MAGDALENE COLLEGE

CAMBRIDGE

COMPUTING FACILITIES

Guide for 2019 – 2020

Contents

1 Computer Facilities at Magdalene 4

1.1 Computer Office 4

1.1.1 Staff 4

1.1.2 Cleaning Infected Machines 4

1.1.3 Providing Technical Assistance 4

1.1.4 Hardware Support 4

1.2 Network 5

1.3 College Student Computers 5

1.3.1 Andrew Clarke Suite (Mallory Court) 6

1.3.2 College Library 6

1.3.3 Cripps Court computer room 6

1.3.4 Thompson's Lane Hostel 6

1.3.5 Basing House Hostel 6

1.3.6 Porters Lodge 6

1.4 Charges 7

1.4.1 Black & White Printing 7

1.4.2 Colour Printing 7

1.4.3 Library Photocopier 7

1.4.4 Large Format Printing 7

1.4.5 Document Binding 7

1.4.6 Payment 7

1.5 UIS Desktop Services 7

2 CRSID & Email 8

2.1 Your CRSID 8

2.2 Retrieving Your CRSID 8

2.3 Email 8

3 Connecting Your Personal Computer to the Network 8

3.1 College Wireless Access 8

3.2 Room connection 9

3.3 Personal Wireless Routers 9

3.4 Registering Your Computer on the Network 9

3.5 Internet Charges 9

4 Security 10

4.1 General 10

4.2 Patches 10

4.3 Staying safe online 10

4.4 Viruses 10

4.4.1 Types of Virus 10
4.4.2 Anti-virus software 11
4.5 Spyware and Malware 12
4.6 Ransomware 12
4.7 Personal Firewall 12
5 Network Use 13
5.1 General 13
5.2 LAN Traffic 13
5.3 Copyright Infringement Notice 14
5.4 Peer to Peer file sharing 14
5.5 Skype 14
5.6 Streaming Audio and Video 15
5.7 University Rules and Regulations 15
5.8 Magdalene Rules and Regulations 15
6 Useful Websites 17
6.1 Magdalene College Internal Website 17
6.2 University Information Services 17

1 Computer Facilities at Magdalene

1.1 Computer Office

The Computer Office is responsible for all matters relating to the use of the College LAN and provision of computing facilities and support for administrative staff, students and fellows. The Computer Office is located in the Lutyens Building (Benson E3) on the West side of the college and is manned 9.00am – 5.30pm. Outside of these hours, for emergency support only, the Porters' Lodge should be contacted: they will make contact with a member of the Computer Office staff.

1.1.1 Staff

The Computer Office is manned by the following full time staff:

Computer Officer:	Nigel Hawkes
Deputy Computer Officer:	Mark Reed
Assistant Computer Officer:	Usman Zia-Ul-Haq
System Developer:	Iain van Gardingen

Computer Office staff can be contacted during office hours by telephone on (3)32127, or at the following email address: computer.office@magd.cam.ac.uk

1.1.2 Cleaning Infected Machines

Although the Computer Office has no duty to clean or rectify problems with a Student's personal machine, it does provide this service when operationally possible.

No responsibility can be taken for any loss of work or damage to the computer while it is left with the Computer Office. Obviously, the Computer Office will take great care not to cause any loss, but it is the duty of the owner to ensure that their work is backed up. If, as part of the clean up process, it is necessary to reinstall any software, the owner must provide the required media (CD/DVD's) and legitimate software licences to use. During the cleanup process, any inappropriate software which is known to be or is a potential cause of problems will be removed.

One of the biggest problems faced by the University is use by Students of inappropriate peer-2-peer software to download unlicensed copyrighted material. Please see the sections titled 'Network Use' and 'peer to peer file sharing'.

1.1.3 Providing Technical Assistance

The Computer Office will provide technical advice and assistance where it can. This can be to do with using the college computers or personal computers or advice on purchase of computer equipment.

1.1.4 Hardware Support

The Computer Office will provide support and advice for problems concerning hardware, if it is unable to help then the owner will be directed to the University hardware support service. They can provide extensive support for all computers and data recovery, however, this service is not free.

1.2 Network

The College is connected to the Cambridge University Data Network (CUDN), which covers the City and other local institutions. In turn, the CUDN is connected to the Joint Academic Network (JANET) which connects the UK's education and research organisations to each other as well as to the global Internet. The CUDN provides access to JANET and the Internet at speeds of up to 10Gb/s. Each of the institutions connected to the CUDN maintain their own networks, Magdalene is connected to the CUDN via a 1Gb/s link. The network infrastructure within the College provides 100Mb/s connection in all student rooms.

1.3 College Student Computers

There are a number of computers provided for general use principally in three locations: Benson Court E1, the College Library and Cripps Court. There is a mix of Windows and iMac computers installed with Microsoft Office software. They also have a range of course specific software installed. There are scanning facilities available in each location.

Access to the machines is controlled by a user ID and password. Your **UserID** to login to the College computers is the same as your **CRSID** (see section 2.2 Retrieving your CRSID), your password will however be different and will be emailed to your *crsid*@cam.ac.uk email address.

Once you have logged on you will find there is a network drive g: which is where you should save your work to.

It is important that when you have finished using the Computers you must logoff, failure to do so could make you liable to print charges through someone else using your logon

On each of the College computers there is a loose USB cable near the monitor, this should be used to plug your memory sticks into. Some USB memory sticks have not been recognised when plugged into the extension lead and these will have to be plugged directly into the computer. Your memory stick will appear as drive D: in Windows Explorer. When you have finished using your USB stick ensure that you use the 'Safely Remove Hardware' icon in the bottom right corner of the screen to avoid corrupting it.

Access to the buildings is controlled via your University Card. Currently each student is initially allocated 8GB of storage on the server which is backed up daily.

All College Student machines are maintained by the Computer Office. Any problems with these machines should be reported to the Computer Office, this includes problems with printing and resetting forgotten passwords.

1.3.1 Andrew Clarke Suite (Mallory Court)

- 2 x Windows 7, dual monitors and Epson flatbed scanner
- 1 x Windows 7 with dual monitors
- 2 x Windows 7 with single monitor
- 1 x 21” Apple iMac
- 1 x 27” Apple iMac with Autocad installed
- 1 x 27” Apple monitor for connection to Mac laptops
- 1 x 27” PC monitor with VGA & HDMI connections
- 1 x HP Laserjet 4700 Colour (simplex) printer
- 1 x Large format paper trimmer

1.3.2 College Library

- 1 x Windows 7 with Fujitsu Scansnap sv600 book scanner
- 4 x Windows 7 with single monitor
- 2 x 21” Apple iMac
- 1 x HP Laserjet 4700 Colour (duplex) printer
- 1 x Terminal opposite Library counter to access College Library Catalogue and the University Library Catalogue
- 1 A3 Colour Photocopier, this can also be used to scan and print from a USB memory stick

1.3.3 Cripps Court computer room

- 1 x Windows 7 with Epson flatbed scanner
- 2 x Windows 7 with single monitor
- 1 x HP Laserjet 4700 Colour (duplex) printer

1.3.4 Thompson’s Lane Hostel

There is a Windows 7 based PC with a HP LaserJet 4250 B/W (duplex) printer available primarily for printing although the standard software is installed.

1.3.5 Basing House Hostel

There is a Windows 7 based PC with a HP LaserJet 4250 B/W (duplex) printer available primarily for printing although the standard software is installed.

1.3.6 Porters Lodge

There is a Windows 7 PC in the Porter’s Lodge available for quick access.

1.4 Charges

1.4.1 Black & White Printing

There are black and white laser printers in the **Andrew Clarke Rooms (Benson E1)**, **Library, Cripps Cour**t, **Basing House** and **Thompson's Lane** hostels which you can print to. Single sided printing is charged at 6p per sheet and duplex printing is charged at 4p per side i.e. 8p per sheet. The printer is filled with standard 80gsm laser paper, personal paper up to 180gsm can be used via the multi-purpose tray.

1.4.2 Colour Printing

There is colour A4 laser printing available in the **Andrew Clarke Rooms, Library and Cripps Cour**t. Single sided printing (the default) is charged at 10p per sheet and duplex printing is charged at 7.5p per side i.e. 15p per sheet. This printer will handle paper up to 200gsm via the multi-purpose tray.

1.4.3 Library Photocopier

The library has an A3 colour photocopier which you can access using your College User ID (CRSID) and password. You are also able to associate your College user id with your University Card and then use that as a more convenient way to use the photocopier.

Prints can be sent from the Library computers directly to the photocopier as well as printing directly from a USB memory stick. It is also possible to scan A3 documents to a memory stick.

The cost of A3 single sided printing is 20p per sheet and duplex printing is charged at 15p per side i.e. 30p per sheet.

1.4.4 Large Format Printing

Large format printing is available up to A0 from the Computing Office. Files should be presented in PDF format and prices vary from £2 for A2 on 90gsm paper to £7.50 for A0 on 180gsm paper.

1.4.5 Document Binding

Documents up to 125 sheets can be wire bound with clear acetate front cover and thin card back cover. The cost per document is £3.

1.4.6 Payment

All charges are added to your college bill at the end of term. This covers network charges, printing and ad-hoc charges e.g. hard disk replacement, document binding.

1.5 UIS Desktop Services

At various locations in the University there are public rooms with DS (desktop services) machines which are maintained by the Computing Service. These machines have all of the standard software installed and also course specific software too. Access to these machines is via your CRSID and password.

You can access your DS-filestore space from your personal computer, instructions on how to do this can be found here:

http://www.ucs.cam.ac.uk/desktop-services/ds-filestore/cifs

Please note that the Windows based college Student computers are not set up as DS machines. We do however maintain a subset of the DS software on them.

2 CRSID & Email

2.1 Your CRSID

Your **CRSID** is used extensively throughout the College and University as your ID. It is usually made up with your initials followed by some digits. e.g. ngh24.

A centralised authentication system, known as **Raven,** uses the same ID as does the University email system, your email address will be ***'yourcrsid'*@cam.ac.uk**.

2.2 Retrieving Your CRSID

For information about how you retrieve your CRSID please visit this webpage https://help.uis.cam.ac.uk/service/accounts-passwords on the University website.

2.3 Email

Full information about the University email system and how you can access it can be found here: https://help.uis.cam.ac.uk/service/email

3 Connecting Your Personal Computer to the Network

3.1 College Wireless Access

The College wireless network is accessible in the majority of locations and work is ongoing to improve this further. There are four wireless networks visible: **eduroam, magd, magd-blue** and **magd-local**.

eduroam
This is part of a global academic wireless provision which provides internet access using your locally provided access token. It is available in many Colleges and Departments as well as the majority of Cambridge city centre. To retrieve you **eduroam** token you need to go to http://tokens.csx.cam.ac.uk using you Raven logon.

Once you have this token, the logon ID is you full Cambridge email address and the password is the token retrieved.

When you access the **eduroam** network from within the College you will also have to register you machine on the College network as described in section 3.4.

magd
This network is primarily used for conference business or adhoc guest visitors. A temporary registration can be requested from the Porters lodges or from the Computer Office.

magd-blue

This network is not for general use.

magd-local
The **magd-local** network is available to members of the College only, it does not require a user ID and has the password 'gardetafoy'. This connection does require the device to be registered on the network as described in section 3.4. There are occasions when **eduroam** and **magd** may not be available due to operational reasons which this SSID will not be affected by.

3.2 Room connection

We aim to have Wi-Fi available in all College rooms but where this is not the case each room does have an Ethernet socket. In rooms where this is a weak wireless access we are installing Wi-Fi enabled network sockets. These provide wireless access but still enable a wired connection to be made. A wired connection will always give the best connection, if your computer has an Ethernet socket but you have no cable to connect it with we can provide you with one.
The location of the wall sockets is not always in a convenient position for the desks therefore, the length of the patch cable you will need will vary from room to room. Patch cables in various lengths are available from the Computer Office free of charge.

3.3 Personal Wireless Routers

We do not encourage the use of personal wireless routers as they can have a detrimental effect on the College network if they are not configured correctly. However, we do recognise that there can be circumstances when more than one wired connection is required or the Wi-Fi signal is weak. If either of these is true, please come along to the Computer Office in Benson E3 before taking any action yourself and we will try to help.

3.4 Registering Your Computer on the Network

Ensure you have connected your computer to the network via a wired or Wi-Fi connection. Open your preferred web-browser and if no registration page is presented go to it directly by entering http://register.l.magd.cam.ac.uk this will open a Magdalene College logon screen which will ask you to enter your **CRSID** and **Raven** password (see section 3.2 re collecting your **CRSID** and **Password**). Once you have done this and have agreed to the rules regarding 'use of the network', your machine will be registered and you will have full Internet access (the process can take a few seconds and may require a reboot). The IP address allocated will always be the same for each registration; this registration process will take place at the start of each quarter. You are able to register up to six connections, it should be noted that connecting a device by a wired and wireless connection counts as two connections.

3.5 Internet Charges

All student rooms are provided with and billed for Internet access; this is charged for on a daily basis at the pro-rata rate of £3.40 per week. Although there is no daily download limit it is expected that the average daily traffic will not exceed 10GB/day over the term. To avoid accidental excess use you get an allowance which accumulates at 10GB per day. You will receive an email warning if you traffic exceeds the average of 10GB/day and your connection will be limited. This can be over ridden by going to your personal traffic management webpage http://register.l.magd.cam.ac.uk. You will be asked for an explanation if you exceed the term average of 10GB/day.

4 Security

4.1 General

Cambridge University has been and continues to be a prime target for hackers from all around the world, so it is essential that security is taken seriously. Threats from various sources are constantly evolving and need to be monitored. There is no sure way to be totally secure other than to keep your PC turned off. Clearly this is not an option but the following should help you to reduce your risks. It is important that you ensure that your machine is as secure and clean as possible before it is connected to the College network. Students should be aware that they are personally responsible for the security of their own computers.

4.2 Patches

Operating systems and software applications are constantly being updated to fix flaws both in their functionality and security. Most of these updates are available free of charge from the relevant company websites.

Most operating systems have automated update systems. In the case of Microsoft Windows 'Automatic Updates' should be enabled, so that new patches and updates are downloaded and installed on a regular basis. MacOS X systems have a 'Software Update' facility which should be run on a regular basis. Since MacOS X machines are beginning to be targeted more by hackers, it's vital that patches are applied. Linux and other UNIX like systems also need to be updated on a regular basis too. The way that updates and patches are applied on these systems varies.

4.3 Staying safe online

Please visit this page on the University website which points out what to look for and advice when going online

https://help.uis.cam.ac.uk/service/security/stay-safe-online

There is also this Moodle interactive tutorial which will raise you awareness and takes 30-40 minutes to complete

https://www.vle.cam.ac.uk/course/view.php?id=137361

4.4 Viruses

4.4.1 Types of Virus

Trojan Horses

As the name suggests, a Trojan horse program is a program that pretends to be something that it is not. A user is enticed to download them and run them manually (as Trojans don't spread on their own). Once run, these programs install themselves so that they are started up each time the computer is turned on. Trojans have a wide range of uses, from hijacking/redirecting web traffic to opening 'back doors' on systems to allow hackers remote access.

Worms

A Worm is typically a small program which spreads very rapidly over a computer network, typically by exploiting a known bug (typically a buffer-overflow) in an operating system or

application. Many worms use email to spread themselves. Worms like Trojans get added to the start up programs on a system, and typically interfere with anti-virus and other security software. Worms can make systems unusable by slowing them down to a crawl or by having an immediate payload which can be destructive.

Boot Sector
This type of virus replaces the 'boot sector' of the PC which contains the program that enables a computer to start up. This type of virus is not very common these days, since these were typically spread by booting from an infected floppy disk.

Parasitic Viruses
Also known as file viruses, these attach themselves to a specific program (or 'executable'), or to all programs on a system. Once a system is infected it may behave strangely and some programs may not work anymore. Anti-virus software may not be able to repair systems which are heavily damaged – requiring all of the infected software to be reinstalled from scratch.

Macro
These take advantage of built in macro commands that are embedded in files and run automatically. These are most commonly found in Microsoft Office documents particularly Word and Excel. Once infected, any new or existing document opened on that system will become infected.

Hoaxes
Hoaxes are reports of non-existent viruses. Typically they arrive as emails which warn of new viruses or security problems and ask you to email everyone you know. Hoax emails will often ask you to delete legitimate files from your system which prevents it from working properly.

4.4.2 Anti-virus software

It is absolutely essential that your machine has anti-virus software installed and that it is kept up to date. Most new machines are supplied with anti-virus software pre-installed but these will normally expire after three months to a year.

If you have a Windows machine (Windows 7 or later) then using Microsoft Security Essentials is a good option and is free from;
https://www.microsoft.com/en-us/download/details.aspx?id=5201

Many antivirus programs can slow your machine considerably, even the newest machines. We have found Security Essentials to be comprehensive, efficient and fairly light on resources.

It is important that you do not install more than one antivirus program and therefore you should remove any pre-installed antivirus programs, if you do not wish purchase them at the end of the initial trial period, before installing another.

Cambridge University has a site licence for McAfee anti-virus software which is available free to all users of the University network.

https://help.uis.cam.ac.uk/service/security/antivirus

Please visit the College intranet page for other useful downloads:

https://www.magd.cam.ac.uk/magnet/it-support

Please note: you will only be able to access this webpage once you are connected to the Magdalene College network.

4.5 Spyware and Malware

In recent years the threat from viruses has been brought more or less under control, but a bigger problem showing enormous growth is '**spyware**' and general '**malware**'. As the name suggests '**spyware**' is software that collects information about your activity and then returns this information back to a remote system.

'**Malware**' is typically a piece of software that gets installed without your knowledge. These are typically search bars, links to premium rate services appearing in your programs menu etc.

Both of these classes of software pose a security threat to you. These programs also tend to make your machine very slow. A lot of current '**spyware**' and '**malware**' is becoming viral in nature making them increasing act like viruses (and thus making them difficult to remove). A clear indication that your machine has become infected is that your web-browser opens up lots of annoying pop-up windows.

Microsoft has a product called 'Windows Defender' which is pre-installed (from Windows Vista onwards). This provides a dynamic background scanner which prevents a lot of '**spyware'** and '**malware'** from being installed. Windows Vista and Windows 7 allow you to use the free Security Essentials (which replaces Windows Defender). In Windows 8, 8.1 and 10 the built in Windows Defender is essentially the same as Security Essentials.

4.6 Ransomware

Ransomware is a type of malware which uses cryptovirology to create malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a successful cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem. Having good backups of all your work is the best way to mitigate your exposure to his threat, engaging with any ransom demand is not recommended.
Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the "WannaCry worm", travelled automatically between computers without user interaction.

4.7 Personal Firewall

Mac and Windows machines have a personal firewall built in, which should be turned on. The Windows firewall needs to be configured to allow 'ICMP incoming echo requests' (required by the University). If you are using an operating system which doesn't have a firewall built in then you should consider installing a third party one.

5 Network Use

5.1 General

Although the College is connected to the Internet at 1Gb/s this is shared by over 600 connections. Generally, the response times are very good compared to a normal broadband connection. However, it doesn't take many people downloading large files simultaneously to reduce the speed of the network for everyone. Using the Internet for normal web browsing, email and messaging will generally not cause problems for anyone, but other activities can. In the interests of enabling the majority to experience a fast network you are asked to follow the rules and guidelines given here.

5.2 LAN Traffic

All student rooms are provided with and billed for Internet access; this is charged for on a daily basis at the pro-rata rate of £3.30 per week. Although there is no daily download limit it is expected that the average daily traffic will not exceed 10GB/day over the term. Usage is calculated as the sum of incoming and outgoing traffic external to the University.

To avoid accidental excess use you get an allowance which accumulates at 10GB per day. You will receive an email warning if you traffic exceeds the average of 10GB/day and your connection will be limited. This can be over ridden by going to your personal traffic management webpage http://register.l.magd.cam.ac.uk , here you can acknowledge your excess use by increasing the amount by which you can exceed your accumulated allowance and your connection will return to normal. You should return the setting to normal once you have accumulated additional allowance.

It is not expected that anyone will exceed the average of 10GB/day so you will be asked for an explanation if you do.

The following table can be used to estimate the amount of traffic caused by the given activities:

For reference: 1GB is approximately equal to the following activity:

	KB	***MB***	***GB***	***qty***
email no attachments	*7*	*0.007*		*142,857*
email with small attachments	*100*	*0.10*		*10,000*
photos	*3,000*	*3*		*333*
typical BBC webpage	*140*	*0.14*		*7,143*
listening to radio for 1hr @ 64kb/s	*28,800*	*28.80*	*0.029*	*35*
64min podcast from BBC	*30,000*	*30.00*	*0.030*	*33*
BBC iPlayer 50min episode	*500,000*	*500.00*	*0.500*	*2*
BBC iPlayer 30min episode	*300,000*	*300.00*	*0.300*	*3*

If it can be shown that high network usage is required for purely academic reasons then provided this is supported by the student's Tutor a high allowance can be agreed.

A student's network connection will be blocked immediately if it is apparent that their machine has been compromised or is being used for inappropriate activity. The machine will need to be brought to the Computer Office for cleaning before it is allowed back onto the network.

5.3 Copyright Infringement Notice

The University receives notifications from various agencies about copyright material that has been downloaded illegally and passes these to the Computer Office for action. The Computer Office is required to immediately disconnect the offending machine and confirm that all copyright material has been removed. The person who has registered that machine on the network will receive an automatic fine of £50.

5.4 Peer to Peer file sharing

All use of "peer-to-peer file sharing" software for sharing copyrighted music, videos or software is forbidden. Kazaa, eDonkey, Bearshare, LimeWire, iMesh, Gnutella, WinMX and BitTorrent amongst others are of particular concern, as they are mostly used to download and redistribute copyright-infringing music and video material. Other peer-to-peer software such as Skype (see below) can also generate substantial amounts of traffic.
NB. Your total network usage is calculated as the sum of all incoming and outgoing traffic external to the University and all excess of your allowance will be at your expense.

5.5 Skype

This is very popular with many students, however it does consume a large amount of data if the call is using HD video. According to the Skype website:-

The bandwidth required by Skype depends on the type of calls you want to make. The table below provides the minimum download and upload speeds required, as well as the recommended speeds for best performance.

Call type	***Minimum download / upload speed***	***Recommended download / upload speed***
Calling	*30kbps / 30kbps*	*100kbps / 100kbps*
Video calling / Screen sharing	*128kbps / 128kbps*	*300kbps / 300kbps*
Video calling (high-quality)	*400kbps / 400kbps*	*500kbps / 500kbps*
Video calling (HD)	*1.2Mbps / 1.2Mbps*	*1.5Mbps / 1.5Mbps*
Group video (3 people)	*512kbps / 128kbps*	*2Mbps / 512kbps*
Group video (5 people)	*2Mbps / 128kbps*	*4Mbps / 512kbps*
Group video (7+ people)	*4Mbps / 128kbps*	*8Mbps / 512kbps*

This implies a network traffic usage of 1.350GB for a 1 hour HD Video call if it uses 1.5Mbps/1.5Mbps.

5.6 Streaming Audio and Video

Streaming Audio and Video can cause a large amount of data to be transferred into the College network. As a general rule, if the radio station you want to listen to can be picked up on an ordinary radio then this is what you should do. If you can only listen to the radio station via the Internet then you should be selective on what you listen to and not just leave your computer on all day playing your favourite radio station.

5.7 University Rules and Regulations

Any use of the Cambridge University Data Network (CUDN) is governed by the University Computing Service and users are advised to familiarise themselves with these rules and guidelines. **Ignorance of them is no defence** either in law or in University/College-determined jurisdiction. Breaches of the rules will be investigated by the University Computing Service and the Magdalene College Computer Officers will do all they can to assist them. The terms and conditions of use issued by the Computing Service can be found at the following link:

Information Services Policies, Rules and Guidelines -

https://www.uis.cam.ac.uk/about-us/governance/uis-policies-and-guidelines

5.8 Magdalene Rules and Regulations

This section outlines the rules and regulations for the use of the College network.

A standard Internet access charge is applied to all College rooms and is charged for on a daily basis at the pro-rata rate of £3.30 per week. The main purpose of the College network is to assist you in your academic studies, it is not expected that you will exceed an average of 10GB/day over the term, so you will be asked for an explanation if you do.

All use of "peer-to-peer file sharing" software for sharing copyrighted music, videos or software is forbidden.

The University receives notifications from various agencies where copyright material has been downloaded illegally and passes these to the Computer Office for action. The Computer Office is required to immediately disconnect the offending machine and confirm that all copyright material has been removed. The person who has registered that machine on the network will receive an automatic fine of £50.

Always apply the latest security updates for your operating system and other software, which are available from the manufacturers' web pages, for example, Windows updates are available from the Microsoft Windows update web site.

All resources will be allocated to an individual for their use only. Allowing others to use your resources, or using another person's resources, will be treated as a serious infringement of these rules.

All software provided on the public computers in College is the property of Magdalene College and subject to license and copyright restrictions.

Equipment other than personal computers may only be connected to the College network with express prior permission of the Computer Officer.

The College accepts no responsibility for the integrity of any program or data stored on College equipment. The onus is on the individual to backup any data files in their personal disk space.

The use of any College facility to transmit, store or display offensive material is forbidden. This point should be borne in mind if posting to newsgroups in particular.

It is forbidden to use the Magdalene Computer Network as a forum for any commercial organisations.

All users are expected to take reasonable care not to introduce viruses into the network. Anti-virus software must be installed and kept up-to-date. (Refer to the viruses section for further information).

All shared equipment faults should be reported to the Computer Officer. Do not call up the Computing Service, or anyone else directly, as most of the equipment is under warranty or a maintenance contract so that it is important that the correct company is contacted by the College designated authority.

There may be times when the shared machines are required for maintenance, courses, examinations or conferences and access will be restricted accordingly.

No one shall use the computer facilities to hold or process personal data except in accordance with the Data Protection Act.

After working on the shared machines, users must leave the work area tidy for others. Neither the College nor other users can be held responsible for work left behind, either on paper or on USB sticks or any other storage media.

Food and drink may not be consumed in the ACS, Cripps or the Library.

Incidental noise should be kept to a minimum. Most users wish to work in library-type conditions. Noisy or rowdy behaviour will not be tolerated.

The ACS is available for use at any time.

Changes and amendments to these rules may be posted on the notice boards from time to time.

Breaches of these rules will be dealt with by the I.T. Committee or the Dean, as appropriate. Depending on the outcome of any investigation, appropriate disciplinary action will be taken, including the removal of rights to use the College Computing Facilities. Breaches of the University of Cambridge Information Technology Syndicate Rules will be reported to the Director of the University Computing Service.

6 Useful Websites

6.1 Magdalene College Internal Website

http://www.magd.cam.ac.uk/magnet

6.2 University Information Services

The University Information Services website contains a wealth of information of all aspects of computing and services available in the university. The site covers everything from Rules and Regulations, Email, Software sales and Training courses to Printing, Photography, Videoconferencing and Health and Safety.

Here are a few key links;

The University Information Services homepage

https://help.uis.cam.ac.uk/

University Email service

https://help.uis.cam.ac.uk/service/email

Retrieving your CRSID

https://jackdaw.cam.ac.uk/signup

Retrieving your eduroam token

https://tokens.csx.cam.ac.uk/