Computer Equipment
Acceptable Use Policy for Learners

This policy applies to all learners and others who have access to NCC computer equipment and systems.

NCC reserves the right to monitor system use at any time to ensure adherence to internal policies and the law. Use of any equipment, service or system for unlawful purpose or activity may require NCC to co-operate and assist the police or others with their investigations:

- No additional hardware (e.g., USB memory devices, MP3 players, cameras, mobile phones, etc.) may be connected without prior authorisation from the appropriate staff member.
- No software may be downloaded using NCC equipment. Unlicensed duplication of any software program is illegal and will not under any circumstance be tolerated.
- NCC uses Anti-Virus software to safeguard its systems from malicious code. All disks, CDs, DVDs, memory sticks, or other transportable media must be virus checked prior to use on NCC equipment.
- No food or drink should be brought near the computer equipment.

Prohibited Uses

- Obtaining, displaying, or distributing material which could be considered obscene, pornographic, offensive, racist or abusive.
- Counter Terrorism Act 2015 - The Counter Terrorism Act creates a `Prevent Duty` that requires specific organisations, such as CITB, to take appropriate actions to prevent persons being drawn into terrorist or extremist groups. CITB Safeguarding policies and procedures cover this duty in much more detail. Individuals must not access terrorist or extremist websites or access any materials. Further, they must report any violation by themselves or any other person immediately. Any failure may result in disciplinary action and may result in reporting to authorities.
- Conducting a business online - *includes personal financial transactions*.
- Distribution of unsolicited advertising.
- Making or attempting to make unauthorised access to other computers or networks.
- Alterations to the set-up of the computers or to the software running on them.
- Accessing chat rooms or social networking sites.
- Network game playing.
- Downloading copyright-protected material, including copy-protected music files, without permission.
- Copying copyright-protected CDs without the necessary permission.
- Any illegal activity.
- Deliberate activities with any of the following characteristics:
    - attempting to introduce a computer virus
    - attempting to corrupt or destroy data
    - disrupting the work of other users
    - wasting staff time e.g., unauthorised tampering with hardware or software
    - attempting to install or download any software on the hard disc of the PCs

Filtering & Monitoring

CITB has adopted a Wi-Fi access process to ensure compliance with Keeping Children Safe in Education (KCSIE) and to safeguard all learners. All learners attending NCC sites will receive unique login credentials from the CITB administration team when signing up for a course. These credentials must not be shared.

A robust filtering and monitoring system is in place to block harmful or inappropriate content and protect all users. These systems are monitored daily by the Designated Safeguarding Lead (DSL). Any attempts to access harmful content will be dealt with in line with CITB's Operation Safeguarding Policy and KCSIE guidance.

All interventions are recorded in safeguarding records and, where relevant, logged in the safeguarding management system. Where serious concerns arise, these may be shared with external agencies such as PREVENT, Police, or Local Authorities. This process aligns with linked policies, including the CITB Acceptable User Agreement, KCSIE 2023, Learner Code of Conduct, and Prevent Duty.

Please note – <u>risks are attached to some online activities</u>:

Broadcasting of personal or private details over the network may lead to the receiving of unwanted mail or attention. Additionally, there can be risks associated with using social networking sites or chat rooms.

- Online financial transactions are often conducted safely over secure connections. However, NCC cannot be held responsible for any losses resulting from sending confidential financial information via the Internet.
- As part of your apprenticeship there may be activities which involve the use of audio/video communication and/or recording, all recordings will be used solely for the purpose for which they were obtained, shall be treated confidentially, and will be deleted once their purpose is fulfilled.

CITB and National Construction College policies are implemented to safeguard us from the many varying laws surrounding equipment and software use. Any student found to be breaking these policies will be subject to disciplinary procedures.

All policies and procedures are reviewed regularly, and amendments or additions will be communicated to all students. You should keep yourself up to date with the latest policy.