Keble network rules and regulations

If you use any computer connected to the Oxford network, whether it is yours or one provided by the college or department, you MUST abide by all applicable laws and by terms contained in the University regulations as well as local College policies. If you do not obey the rules you may face fines or other disciplinary action.

University policies, rules and regulations can be found at:

https://unioxfordnexus.sharepoint.com/sites/DIGITAL-HUB/SitePages/Rules-and-regulations.aspx

https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002

Access to facilities

1. Computers may be connected to the College wired and wireless networks by Keble students and must only be done through the registration system unless specifically authorised and instructed by the Keble IT department. Note: it is fine to use computers on the centrally provided 'Eduroam' wireless network throughout the University in addition to this.
2. Wireless access points, routers, networked cameras or dedicated networked entertainment devices are not permitted to be connected to the College network.
3. It is not permitted to connect 'Internet of Things' devices such as smart lightbulbs, sensors or home automation systems to the College network. Exceptions may be made if there is a justifiable reason and provided the equipment meets certain requirements concerning security and privacy.
4. Access to the network from personal equipment may be withdrawn from any user by the IT Manager for any breach of the College regulations, or if instructed by central IT Services the University Proctors following disciplinary measures or detection of malicious activity.

Use of facilities

1. By connecting their own equipment to the College network, users agree to abide by all relevant College and University rules and regulations. It is your responsibility to ensure that you stay up-to-date with these regulations which will be accessible from the Keble website.
2. Only the paper provided by the college may be put into the printers unless express permission from the IT department has been given. Repairs to damage caused by labels or transparency film, which is not certified as laser printer-compatible, will be charged to the individuals responsible.
3. No material that may be expected to cause offence may knowingly be created, transmitted, received or handled on College IT facilities.
4. Users must safeguard their usernames and passwords and must notify the IT department immediately if they suspect the password has become compromised. Users must not share accounts or passwords with anyone else.
5. Use of the College network for any commercial use or personal gain (except for academic use) is strictly forbidden.
6. Use of the College network is primarily intended for academic purposes but personal use and entertainment is permitted provided it does not impact other users.
7. Users must comply with the following 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'.
8. Users must not engage in any unacceptable activities. Examples include: attempting to access College facilities without authorisation; attempting to access another users' computer, account or email; masquerading as another user or sending emails impersonating 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 email or junk email.

9. Illegal transfer of copyright material is forbidden. This includes, but is not limited to, music, films, commercial software. Legitimate downloading of content with the permission of the copyright holder is permitted.
10. Use of the network is not permitted for the access of extremist material which has the real potential to lead to serious terrorist crime on the part of the user, or with the intention of drawing people into terrorism (contrary to the College and University's statutory duty under *Prevent*)
11. Students are responsible for ensuring that their computer is kept up-to-date in order to prevent a way for people to break into the College network. This includes the operating system updates as well as any other security related updates.
12. Students are not permitted to run any network accessible server or service on their computers without the express permission of the IT department.
13. Users owning a computer connected to the College or University network are responsible for the actions of any person they allow to use that computer. This includes friends who have been allowed physical access to the computer as well as people using it across the network, whether authorised or as the result of not keeping a computer secure. It also includes use from home when you have connected your computer to the University VPN service.
14. Attempting to circumvent, or assisting others to circumvent, the security restrictions imposed by the College or University (for example, the use of a network tunnel or changing the unique hardware identifier of your computer) or other security measures is a serious offence and will be referred to the Dean or Proctors.
15. It is required that users have up-to-date anti-virus software installed. If it is detected that a computer is infecting others within college or the University, that computer will be disconnected immediately to protect others.

Monitoring and securing the network

1. The College routinely monitors traffic levels in order to detect problems and to ensure the network is operating correctly. This monitoring records only the address of the client and server, and the quantity of traffic transferred. It does not routinely record the contents of the network traffic.
2. In the event of a network fault, or a case of network abuse (from within the 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. The College and University also run occasional network probes in order to detect any unauthorised devices, services running without permission or security vulnerabilities. This is largely to protect the College network, but will occasionally be run on student machines if major security vulnerabilities have recently been discovered. If anything is found, then attempts will be made to contact the owner of the computer to advise them.
4. The College and University both have firewalls in place to prevent unauthorised access to the network or to known insecure services. Please contact the College IT department if this impedes genuine academic work and it will be investigated.