College IT Rules and Regulations for the use of computing facilities

This document is available at https://www.queens.ox.ac.uk/official-information/

Access to facilities

1. By connecting a wired or wireless device to the network, you agree to abide by all terms contained in the University and College IT regulations. You are responsible for staying up-to-date with these regulations. Ignorance is not a defence.
   See: https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002
2. Access to the College and University network may be withdrawn if you are in breach of any of these regulations; you may also face disciplinary action from the Dean and/or Proctors. The University Proctors may also request that your network access is withdrawn following disciplinary measures.
3. A valid OXFORD SSO (Single Sign-On) username and password is needed to use the College computer room, printing facilities and student meal booking system. Access to the College network requires a valid REMOTE ACCESS username and password. https://it.queens.ox.ac.uk/get-connected/ Your OXFORD SSO user credentials are sent to you by Oxford University IT Services.

Use of facilities

1. Your computer MUST have anti-virus software that updates automatically from a trusted software vendor. Computers that display suspicious network activity or that are infected with viruses will be disconnected from the network.
   FREE anti-virus for University members: http://help.it.ox.ac.uk/viruses/
2. Your computer MUST be kept up-to-date with operating system updates and security patches. Failure to install updates leave computers vulnerable to viruses, malware and malicious attacks. See 1 above.
   Keep computers up-to-date: https://it.queens.ox.ac.uk/protection/
3. You are responsible for the actions of any person using your computer. This includes friends who have physical access to the computer in your room as well as people using it across the network whether authorised or as the result of not keeping a computer up-to-date with security and anti-virus updates.
4. Peer-to-Peer (P2P) file-sharing software is forbidden in College without prior written permission. This includes, but is not limited to: Gnutella, Gnutella2, EDonkey, BitTorrent, uTorrent, Shareaza, eMule, FrostWire, Ares Galaxy, WinMX and Soulseek. Depending on the seriousness of the matter you may be referred to the Dean and / or Proctors.
5. You MUST comply with the appropriate laws and codes of practice which include but are not limited to: 'Data Protection Acts', 'Computer Misuse Laws', 'Copyright Laws', 'Licence conditions of software', 'CHEST licence conditions', 'Federation Against Software Theft guidelines', and UKERNA rules, codes of practice and guidelines. For instance, downloading and distributing copyright material (eg commercial music, movies, audiobooks, software or eBook publications) without the copyright holders permission is in breach of copyright laws and you will be liable for prosecution in the Courts as well as face disciplinary action and fines from IT Services.
6. You are not permitted to run any network service on your computer without the express written permission of the IT Office. This includes, but is not limited to: IIS; Apache; SMB/CIFS; Samba; DNS; DHCP; WINS; Internet Connection Sharing (wired or wireless); File and Printer sharing. Running unauthorised services such as these can lead to security vulnerabilities and can cause connection problems for you and other network users.
7. All network devices connecting to the College wired network must be registered with the IT Office registration system. You MUST NOT connect any wireless access point, cable/broadband router, hub, switch or femtocell to the College network without written permission from the IT Office.
8. You should not knowingly create, transmit, receive or handle any material on University network that may be expected to cause undue offence to the staff, academics, your student colleagues or the public.
9. Unacceptable activities will result in disciplinary action. Examples include, but are not limited to: attempting to access College facilities without authorisation; attempting to access another user's computer, account or email; masquerading as another user; creating programs with malicious intent; introducing programs with malicious intent; software theft; using College facilities to harass any company or individual; sending chain or junk mail.

10. You MUST keep your passwords secure. Do not disclose them to, or allow them to be used by, any other person. Notify the IT Office immediately if you suspect that your University passwords have become compromised. A compromised password can have financial and credibility implications to you and the College. For example, someone could use your email password to access password recovery features on social network sites and send threatening or defamatory emails or posts.
11. The College network and the computer room facilities are for academic work and should not be used for any personal or commercial profit. This includes, but not limited to running any Crypto Mining Software.
12. The computer room facilities are available for your use not your abuse. You are expected to take reasonable care of these facilities and report faults immediately to the IT Office.
13. No food or drink may be taken into or consumed in the computer rooms. Repairs to computers damaged by spills will be charged at full cost to the individuals responsible. Also, no smoking is allowed anywhere in College.
14. You should only use paper provided by the College in the computer room printers unless the IT Office has given express permission. You will be charged the full repair cost for any damage caused by labels, transparency film or any other media that is not certified compatible.
15. Attempting to circumvent network and computer security restrictions imposed by the College or University (for example running an encrypted tunnel or changing your computer's MAC address) is a serious offence. Such security breaches will be referred to the Dean and Proctors.

Monitoring and securing the network

1. The College monitors network traffic in order to detect problems and to ensure the network is operating correctly. Logs record timestamps, source IP, destination IP, port, traffic type, application classification and amount of data transferred. Logs are typically kept for 60 days.
2. In the event of a network fault, or a case of serious network abuse (within College or from outside), it may be necessary to actively record certain network traffic. This is done as tightly as possible to only record what is under investigation, and will usually be restricted to just the activities of one computer or one service. Recorded data will be discarded as soon as possible, and nothing accidentally recorded will be analysed.
3. Any investigations into network use will be done with the express permission of a senior member of the College (usually the Dean). Users will always have the right to a fair hearing and an opportunity to put forward any information that they may think relevant.
4. The College occasionally runs network scans to detect unauthorised devices, services running without permission and recently discovered security vulnerabilities. This is to protect the College network and all of its users. If a scan flags any issues with a particular device, then attempts will be made to contact the owner of the device.
5. Firewalls are in place to prevent unauthorised access to the network and to known insecure services. Contact the IT Office if you think the firewall is impeding genuine academic work and we will investigate.

August 2023