Keble College has a computer room containing a number of PCs as well as a high quality laser printer for student use. There are additional computers in the College Library and the MCR offering access to email, web and library services, and there may be additional computers available for use in your department, central University libraries and the University’s IT Services department.

**Note:** Due to the ongoing pandemic, the college computer room and other shared facilities are currently closed in order to reduce the risk of infection to students and staff. We will make alternative printing facilities available, and we are investigating ways in which we might be able to safely reopen these resources in the future, but this is not likely to be possible in the short term.

It is strongly recommended that where possible students bring their own computer to the College. Each student room within College has a network socket that will connect their computer to the College network and the Internet. This requires that your computer is equipped with an Ethernet card or adapter. Wireless connections are also available throughout much of the College and elsewhere in the University. Students are not permitted to connect their own wireless access point, network switch or router in their room.

Students living outside College should check whether any network connection is available. Students living in private accommodation may need to sign up to a broadband service. You must check with your landlord before doing so, and be aware that many Internet service providers will insist on a 12 month contract.

University IT Services provides, amongst many other computing facilities, an online shop which can provide access to a number of software packages for free or at academic pricing – however you won’t be able to make use of the shop until you have started at Oxford and have received your University identification card.

**Viruses and Security**

You are required to have up-to-date anti-virus software installed on your computer at all times, and to keep your computer up to date with security updates. New viruses come out every day so anti-virus software quickly becomes out of date unless it is kept current. The University has site licenses for anti-virus software which can be installed free of charge. Without anti-virus software the IT Department may be unwilling to spend much time helping you when your computer becomes infected.

You are not permitted to run any service such as a web server on your computer without permission or use any form of file sharing service for illegally downloading or exchanging copyright material such as music or films. If caught doing so, you may face disciplinary measures and will be fined.

Anyone found trying to break into other systems, bypass security measures, distribute illegal or offensive material or otherwise abuse the network or any computing facilities will be dealt with appropriately.

Use of any computing facilities available within the University or connecting your computer to the network implies that you have read and agree to abide by the rules of computer use laid down by the College and University.

**Social Media**

Communication via social media, especially when interacting with accounts set up in the name of the College, or attributable to the College, should be treated as an extension of the Keble community, with users remaining respectful and mindful. Individuals should not publish any information or material which discriminates against any of the protected characteristics as outlined in the Equality Act 2010, nor publish any personal information on individuals which might contravene data protection laws.

If you have any questions concerning computer usage at Keble then please contact us and we’ll try to help. **Please be aware that due to the ongoing pandemic, we will be limiting support to virtual appointments and remote support tools whenever possible for the time being.**

Steve Kersley (IT Manager) Tel: 01865 272788
Howard Thomas (IT Officer) Email: it-support@keble.ox.ac.uk
Ran Michaeli (AV Technician)
IT Dos and Don’ts

This is not an exhaustive list, but just some useful tips to help you

**Do...**

- Install, and keep up-to-date, antivirus software.
- Install all security updates for operating system and applications.
- Keep regular backups of your important files.
- Check your email regularly.
- Bring all installation disks and/or license codes that came with your computer. Without these, if your computer needs reinstalling we cannot help.
- Make use of services such as training courses offered by University IT Services.
- Report any problems with College IT facilities to the IT Department.
- Be respectful to others via social media.

**Don’t...**

- Illegally download copyright content such as music or films. If caught, you’ll face a hefty fine.
- Install any network devices such as routers, wireless access points in your room.
- Trust unexpected email attachments, even if they claim to be from people you know.
- Let others use your computer unless you know what they’re doing and accept full responsibility.
- Give out your passwords to anyone else.
- Misuse the network or any College or University facility.
- Eat or drink in the Computer Room.
Recommendations for student IT equipment: home and college use

Introduction

This document has been written in the summer of 2020 to address specific requirements of pandemic-time teaching and learning. The document aims to offer students advice on IT and AV equipment, particularly to use the centrally supported software for online learning - Canvas, Panopto and Microsoft Teams. It provides equipment recommendations, best-practice on using the software options, and advice on set-up. This information has been prepared by University IT Services, with some changes by Keble IT department.

Recommended equipment

A computer

A laptop or desktop computer, running Windows, MacOS or Linux operating systems is the preferred equipment. Although tablet computers and smartphones can run standard web browsers and Microsoft Teams applications, the small screen and keyboard are generally limiting when working online and with documents for long periods. It is a good idea to check with your faculty whether there is any software that would be helpful for you to be able to run which might govern your choice of computer and operating system.

It is generally a good idea to consider a mid-range model with adequate memory (RAM – 8Gb should be adequate for most tasks), sufficient storage (at least 250GB), and plenty of USB sockets. Cheaper models tend to have poor battery life or performance and should be avoided. A good independent review site is Which - https://www.which.co.uk/reviews/laptops/article/laptops-for-students.

Some laptops do not come with an ethernet network socket and you may wish to purchase an adaptor to allow you to use a fixed wired connection with your laptop. If your subject involves specialist applications that need a lot of computing power you may wish to purchase a higher spec laptop, or alternatively your department is likely to have a computer suite which you can use.

A webcam

Most laptops and some monitors have a built-in camera, otherwise we recommend the Logitech range – ideally the Logitech C920 / C920s or C922 (~£80+ approx.). Note that some models may be unavailable but similar models are functionally fine. Alternative well-known models include Razer Kiyo or Microsoft Lifecam Studio.

A microphone and set of headphones, or a combined headset

A built-in laptop microphone may suffice, provided the laptop is close to you and the laptop fan is not running at high speed during the meeting. Webcams also usually come with a built-in microphone. Otherwise an external microphone or a headset would be better. You may need to use the sound control panel to choose which sound source you are using as default and test to see which sounds better.
Headphones offer advantages in online meetings as it helps the software reduce echoes, it’s easier to concentrate on the sound, and it makes the call less prone to feedback. For long sessions at home it is best to purchase DJ-style headphones that cover the ears rather than the tiny earbud types which are more suitable for on the go. Good headphone brands include Sony, JVC and Panasonic. An affordable option is **JVC Foldable Headphones (Model HAS160A)**.

A headset with a built-in microphone is an excellent option. It is best to purchase a headset that offers a reliable wired connection to the computer, rather than Bluetooth connections that might rely on batteries. An inexpensive model is the **Logitech H340 or H570e** wired headset. Alternative models include the **Razer** headset range popular with computer gamers. Though audio quality of these headsets can be variable on the cheaper models, the overall quality on better models should be reliable and consistent.

These headsets are also extremely useful for online Teams Meetings and Zoom calls home as using headphones increases the quality of the call experience particularly if using a laptop, tablet or phone and in noisy environments. When used for calls, as the microphone is very close to the mouth, careful placement of the microphone stem is required to avoid harsh sounds.


If you do need to purchase an external standalone microphone then the desktop USB microphones such as the **Blue Yeti Nano USB** (£99) or **Rode NT-USB** (£100 approx.) or **Samson Meteor USB microphone** (£150), are recommended for personal use.

**A mobile device**

Email and other forms of digital communication are central to both academic and social life at Oxford. You’ll often be notified of changes to rooms or tutorial times by email, and many social events are organised through Facebook. So, you will probably want to have a smartphone or other digital device to hand during the day.

Some students take their laptops out and about with them, while others prefer to keep them in their rooms. All libraries have plugs where mobile devices can be charged and used.

**Additional accessories**

Make sure you bring all the adapters and power supplies you need and make sure you have plenty of chargers and phone cables. If you are coming from overseas remember to bring a suitable plug adaptor and ensure that your equipment is able to work with standard 240 volt AC power here in the UK.

If you are still unsure of what IT to take to university and whether you need to buy anything beforehand, consider going to university with a very light load. This will make certain you don’t buy anything useless – after all, it will be just as easy to buy what you need once you’re settled in and you can ask for advice from your college IT staff. Here’s a short checklist:

- Mobile phone cables and charger(s)
- Electrical extension cables aka ‘gang sockets’ (handier than you might imagine)
- USB memory sticks (for backing up important assignments)
- SD/microSD storage cards for camera or tablet
• Installation disks or license codes, should you need to reinstall your computer or software.
• Long ethernet cable as an alternative to wireless. Most of college has reasonable wireless coverage, but there are a few areas where coverage is weaker so a wired network connection may be required.
• Please do not bring your own wireless access point or router, these are not needed and are expressly prohibited from being connected to the network in Keble.

Software

Two related sets of centrally supported teaching systems that are accessed through a standard web browser with your University username and password are:

• Canvas – A Virtual Learning Environment (VLE) - used for online course activities
• Panopto – Online Lecture recordings - accessed through Canvas

These web systems don’t require you to download any additional software. For online tutorials, conferencing calls and meetings the University centrally supports the Microsoft Teams application, again linked to your University username and password. Although Microsoft Teams can run through a web browser the experience is much better and more reliable by downloading a standalone application. Teams is a free download, and is available for both desktop, tablet and phone (Mac/PC/Linux). ([https://www.microsoft.com/en-gb/microsoft-365/microsoft-teams/download-app](https://www.microsoft.com/en-gb/microsoft-365/microsoft-teams/download-app))

As part of the University’s subscription you will be able to download and install Microsoft Office 365 on your computer, which will be licensed for the duration of the time you are a student at Oxford.

Similarly, the University’s subscription to Sophos antivirus is also extended to cover your computer. Information and instructions for downloading and installing can be found here: [https://help.it.ox.ac.uk/security/endpoint](https://help.it.ox.ac.uk/security/endpoint)

Using Microsoft Teams for meetings

To ensure your microphone and camera are set up correctly for using Microsoft Teams we recommend checking your settings and make a test call - select your profile picture then choose Settings > Devices. Choose Make a test call under Audio devices.

In a test call, you'll see how your mic, speaker, and camera are working. Follow the instructions from Test Call Bot and record a short message. The message will play back for you. After that, you'll get a summary of the test call, and you can go to your device settings to make changes.

In a Teams meeting you have a main toolbar that appears if you rollover the bottom of the screen – this has all the main options for your video and audio. It’s generally best to mute your microphone during a meeting if not speaking as this makes to call better for everyone. Equally you can turn off your camera if you want and this helps in very low bandwidth calls or if the application is giving you a warning that the network quality is poor. You can also turn off the incoming video of call participants and just use audio, this again will help conserve bandwidth if you’re experiencing dropouts in video or audio.
Security

If you are investing a great deal of money and time in choosing and buying your computer, there are a number of things you should do to take care of it:

First, we strongly recommend getting a 3-year warranty if possible, particularly for laptops. If the screen on a laptop fails, you may be looking at almost the cost of a new laptop to repair it. Desktops typically use standard parts and are therefore easier to repair than laptops but some parts can still cost over a hundred pounds if they fail. Manufacturer’s warranties are the best, and many will offer on-site engineers or next day collection. High street stores offer ‘extended warranties’ but they can be expensive and often do not have the best of reputations. Check online to see if anyone has any good or bad experiences and check for exclusions. If you already have a computer, the University has a contract with an external warranty company and students can purchase annual hardware support for their computer or printer reasonably cheaply through IT Services.

Insurance is also essential for full peace of mind. Warranties only cover hardware failure rather than accidental damage or theft. If you intend travelling overseas or are an international student then check that both warranties and insurance provide cover outside your home country.

Theft of a computer, while very uncommon, unfortunately does happen. To reduce the risks of theft, you should take the following steps:

- Never leave your computer unattended in a public place such as a library, and never leave the door to your room unlocked or windows open while you are away from the room. Most thefts are opportunistic rather than planned and many insurers will not pay out if the machine was left in an insecure environment.
- Make a note of the serial number of your computer, as well as the make, model and any identifying features. If possible, have it marked either with a non-removable label or an ultraviolet pen with your surname and postcode. This won’t prevent theft but may deter a potential thief and may also lead to your computer being recovered by the police.
- Use a security device such as a Kensington Lock, particularly with a laptop if you use it in a public place. Most modern laptops and a few desktops have a small oval hole somewhere on them which is designed to take a Kensington Lock connection. The other end of the cable should be attached to a secure immovable object.

Keep regular backups of your work and any other data files that are not easy to reinstall. If your hard disk fails, or your computer is stolen or seriously damaged then there is very little that we can do to recover your work. Use cloud storage services such as OneDrive (included as part of the University’s subscription to Office 365), or buy an external hard disk and make sure you keep backups of important files. **Tutors do not accept computer failure as sufficient reason for not completing work on time.**

Ensure that you have antivirus software which provides regular updates, and keep up to date with software updates for your Operating System and applications. You are entitled to install Sophos Endpoint Security as part of the University’s subscription. Information can be found on the IT Services website here: [https://help.it.ox.ac.uk/security/endpoint](https://help.it.ox.ac.uk/security/endpoint).

General Tips & Notes

**Webcam:** Whether you are using a USB webcam or the built-in webcam on your laptop, try to make sure that the camera lens sits at or slightly above eye level, no higher than your hairline. If you are using a built-in webcam on a laptop placed on a table, you may need to place it on a stand to make it
Higher. Ensure any support is sturdy to avoid camera shake when you tap the keyboard. Do not sit with your camera facing a window or with a window directly beside you as your face will be silhouetted. If using a tablet or phone purchase a stand or try and prop the device up to keep the image stable.

**Microphone:** Do not place your microphone close to your computer as the fan noise may be picked up. Try to sit or stand within 0.5m of the microphone. Use your OS sound settings to ensure input volume levels are high enough, but not so high as to cause distortion. Using a carpeted space will help to improve sound quality and reduce echo, conversely talking in kitchens or tiled laboratory rooms will cause unnecessary reverberation. If using a headset microphone, try to position the microphone stem to the side of your face to avoid pops and speak slowly, clearly and at a steady volume, perhaps regularly checking people can hear you ok.

**Laptop:** It’s a good idea to restart your computer every day. This can often improve the memory performance and makes glitches less likely to happen. Online video sessions can be processor-intensive so use a laptop stand to allow airflow beneath the laptop to avoid overheating and related fan noise. Keep the computer away from direct sunlight.

**Network connectivity:** It is always best to use a wired direct connection to your network hub. In most college rooms there will be a socket that allows a wired connection to your local network. You may need to purchase a standard long ethernet cable. If this is not possible, try to make your wireless connection as fast as possible by reducing activity across your shared network and not running too many video applications in parallel or on multiple devices. It is strictly against College rules to install your own Wi-Fi access point, switch or router in your room.

**Lighting:** All cameras capture better-looking video when there is a good light source. The room should be well-lit with natural light where possible. When selecting a place to make a call, avoid locations with low light or too much backlighting (avoid windows in the background as mentioned above). If a location with ample natural light is not available, you ideally want to light yourself from the front with soft, indirect light, and minimise other lighting in the room.

**Links to further information**

Getting started and IT help from IT Services at Oxford University

https://help.it.ox.ac.uk/

Email help line for IT at Oxford University

help@it.ox.ac.uk

Microsoft Cloud Service - called Nexus 365 at Oxford - includes Microsoft Teams guidance

https://help.it.ox.ac.uk/nexus365/index

Canvas VLE for students guidance

https://www.ctl.ox.ac.uk/canvas-for-students
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 policies. If you do not obey the rules you may face fines or other disciplinary action.

University rules and regulations can be found at http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

Access to facilities
1. Use of the Computer Room computers and printer requires a valid username and password issued by the Keble IT department.
2. A single computer may be connected to the College wired network by each student and must only be done through the registration system unless specifically authorised and instructed by the Keble IT department. If you replace your computer during the year or you have a genuine need to register a second computer for your academic work, you should contact the IT department. Wireless access points, routers, games consoles or dedicated networked entertainment devices are not permitted to be connected to the College network. Note: it is fine to use multiple computers on the ‘Eduroam’ wireless network throughout the University in addition to this.
3. Access to Computer Room facilities and/or access to the network from other equipment may be withdrawn from any user by the IT Manager for any breach of the College regulations, or if instructed by the University Proctors following disciplinary measures.

Use of facilities
1. By either using the Computer Room facilities or 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. No food or drink of any kind may be taken in or consumed in the Computer Room. Repairs to computers damaged by spills will be charged at full cost to the individuals responsible.
3. 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.
4. No material that may be expected to cause offence may knowingly be created, transmitted, received or handled on College IT facilities.
5. 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.
6. Use of the Computer Room facilities or the College network for any commercial use or personal gain (except for academic use) is strictly forbidden.
7. Access to the network is provided for academic purposes only. Excessive use of the facilities for downloading non-academic material, playing games or other usage that affects other users is not permitted.
9. 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.

10. Users must take reasonable care of the Computer Room facilities and report any faults to the IT department immediately.

11. 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.

12. 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)

13. 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.

14. Students are not permitted to run any network accessible server or service on their computers without the express permission of the IT department.

15. Users owning a computer connected to the College 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.

16. 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.

17. 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.