The City College
WHERE STUDENTS COME FIRST

Computer Access Policy

Document Summary

Date of approval: 09/09/19

Approved by: Academic Board

Last revision date: 13/09/18

Next revision date: 08/09/20

Computer Access Policy

1: Purpose

The reason for this policy is:

- To ensure the proper use of all College computing and network facilities.
- To ensure users accept certain responsibilities and obligations required to access the College's computing and network facilities.
- To ensure use of the computer systems and networks should always be legal and ethical, and reflect academic integrity and the standards of the College community.

2: Authorisation

In order to use the computing facilities at the College, you must first be authorised. Authorisation is in the form of a unique user-id and password. User ID's can **only** be obtained from the systems administrator. Once a User-ID has been issued, the corresponding password is required to be changed periodically. For security reasons previous passwords associated with the User-ID may not be used again.

3: General Principles

- Users must respect the privacy of other users and must not access private files or communications of others, even if these files are unprotected.
- All files stored on College systems are considered to be the property of the College and so are not confidential to the user.
- The College reserves the right to view or alter files, as necessary.
- The College will routinely monitor data, traffic flows and will remotely monitor all workstations.

4: When using computer facilities:

- You must not give your user-ID or password to anyone.
- You are responsible for anything that is done using your User-ID on a computer.
- Never use a computer to cause offence, worry or inconvenience to anyone.
- Do not display anything on your screen which is likely to cause offence or upset other users.
- Respect other peoples' privacy.

5: Use of IT Facilities

- You must use the IT facilities responsibly and in a safe manner at all times.
- You may send electronic mail only by an approved program configured in an approved manner. The City College reserves the right to monitor use of electronic mail and the Internet.
- The I.T Administrator may specify precautions to be taken from time to time against the spread of computer viruses. All files transferred between computers and, where appropriate, executable files copied over networks, must be virus checked.

- You must not leave logged-in College workstations unattended. Always log off and shut down the computer after use**.**
- It is your responsibility to ensure that your data is backed up, for instance on your personal computer/ flash drive/external hard drive/cloud or such other external media. (Please note the College computers run on Windows and use Microsoft Office. All students should keep this in mind when using documents which are not saved as Microsoft Word documents).
- Reasonable precautions will be taken to ensure the reliability of the service, but no guarantee of the correct functioning of a program or equipment is given.
- You may not install or uninstall any program without prior authorisation from the IT Administrator.
- You must undertake to abide by all license agreements for software entered into by the College with other parties.
- You may only use software and/or information provided by the College for educational purposes or as part of your duties as an employee or student of the College.
- You must respect the intellectual property rights, copyright and moral rights of authors.

6: Unacceptable Use

- Users are only to log onto ONE terminal at a time. If you continue to log on to more than one terminal at a time, your computer access will be restricted to class time only until the end of the semester.
- You must not use the IT facilities to engage in any unlawful activity.
- In using any of the College IT facilities you must not access or attempt to access any programmes, data or resources which belong to any other user.
- **DO NOT** unplug any computer or equipment from the mains. This could be dangerous, damage equipment and may risk loss of work. You are not allowed to charge your mobile phones in the building or remove plugs to access your own computers or other electronic equipment.
- Given the College's duty under the Counter-Terrorism and Security Act (2015), steps will be taken to prevent people being drawn into terrorism. To meet this duty, the College's systems must not be used to create, access, store, transmit or download inappropriate materials as defined in this document and under the Prevent legislation (eg. materials concerning extremism, radicalisation, and terrorism). The College reserves the right to monitor, alert and report attempted access to, or dissemination of, such inappropriate material.
- If you discover inappropriate material on a College computer or system you **must** report the matter immediately to the Prevent Lead Officer, Principal, or Director of Studies, leaving the material discovered in its original state in order that an investigation into its origin can be conducted.

7: Penalties for contravention

Any breach of the College Access Policy may result in immediate suspension from using the I.T facilities and those responsible may be held liable for any cost incurred or damage caused.