STUDENT IT CODE OF CONDUCT 2023/24

Anyone using computers, tablets, mobile phones, digital cameras, MP3 players, mobile network "dongles" or any other digital technology at Queen Mary's College (QMC) must keep to the College's IT Code of Conduct. All users are expected to act responsibly and to show consideration to others. By using the College computers or other devices you are agreeing to keep to the IT Code of Conduct and agree not to deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of, or offend any member of the college community.

COMPUTING FACILITIES

The College's computers are provided to support the administration of the College and the education of students and other users. The College's computers and network are not a place to store personal files such as movies, photographs or music files. Any such personal files could be removed without warning to conserve storage space for the proper use of the computers and network. Users must not do anything that will affect how the College's network performs or operates. For example, users must not:

- Try to download, store or install software onto College computers without discussing this first with the Network Engineer and/or the Deputy Head (Academic). Usually, students will never be allowed to do this.
- Try to introduce a virus or malicious code to the network.
- Try to bypass network security or other security systems, including the College's firewall.
- Try to access another user's account.
- Try to access an area or system they are not allowed to use.
- Try to use any form of hacking/cracking software or system.
- Connect a personal device to the network that acts as a Wireless Access Point (WAP) or router or a server.
- Connect any device to the network that has access to the Internet via a connection not provided by the College.
- Access, download, create, store or transmit material that is in conflict with the values or ethos of the College.
- Do anything that wastes technical support time and resources.

NETWORK ACCOUNT SECURITY

Network accounts will be set up when new users arrive at QMC. All users are responsible for the protection of their network account and must not let anyone else know their password. Users' passwords should not be easy to guess by anyone else. They should be a minimum of 8 characters long, contain at least one letter and one number, and at least one non-alphanumeric character. Passwords should be changed at least every six months. Users should not know anyone else's password. If any user suspects that someone else knows their password or they accidentally find out someone else's password, they must tell the IT Support Team (IT.Support@qmc.ac.uk) as soon as possible so that the password can be changed.

INTERNET ACCESS

The College's Internet service is filtered to prevent access to inappropriate content. The College keeps a record of all the webpages visited by all users.

- The use of public messaging services such as Skype or Facebook is allowed only at certain times; its use is not allowed when users should be working, unless using such a service is an essential part of their work.
- Users must not copy and use material from the Internet to gain unfair advantage in their studies, for example their coursework. Such actions may lead to disqualification by Examination Awarding Bodies.
- Users must make sure that they are not breaking copyright restrictions when copying and using material from the Internet; for instance they must not illegally download music or movie files by any means.
- Anyone using a 3G or 4G Internet "dongle" on their personal computer, or any other means of connecting to the internet, within College, must keep to the IT Code of Conduct.
- Wireless access is available in many areas of the College and must be used in accordance with the IT Code of Conduct, in just the same way as the wired network. Any individuals found to be misusing the system e.g. downloading illegal content, may be subject to disciplinary procedures, which may include being banned from the Wireless network.

EMAIL

All students are issued with a College email address. This is to allow them to conduct College business. Automated software scans all email and blocks any email containing any offensive or inappropriate material.

- Students are not allowed to use email during lessons, unless the teacher for that lesson has requested its use.
- If any user receives an email which is in conflict with the aims and ethos of the College or is offensive or upsetting, the IT Support Team (IT.Support@qmc.ac.uk) or the Principal should be contacted. The email in question should not be deleted until the matter has been investigated.
- SPAM emails received should be deleted.
- Sending or forwarding chain emails is not acceptable.
- Sending or forwarding emails to a large number of recipients is acceptable only for a good reason. Before doing so, the user must obtain permission from the IT Support Team or the Principal.
- No-one should open attachments from senders who are not recognized, or attachments which look suspicious.
- All users should periodically delete unwanted sent and received emails, remembering to empty the deleted items folder.

e-SAFETY and PRIVACY

Any computer or digital technology used within QMC must be used in accordance with all other College policies, especially the College's Anti-Bullying and Safeguarding Policies. **It is a legal offence to breach safety guidelines and search for anything related to extremism, pornography or other inappropriate content.** We regularly monitor usage and anything which breaches our guidelines could lead to suspension, exclusion and/or police referral.

Students are allowed to use Social Networking sites (e.g. Facebook) and Instant messaging services only at certain times and in accordance with the terms of use of the service they are using. However:

- Students are not allowed to use social networking sites during lessons, unless the teacher for that lesson has permitted their use.
- Students should only communicate with people whom they know personally.
- Students must not make arrangements to meet people they have met on the internet.
- Students must never accept files or downloads from people they do not know, or which look suspicious.

- Students must not use a screen-name which is offensive, or gives away additional personal information.
- Students must not add unnecessary or misleading personal information to their profile or account details.
- Students must not add or allow their profile, screen-name or contact information to be shown anywhere on-line.
- Anyone using voice or video communications must do so in accordance with other College policies and not in a situation where this could annoy other people.
- All users must, at all times, respect the privacy of other users.
- All users must not forward private data without permission from the author.
- All users should understand that the College can and will access personal areas on the network in order to ensure the safety and security of all users. Privacy will be respected unless there is reason to believe that the IT Code of Conduct and general expectations are not being followed.

PRIVATELY OWNED COMPUTERS and OTHER DIGITAL EQUIPMENT

Personal computers are allowed to be connected to the College network. The content on personal computers must be in keeping with the aims, ethos and values of the College. Privately owned computers and other digital equipment are subject to the IT Code of Conduct.

- All computers must be made available to be inspected and configured before being connected to the network. This may include 'PAT' testing.
- All computers should, for their own protection and the protection of the College's computers and network facilities, have the College-approved anti-virus software installed.
- Personal computers and other digital technologies are brought into and used at College entirely at the owner's risk.
- Any user must stop using personal computers and other digital equipment in College if requested to do so by the IT Support Team. Requests such as this may be made if personal equipment is interfering with the College's equipment.
- All users should make sure that personal digital equipment is turned off when unattended – e.g. students' laptops when not required during lesson times. All users who misuse the computer facilities or break the IT Code of Conduct may be subject to disciplinary procedures.

KEEPING CHILDREN SAFE IN EDUCATION (KCSiE)

The College has a responsibility under Keeping Children Safe in Education (KCSiE) to filter and monitor student internet usage on devices accessing College Wi-Fi and desktop PCs without 'overblocking' material that is useful to teaching and learning. The system we use to assist us is Smoothwall. Categories our filtering system, Smoothwall, blocks and reports on include:

- Adult Content (pornography and some chat and gaming sites)
- Suicide
- Substance abuse
- Criminal Activity
- Abuse
- Radicalisation
- Bullying

As part of our monitoring processes, attempts to access blocked content will be monitored and followed up by our Designated Safeguarding Team. Repeated attempts to access blocked content will be referred on under our wellbeing/behaviour procedures.

If you require access to a site that is blocked for legitimate reasons e.g. research for your studies, please speak to your Subject Tutor in the first instance.

SUPPORT

- If you have any questions, comments or requests with regard to the systems in place, please do not hesitate to contact the IT Support Team or the Principal. Faulty equipment should be reported to IT Support by sending an email to IT.Support@qmc.ac.uk.
- Users should not attempt to repair equipment themselves.

July 2023