College IT Rules and Regulations

Summary

- Keep devices updated
- Use MFA
- Protect passwords
- No unauthorised network equipment
- No copyright infringement
- Report security incidents immediately

Access

1. By connecting a wired or wireless device to the network, you agree to abide by all University and College IT regulations and are responsible for remaining familiar with them. See also: 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 Access to the College and University network may be withdrawn if you breach these regulations. Serious breaches may also result in disciplinary action by the Dean and/or Proctors.
3. A valid OXFORD SSO account is required to access University email, online services and certain College systems.
4. A valid REMOTE ACCESS account is required to access the Eduroam wireless network.

Security

1. You must use Multi-Factor Authentication (MFA) where provided and must not attempt to bypass or disable MFA protection.
2. Your devices must be protected by current anti-malware measures appropriate to the operating system and must have security updates enabled. FREE anti-virus software is available to all University members: https://www.infosec.ox.ac.uk/endpoint
3. Your devices must be kept up-to-date with operating system updates and security patches.
4. You are responsible for ensuring that important data is backed up appropriately. The University provides Microsoft OneDrive for cloud storage and synchronisation. The College cannot guarantee the recovery of data lost as a result of device failure, theft, accidental deletion, malware, ransomware, or other security incidents.
5. You must keep your passwords and MFA credentials secure and must not share them with others.
6. Notify the IT Office immediately if you believe your account credentials have been compromised.
7. You must exercise caution when responding to emails, messages, phone calls or websites requesting credentials or personal information. Suspected phishing attempts should be reported immediately. Forward suspect phishing messages to: phishing@infosec.ox.ac.uk
8. You are responsible for the actions of anyone using your computer, whether through physical access or as a result of inadequate security.
9. Attempting to circumvent College or University security controls is prohibited. Examples include changing your device's MAC address or using encrypted tunnels to bypass network restrictions.

Acceptable Use

1. The College network and computing facilities are provided primarily for academic purposes. Reasonable personal use is permitted provided it does not interfere with academic activities, consume excessive resources, breach regulations, or generate personal or commercial profit. This includes, but is not limited to running crypto mining or similar software.
2. You must comply with all applicable laws and licence conditions, including UK GDPR, the Data Protection Act 2018, the Computer Misuse Act 1990, copyright law, software licence agreements, CHEST licences, FAST guidance and JANET policies.
3. Downloading, distributing or making available copyright material without permission is prohibited.
4. You must not knowingly create, transmit, receive or handle material that may reasonably be expected to cause undue offence or harassment.
5. Unacceptable activities include, but are not limited to:
    - Unauthorised access to systems or accounts
    - Accessing another user's email or files
    - Impersonating another user
    - Creating or distributing malicious software
    - Software theft
    - Harassment of individuals or organisations
    - Sending chain letters or junk mail
6. Peer-to-peer file-sharing software may not be used without prior written permission from the IT Office.
7. Users are expected to take reasonable care of College computing facilities and report faults promptly.
8. No food or drink may be consumed in the Moffatt Room (BQ6). Damage caused by spills may be charged to those responsible.
9. Only approved paper and media may be used in College printers unless authorised by the IT Office.

Network Services

1. You may not operate network services on College connected devices without prior written approval from the IT Office.
2. Examples include web servers, DNS services, DHCP services, file-sharing services, printer-sharing services, Internet connection sharing and similar services.
3. All devices connected to the College wired network must be registered where required. https://it.queens.ox.ac.uk/get-connected/wired-connection/
4. You must not connect wireless access points, routers, switches, hubs, femtocells or similar networking equipment without written permission.

Monitoring

1. The College monitors network traffic to maintain security, investigate faults and ensure the network operates correctly.

2. Network logs may record information such as timestamps, IP addresses, ports, application classifications and data volumes. Logs are normally retained for approximately 90 days.
3. In cases involving network faults or serious network abuse, targeted traffic monitoring may be undertaken to investigate specific systems or services.
4. Any investigation into network use will require authorisation from a senior member of the College, normally the Dean.
5. The College may perform security scans to identify unauthorised devices, unauthorised services and security vulnerabilities.
6. Firewalls are used to protect the network from unauthorised access and insecure services.

Enforcement

1. Failure to comply with these regulations may result in:
    - Temporary or permanent withdrawal of network access
    - Referral to the Dean
    - Referral to the University Proctors
    - Financial liability for damage caused
    - Disciplinary action under College or University procedures
2. Serious offences include:
    - Attempts to gain unauthorised access to systems
    - Circumvention of security controls
    - Malware distribution
    - Copyright infringement
    - Harassment
    - Network abuse
3. Users will be given a fair opportunity to respond to any allegation and present relevant information during any investigation.

IT Office
June 2026