PCI College systems must not be shared among learners or staff (Associate Lecturers).

4. STAYING SAFE ONLINE

4.1. Due to the increasing prevalence and sophistication of cyber criminals, scams and methods of extortion and exploitation are rife in contemporary internet usage. As a result, the following policies apply:

4.2. Never enter your username and password into a website or document unless you are certain that it is safe to do so

4.3. Be careful to check incoming and outgoing email – you recognise the sender and you do not click on any links or attachments which may be unsolicited (this includes monitoring your Spam/Junk email).

4.4. Ensure that your use of College provided internet access is for the purposes of PCI College business only.

4.5. Only trusted sites may be accessed when using PCI College internet access points.

4.6. Where your work necessitates use of a public hotspot or access point, you take reasonable precautions to safeguard that connection e.g. install and ensure your Virtual Private Network software (VPN) is up to date.

4.7. Should you be required to access PCI College resource from a home or private network, it will be necessary to ensure that your WiFi/Router is secured with a strong password.

4.8. All staff, Associate Lecturers and learners are responsible for reporting cyber security concerns in a timely manner (within 24 hours is preferable).

5. CONFIDENTIALITY

5.1. Data privacy and confidentiality are essential components to effective remote working, please refer to the Confidentiality Policy, Information Systems Policy and Data Collection Use and Management Policy for further information.

6. MISUSE OR IMPROPER CONDUCT (INTERNET, SOCIAL MEDIA & EMAIL)

6.1. Learners, staff or Associate Lecturers who are found to have breached the above policies may be subject to progression, dismissal or disciplinary actions.

6.2. Particular emphasis should be paid when referring to PCI College in public communications or on internet platforms and it is every stakeholder's responsibility to carefully consider the implications for any action which may bring the College, another learner, or the profession into disrepute.

7. LINKED POLICIES AND PROCEDURES

Linked Policies	Confidentiality Policy Data Collection, Use and Management Policy Privacy Policy Support for Learners Policy
Linked Procedures	Confidentiality Procedure Data Collection, Use and Management Procedure Support for Learners Procedure