cetb

Bord Oideachais agus
Oiliúna Chorcaí
Cork Education and
Training Board

Document:	**Information and Communications Technology (ICT) Policy for College Adult Learners**
Procedure No:	**18-01 (year and version number)**
Effective Date:	**March 2019**
Supercedes:	**N/A**
Issued By:	**Cork ETB**
Reviewed On:	**19 February 2019**

Information and Communications Technology (ICT) Policy For College Adult Learners

Purpose

Access to college ICT resources is a privilege extended to learners by the college authorities. Providing an efficient and reliable computing and networking service, as well as access to communications devices, to Students and alumni depends on the cooperation of all Users. It is therefore important that you, as a User, are aware of your responsibilities. The purpose of this Policy is to provide all Users of the College's IT Resources with clear guidance on the acceptable, safe and legal way in which they can use the College's IT and Network Resources.

By using any of the College's IT and Network Resources, you agree to comply with the terms of this Policy. This Policy is without prejudice to the right to privacy as protected by the constitution and the European convention on human rights.

Scope/to whom it applies

This Policy covers documentation of policy, procedures, and standards relating to:

- College Information
- College IT and Network Resources

This Policy applies to all Learners of the College participating in course(s) of further education who may have access to the College's IT resources which includes, without limitation, its networks (accessed on site or remotely) and/or communications devices hereinafter the College's IT resources.

This document should be read in conjunction with the following associated documents;

- Learner Complaints Procedure
- Learner Disciplinary Procedure
- College Social Media Policy
- Cork ETB Assessment Handbook for Learners

Roles and Responsibilities

IT Services within the College / ETB is responsible for:

- Monitoring use of College IT Resources to ensure this Policy is not breached;
- Acting on breaches to this Policy and bringing any breaches to the attention of the Principal and/or Cork ETB IT Manager.

Each User is responsible for:

- Complying with this Policy and all other relevant policies and procedures;
- Ensuring all passwords assigned to them are kept confidential;
- Reporting all breaches of this Policy to the Deputy Principal and/or Principal

Principles of Acceptable Use

This Policy is based on the following principles:

1. Users must use the College's IT Resources in a responsible, safe and lawful manner.
2. Users must respect the integrity of computer systems, communication devices and networks to which they have access.
3. Users must respect the integrity of the data to which they have access.
4. Users must store and process College data in compliance with relevant Data Protection Legislation.
5. Users must follow any standards and guidelines (including those set out in this Policy) relating to the use of the College's IT Resources.

Principles of Unacceptable Usage

Users must not use the College's IT Resources, including its Networks on personal mobile devices, to:

1. Other than in the course of accessing material related to their course, knowingly access, download or distribute illegal or inappropriate material, including material that is in any way pornographic, obscene, abusive, racist, libelous, defamatory or threatening.
2. Engage in any form of bullying or other behaviour which is illegal or likely to cause harassment to others.
3. Use social media to degrade, bully or intentionally offend Staff, Students or other Users or use these tools to bring the reputation of the College into disrepute. Please reference the College's Social Media Policy for more details.
4. Gain unauthorised access to the account, systems or equipment of any third party - attempts at 'hacking' may result in criminal prosecution in Ireland or elsewhere.
5. Use another Users account.
6. Perform any activities which contravene the laws of the State, or the destination country in the case of data being transmitted abroad.
7. Undertake commercial activities or to otherwise further commercial objectives which are not a part of your work/studies in the College.
8. Infringe the copyright, patent or other intellectual property rights of any person including, by downloading unlicensed software or other unauthorised materials.
9. Infringe the data protection or other privacy rights of any person. Please refer to the ETB's Data Protection Policy.
10. Use of University systems or resource to facilitate plagiarism or cheating in exams or assignments.
11. Access, modify, or interfere with computer material, data, displays, or storage media belonging to the College or another User, except with their permission.
12. Connect unauthorised equipment to the College network.
13. Load or execute unlicensed software or other material on the College's IT Resources where this is likely to breach the licensing conditions or other Intellectual Property rights.
14. Knowingly introduce any virus, malware or other destructive program or device into the College's systems or network.
15. The use of computers to play online games is not allowed
16. learners are directly responsible for backing up their computer based work. While the use of removable devices is permitted, learners are expected to use the provided anti-virus software to scan any such device before opening files therein. The college accepts no responsibility for the transmission of viruses or malware if precautionary scans are not undertaken

17. learners are not allowed to interfere with, remove or dismantle any computer or audio-visual equipment and/or disconnect computers from the college network without the express permission of the IT department
18. The User should take all reasonable steps to ensure that they do not inadvertently introduce such programs or devices into the systems or network.
19. Store sensitive or confidential College data on personal devices.

If you process (or intend processing) personal data about others on a computer, you are obliged to comply with the provisions of the Data Protection Acts as amended, updated or replaced from time to time and the ETB's Data Protection Policy.

Use of Computer Rooms

Computer rooms are classrooms! Learners are to work quietly at all times and avoid unnecessary disruption to other users of the facility. Each Learner is responsible for his/her actions and is accountable to all staff members of this college. If a member of staff observes any Learner in breach of college regulations, the offending Lerner will be required to cease that activity immediately. Learners who do not fully comply with any such request may also face sanctions or punitive measures.

- no food or drink is allowed in any room that hosts computers, at any time
- the use of mobile phones in computer rooms is prohibited

Passwords and Access

Users have a responsibility to safeguard any credentials granted to them by the College. In order to limit security risks, all Users must abide by the following:

- Attempts must not be made to by-pass or render ineffective security measures provided by the College.
- Do not:
  - Share user IDs or usernames
  - Divulge passwords to other users
  - Seek to impersonate other users
  - Leave their computer unattended without logging out
- User Passwords must not be shared between users

Email

Each registered Learner may be provided with an email account for their use. If issued account is the primary way that the College will communicate with Learners. Email account holders must comply at all times with this Policy.

The email account of a Learner is provided for the duration of the course and will be deactivated on completion of the course. Any information contained in it including content, headers, directories and email system logs, remains the property of the College. Usage of the email system for academic purposes is encouraged (journals, review papers, professional bodies, etc.). However, this email address is temporary in nature therefore it is not recommended for ongoing personal use, any personal use should be incidental and is subject to the same policies and regulations as official use.

The College is not liable for the loss of any personal information contained in emails

Users are responsible for the integrity of their mailbox. IT Services cannot restore any emails deleted accidentally or otherwise. All email messages may be subject to the Freedom of Information Act 2014 (as amended, updated or replaced from time to time). Arising out of the need to protect the College's network, the College cannot guarantee the confidentiality of information stored on any network device belonging to the College.

- An email should be regarded as a written formal letter. Any defamatory or careless remarks can have very serious consequences. The use of indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise, is strictly prohibited.
- To prevent computer viruses being transmitted through the network, care must be taken when dealing with suspect e-mails and attachments of unknown origin are received. Suspect e-mails should be deleted immediately and never forwarded to other Users.
- Learners are not authorised to retrieve or read any e-mail messages that are not sent to them.
- Email messages must not be automatically forwarded (redirected) to external non-College accounts
- If you receive any offensive, unpleasant, harassing or intimidating messages via e-mail, you are requested to inform the College Management immediately

Internet

The College provides Internet access via a college-wide wireless network zone. The wireless service is provided on an *'as-is' basis* and individual 'one-on-one' support is NOT provided. Learners wishing to avail of this service can do so at no additional cost, but any such access will only be possible via a 'login' screen AND an active College account. Access will not be provided without a legitimate account. The usage of the internet is governed by the parameters set out in this policy.

Compliance with Policy

The College reserves the right to monitor, intercept and review, without notice, the activities of Learners where there is reason to suspect that this Policy is being breached, or where deemed necessary by the College for other legitimate reasons. The College reserves the right to disable access to IT networks if there is ANY evidence that their continued use is likely to cause a degradation of network performance or security or there is a risk that it will expose the college to legal action. It also reserves the right, through the IT department, to disconnect ANY computer and/or Learner from the network where there is evidence that the computer is being used in a manner which breaches copyright or data protection legislation, or which puts the services available to other users at risk.

Breaches of this policy will be dealt with under the Learner Disciplinary Procedures and may be considered as gross misconduct.