Wirral Met College

ICT Student Usage Policy

Document status	
Document owner	Deputy Principal
Document author	IT Manager
Document type	Policy
Date of document	November 2021
Version number	09
Review requirements	Annual
Date of next review	November 2022
Approval body	Senior Leadership Team
Publication	All Staff and Students
Code	PO56

Definitions

"ICT" (Information Communication Technology) includes the following; Computer hardware, software and peripheral devices, email, Internet, Virtual Campus (including discussion forums and messenger), and computer network (including wireless).

"The College" refers to Wirral Metropolitan College.

"Document" covers just about any kind of file that can be viewed on a computer screen, including; files read in an Internet browser, any file meant to be accessed by a word processing or desktop publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools.

"Graphics" includes photographs, pictures, animation, movies, or drawings.

"Display" includes monitors, flat-panel active or passive matrix displays, LCD projectors, televisions and virtual-reality tools.

1. Aims and objectives

1.1. The College recognises that ICT systems play a key role in the conduct of the College's curriculum and that these systems support students in carrying out their studies efficiently. Nevertheless, the provision of ICT systems to students does expose the College to a number of risks and liabilities. This Policy highlights those potential liabilities to ensure that students understand how they should be avoided.

1.2. The College invests substantially in ICT systems and the facilities provided represent a considerable commitment of resources. This Policy informs students of the College's expectations for the use of those resources to ensure that they are used appropriately.

We are committed to adhere to the JANET Internet Acceptable Usage Policy

2. Legislation

2.1. The College will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which is predominantly the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Data Protection Act 1998 and the Human Rights Act 1998, The EU General Data Protection Regulation (GDPR), and more recently the Prevent guidance for the Counter Terrorism and Security Act 2015.

3. Monitoring

3.1. Computers and network accounts are the property of the College and are designed to assist in the performance of students' work. Students should therefore have no expectation of privacy in any email sent or received; internet sites that they access or files they store in order to assure compliance with this Policy.

3.2. The College monitors ICT usage for business and security purposes and to ensure that students make appropriate use of the systems at all times.

3.3. The College may exercise its right to intercept email and internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons:

- To establish the existence of facts relevant to the College's business.
- To ascertain compliance with regulatory practices or procedures relevant to the College.
- To ensure that users of the system are achieving the standards required.
- To prevent or detect crime.
- To investigate or detect the unauthorised use of internet and email systems.
- To ensure the effective operation of the system, e.g. to detect computer viruses and to maintain an adequate level of security.

3.4. Although an email that is clearly marked as private cannot be defined as a communication relevant to the College's business, the College reserves the right to monitor the content of such an email where there is a reasonable belief that it may breach this Policy, for example by containing discriminatory or pornographic material.

3.5. For business continuity purposes, the College may need to check the emails of students who are absent.

3.6. The College reserves the right to use the content of any students' email in any disciplinary process.

3.7. The College has software and systems in place that monitor and record all internet usage. Therefore, students should not have any expectation of privacy in terms of their internet usage.

3.8. The College uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We use software to block access from within our networks to all such sites. However, if you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

3.9. Similar software is used to comply with the Prevent strategy guidance, specifically "*Specified authorities will be expected to ensure children are safe from terrorist and extremist material when accessing the internet by establishing appropriate levels of filtering.*"

3.10. To be able to exercise its rights (as described above), the College must have made all reasonable efforts to inform every person who may use the email and internet systems that monitoring may take place. The College believes that the communication of this Policy to all students meets this requirement and we therefore ask all students to sign to confirm that they have read and understood this Policy (refer to clause 10, below).

4. General operating principles and personal usage

The College's ICT systems are primarily for curriculum use.

4.1. The College operates within a framework of mutual trust and recognises that in certain circumstances, particularly when there is a need to communicate urgently, it may be appropriate for students to use email or the internet for personal reasons. However, such reasonable private usage must not interfere with students' course work or class time. Excessive unauthorised use of any ICT facility may lead to disciplinary action.

4.2. Each user is issued with a unique password for use of the College computer systems, for security purposes which must be changed at login. Students are responsible for safeguarding their password. For reasons of security, students must not print, store online or share their individual passwords with others. User password rights are given for security purposes and should therefore not give rise to an expectation of privacy. All passwords must be of 8 or more characters in length. Passwords should include upper and lower case letters and include numbers and symbols. The system will automatically lock out accounts for 30 minutes following 10 incorrect password attempts.

4.3. Students must not display, download, distribute, store, edit or record any material, including images, that are offensive, capable of constituting any form of discrimination (on the grounds of sex, race, disability, sexual orientation, religion, belief or age), obscene, pornographic or paedophiliac. Any such action will be considered as gross misconduct. If you find yourself connected incidentally to a web site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

4.4. Students should not log on to a computer and allow another user to access their account, specifically so that this student may bypass restrictions on their own account.

4.5. Students must not display, distribute, store or download any illegal material. Any such action will be considered as gross misconduct.

4.6. No user may use the College's ICT facilities to propagate any virus, worm, Trojan horse or malicious code.

4.7. No user may use the College's ICT facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

4.8. Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so.

4.9. Any changes required to ICT hardware configuration are to be performed by and are the responsibility of IT Services Department staff

4.10. The standards set out in this Policy are designed to minimise the risk of incurring liability in relation to students' usage of ICT systems. The College will take disciplinary action against any student who breaches any of the requirements contained in this Policy, which can include exclusion from college for those committing acts of gross misconduct.

4.11. The College's Disciplinary Procedure will be used to handle any disputes concerning the operation or application of this Policy.

4.12. Users shall not perform any other inappropriate uses identified by the network administrators.

5. Use of email and Messaging Services within Microsoft Teams

5.1. Unnecessary emails congest the email system. Students should not; send unnecessary emails (including bulk mail, i.e. to multiple recipients) or attach unnecessary files to email without good reason. Users must not begin or distribute chain emails or any other junk emails, including jokes and advertisements. Users should regularly delete unnecessary e-mails.

5.2. Students must never access another user's email account.

5.3. Emails must not contain any message or image that is discriminatory (on the grounds of sex, race, disability, sexual orientation, religion, belief or age), illegal, obscene, pornographic, abusive or threatening. The College does not tolerate discrimination, harassment or bullying and any breach of this rule will constitute gross misconduct.

5.4. Students should not make derogatory remarks in emails or teams chat about any other person. Written derogatory remarks could be considered to be defamation, which could give rise to legal action being taken against the author and/or the College.

5.5. By sending e-mails on the College's system, you are consenting to the processing of any personal data contained in that e-mail.

5.6. Microsoft Teams offers a platform to chat and message people directly as well as in groups. All of the rules regarding conduct of emails laid out above apply to Microsoft Teams messaging services. Message chats are logged and stored and can be used to provide evidence of misconduct.

6. Use of internet

6.1. College internet access is provided primarily for curriculum related purposes. It is to research relevant topics and obtain useful information (except as outlined below). We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others. All existing College policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of company resources, sexual harassment, information and data security, and confidentiality.

6.2. This College's Internet facilities and computing resources must not be used to violate the laws and regulations of the UK or any other nation. Use of any College resources for illegal activity is grounds for immediate disciplinary action, and we will co-operate with any legitimate law enforcement activity.

6.3. Any attempts to disable, defeat or circumvent any of the College's computer security facilities will constitute gross misconduct.

6.4. Whilst the College recognises students' rights to a private life, during any use of social networking sites or maintenance of personal blogs (online diaries), students are required to refrain from making any references to the College that could bring it into disrepute, or interacting or writing on the sites in a way that could constitute harassment of another student or employer. The College will treat any breaches of these requirements as disciplinary offences. As with any other personal usage of the internet, users are not permitted to write on personal blogs or access social networking sites during class hours unless for curriculum related purposes.

6.5. When using College internet facilities users shall identify himself or herself honestly, accurately and completely (including one's College affiliation and function where requested) when participating in social networking sites, chats or newsgroups, or when setting up accounts on outside computer systems.

6.6. Only those college employees or officials who are authorised to speak to media, to analysts or at public gatherings on behalf of the College may speak/write / broadcast in the name of the College to any website. Students may participate in social networking, newsgroups or chats in the course of studies, but they do so as individuals speaking only for themselves. Only those managers and College officials who are authorised to speak to the media, to analysts or in public gatherings on behalf of the company may grant such authority to publish on the WWW.

6.7. Students must never engage in political discussions through outside newsgroups using the College's computer system.

7. Copyright and downloading

7.1 Copyright applies to all text, pictures, video and sound, including those sent by email or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

7.2. Any software or files downloaded via the Internet into the College network becomes the property of the College. Any such files or software may be used only in ways that are consistent with their licenses or copyrights and in accordance with College policy.

7.3. Users may not upload any software licensed to the College or data owned or licensed by the College without the express authorisation of the manager responsible for the software or data.

7.4. Students must not download or distribute any pirated software using the College internet system. Any such action will be considered as gross misconduct.

7.5. Users may download only software with direct curriculum use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license and in previous agreement with IT Services Department.

7.6. Students may not use College Internet facilities to download images or videos unless there is an express curriculum related use for the materials.

7.7. Students must not use the College's internet facilities to download entertainment software, including games, and must not play games against other opponents over the internet.

7.8 Any file that is downloaded is scanned for viruses before it is run or accessed.

8. Use of WMC Wireless computer network

8.1. When using the WMC Wireless Network, you agree to adhere to rules and regulations as detailed herein.

8.2. To use the WMC Wireless Network, the user must install and maintain up to date antivirus software and operating system patches on their laptop.

8.3. WMC reserves the right to enable and disable wireless network access as appropriate in order to comply with JANET Acceptable Use Policy

8.4. Disclaimer of Warranties and Limitation of Liability

The Wireless Internet Access provided by Wirral Metropolitan College (WMC) is for use free of charge by students and staff of the college only. Wireless Access is provided on an "as is" and "as available" basis and WMC does not warrant that this service will be uninterrupted, error-free, or free of viruses or other harmful components. Users should be aware that there are security, privacy, and confidentiality risks inherent in wireless communications and technology, and WMC does not make any assurances or warranties relating to such risks. By using Wireless internet access, user agrees that WMC is not liable for any costs or damages arising from use of this service and WMC does not control any materials, information, products, or services on the Internet.

9. Responsibilities

9.1. The responsibility for drafting, updating, monitoring and reviewing this Policy belongs to IT Services Department

9.2. Students are responsible for complying with the requirements of this Policy and for reporting any breaches of the Policy to IT Services Department.

9.3. The IT Services Department is responsible for maintaining the College's computer systems and for supporting students in the proper usage of the systems. Where students require any information or help about the use or set up of the computer facilities, queries should be directed to your course tutor in the first instance, any issues with the ICT system can be reported via the ICT call logger, linked to from the virtual campus.

10. Informed consent

10.1. All students by clicking the acceptable usage disclaimer on PC login confirm that they will abide by this Policy and agree to comply with its requirements.