The City College

WHERE STUDENTS COME FIRST

Computer Access Policy

Document Summary

Date of approval: 18/11/19

Approved by: Academic Board

Last revision date: 31/08/2025

Next revision date: 31/08/2026

The City College: Computer Access Policy

1. Purpose

This policy ensures the proper and secure use of all College computing and network facilities. It outlines your responsibilities and obligations when accessing our systems, ensuring all use is legal, ethical, and reflects the standards of our academic community.

2. Authorisation and Responsibilities

To use the College's IT facilities, you must be authorised with a unique user-ID and password, which you can obtain from the systems administrator.

You must not share your user-ID or password with anyone.

You are responsible for all actions taken using your user-ID.

For security, you must change your password periodically and cannot reuse previous passwords.

3. General Principles

Users must respect the privacy of other users. You must not access private files or communications of others, even if these files are unprotected.

The College reserves the right to access and monitor data and traffic flows for a legitimate purpose (e.g., for security, to investigate a policy breach, or for legal reasons).

The College will routinely monitor all workstations.

4. Acceptable Use of IT Facilities

When using College IT facilities, you must:

- Use all facilities responsibly and safely.
- Not use any computer to cause offence, harassment, or inconvenience to anyone. Do not display anything on your screen that is likely to cause upset.
- Use email and other software programmes only as approved by the College.
- Adhere to all software license agreements.
- Use College software and information solely for educational purposes or as part of your duties.
- Respect the intellectual property, copyright, and moral rights of authors.
- Ensure your own data is backed up, for instance, on your personal computer, external drive, or cloud storage.
- Log off and shut down workstations after use. Do not leave a logged-in workstation unattended.
- Do not install or uninstall any programmes without prior authorisation from the IT Administrator.

5. Use of Artificial Intelligence (AI)

The use of Artificial Intelligence (AI) tools must be transparent and responsible.

Academic Integrity: The use of AI tools to complete coursework or assignments without a tutor's explicit permission may be considered academic malpractice and will be subject to the College's Academic Malpractice Policy.

Confidentiality: You must not input any confidential, sensitive, or personally identifiable data (e.g., student or staff names, personal details) into public generative AI services, as this data may not be secure.

Fact-Checking: AI-generated content can be inaccurate. It is your responsibility to critically evaluate and verify any information produced by AI tools.

6. Unacceptable Use

The following are examples of prohibited activities on the College premises:

- Logging on to more than one terminal at a time. Continuing to do so may result in your computer access being restricted.
- Engaging in any unlawful activity.
- Attempting to access programmes, data, or resources belonging to another user.
- Unplugging any computer or equipment from the mains. This is dangerous and may damage equipment or cause data loss. You are not permitted to use College mains sockets to charge personal devices.
- Accessing, creating, storing, or transmitting unlawful, harmful, or obscene material, including pornography.
- Using College systems to create, access, store, or transmit inappropriate materials as defined under the Prevent legislation (e.g., materials concerning extremism, radicalisation, and terrorism). The College will monitor, alert, and report attempted access to such materials in line with its duty under the Counter-Terrorism and Border Security Act (2019).
- If you discover inappropriate material on a College computer, you must report it immediately to a senior member of staff who then may report it to the Prevent Lead Officer, Principal or Managing Director, leaving the material in its original state for investigation.

7. Penalties for Contravention

Any breach of this policy may result in immediate suspension of your access to IT facilities. Individuals responsible for a breach may also be held liable for any costs incurred or damage caused.

8. Further Information and Resources

For additional details on the regulations that inform this policy, please refer to the following sources:

- Office for Students (OfS) Regulatory Framework: The OfS sets out conditions of registration for higher education providers, including expectations on student protection and welfare.
- https://www.officeforstudents.org.uk/publications/regulatory-framework-for-higher-education-in-england/
- The Prevent Duty (Gov.uk): Official guidance on the statutory duty to prevent people from being drawn into terrorism.
- https://www.gov.uk/government/publications/prevent-duty-guidance
- DfE Guidance on AI in Education: The official position on the safe and ethical use of artificial intelligence in colleges.
- https://assets.publishing.service.gov.uk/media/6842e04ee5a089417c8060c5/Leadership_Toolkit_-_Transcript.pdf
- Information Commissioner's Office (ICO): Guidance on data protection and privacy, which is relevant to the monitoring of user data.
- Information Commissioner's Office