19 BRING YOUR OWN DEVICE

22.1 INTRODUCTION

This policy is intended to address the use in the workplace by staff of non-college owned electronic devices such as smart phones, tablets and other such devices to access and store college information, as well as their own. This is commonly known as 'bring your own device' or BYOD. Users persona devices will only be granted access to college WIFI networks but may still indirectly obtain college data on those devices through other means.

It is the policy of PROCAT to place as few technical restrictions as possible on the development and use of new applications and services. However the use of non-college owned devices to process college information and data creates issues that need to be addressed particularly in the area of data security. As data controller PROCAT must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing. Employees and students are required to keep secure college information and data. This applies equally to information held on the college systems and to information held on an employee's own device.

Employees and students are required to assist and support the college in carrying out its legal and operational obligations with regard to college data and information stored on your device. Employees and students are required to co-operate with officers of the college when they consider it necessary to access or inspect college data stored their device.

If you wish to bring your own device and use it to access college data and information (BYOD) you must use your network credentials. The college reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its systems and infrastructure.

22.2 SECURITY OF SYSTEMS AND TECHNICAL INFRASTRUCTURE (OF THE INSTITUTION)

The college takes security very seriously and invests significant resources to protect data and information in its care.

As an employee when you use your company-issued mobile device to access the college systems and its data, you are expected to play your part in maintaining the security of college data and information that you handle. This includes security of transfer of data between the device and the college system.

This college requires that company-issued devices wishing to connect to the college network are installed with the approved device management software provided by the college.

This requires that all devices used for storing or processing college data and content have industry standard security passwords in place and that this security mechanism is used to protect that data.

Where a staff member uses their own device to access and store data that relates to PROCAT that then it is their responsibility to familiarise themselves with the device sufficiently in order to keep the data secure. In practice this means:

- Preventing theft and loss of data.
- Where appropriate, keeping information confidential.
- Maintaining the integrity of data and information.

Users should:

- Delete sensitive or commercial emails once you have finished with them.
- Delete copies of attachments to emails such as spread sheets and data sets on mobile devices as soon as you have finished with them.
- Limit the number of emails and other information that you are syncing to your device.

In the event of a loss or theft, you should change the password to all college services accessed from the devices (and it is recommended this is done for any other services that have been accessed via that device, e.g. social networking sites, online banks, online shops).

Failure to comply with this code is considered a disciplinary offence.

22.3 SECURITY AND E-SAFETY OF STAFF IT USERS

PROCAT is committed to providing a safe environment for students and staff including the online environment.

As an employee you are required to play your part in maintaining a safe working environment and in terms of BYOD this means keeping software up to date and avoiding content that threatens the integrity and security of your device, the college systems and the devices of learners and others. It also means ensuring that the device automatically locks if inactive for a period of time.

The college IT and eSafety Policy applies to the BYOD context. This provides standards expected on appropriate online behaviour including between staff and students. It is particularly important to maintain a distinction between personal content and work related content especially where interaction that takes place between individuals and where images and content are shared and published.

22.4 Monitoring of User Owned Devices

The college will not monitor the content of user owned devices for threats to the technical infrastructure of the institution. However the college reserves the right to prevent access to the college network by any device that is considered a risk to the network.

In exceptional circumstances the college will require to access college data and information stored on your personal device. In those circumstances every effort will be made to ensure that the college does not access the private information of the individual. College data and information can only be stored and processed on personally owned devices under acceptance of these conditions.

If certain secure or confidential categories of data and information are required to be accessed or stored on your own device then PROCAT would be obliged to monitor the device at a level that may harm your privacy and that of anyone you lend your device to.

The college will report regularly on internet usage and any breaches of the terms of use. This report will be monitored and discussed at Safeguarding and Quality Meetings and appropriate actions put in place.
If a member of staff or student is found to be engaging in any form of online activity that is deemed as cyber bullying, bringing the reputation of PROCAT into disrepute, and/or uses the Internet in any way to attack or abuse students, staff members, teachers or tutors then that person will have their access to the network revoked and could face disciplinary action.

22.5 Compliance with Data Protection Obligations

Your attention is drawn to the separate Data Protection Policy which requires you as an individual to process data in compliance with all aspects of the DPA and this applies equally to processing of data which takes place in the context of BYOD.

22.6 Acceptable Use of User Owned Devices

The college requires that all users of the IT system conduct their online activities which concern the college appropriately and particularly in compliance with the terms of acceptable use of the college. This requirement transcends whatever communications technology or device is being used. Our terms provide guidance on appropriate use of information technology and requires accountability of behaviour by individuals. The terms of Acceptable Use are located in the college's Information Technology and eSafety Policy. Failure to comply with the terms is considered a disciplinary matter.

Access to the PROCAT IT systems and networks is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the PROCAT IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any PROCAT IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access PROCATs IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to PROCATs IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-PROCAT authorised device to the PROCAT network or IT systems.
- Store PROCAT data on any non-authorised PROCAT equipment.
- Give or transfer PROCAT data or software to any person or organisation outside PROCAT without the authority of PROCAT.

Use of PROCAT internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to PROCAT in any way, not in breach of any term and condition of employment and does not place the individual or PROCAT in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which PROCAT considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to PROCAT, alter any information about it, or express any opinion about PROCAT, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.

- Forward PROCAT mail to personal non-PROCAT email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of PROCAT unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect PROCAT devices to the internet using non-standard connections.

Please be aware that the IT department will periodically audit all college-owned devices and reserves the right to remove without notice any material deemed to be inappropriate or not work-related. This includes, but is not limited to, the following:

- Photographs
- Films
- Music
- Non-college owned software
- Files such as books in .pdf or .doc format

22.7 Incidents and Response

Where a security incident, involving staff or students using their own devices, arises at the college this matter will be dealt with very seriously. The college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. The college Safeguarding Officer will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the college IT and eSafety Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Compliance with this policy forms part of employee’s contracts of employment and student code of conduct. Failure to comply will constitute the network access being revoked while investigations take place and may constitute grounds for action under the college’s disciplinary policy.