



University of St Andrews
Scotland's first university

600 YEARS
1413 – 2013

IT facilities a quick guide for staff



June 2011

Contents

- 2 *Help and support*
 - On-line help • Helpdesk • Quick answers • Technical support • Service status
 - Academic support
- 4 *University computer account*
- 5 *Using a computer at the University*
 - The basics • Starting work at the University • Moving to a new office or department • Leaving the University • Visitors to the University
- 11 *Email arrangements for University staff*
 - Email addresses • Storage of email • Shared email accounts • Spam and viruses • Email etiquette
- 15 *Managing your data*
 - Central filespace • Accessing the Central File Store • Backing up and archiving your data • Use of central filespace • Shared space • Web space
- 20 *Wireless connections*
- 21 *Remote access to University network services*
 - Remote access to email and calendar • Other access to network services • Virtual Private Network • The University's dial-up service (SARA)
- 24 *Mobile services*
- 24 *Research computing*
- 25 *Videoconferencing*
- 25 *Students with disabilities*
- 26 *Good working practices*
 - Support that we offer • Network services • Email • Keeping your computer safe • Saving and backing up
- 29 *Data creation*
 - Data standards • Sustainability of (research) data
- 29 *IT training*
- 30 *Legal*
 - Software licensing
- 30 *Conditions of use*
- 32 *Help and support summary*

Help and support

On-line help

The Computer and IT Support pages on the University website give further information and instructions:

<http://www.st-andrews.ac.uk/staff/itsupport>

Other web pages referred to in this booklet can be reached from this web page.

The **iSaint** portal displays 'live feeds' about the computer service, such as current availability of computers in public rooms, system status, etc:

<http://isaint.st-andrews.ac.uk>

Helpdesk

We provide a Helpdesk in the main Library; it is staffed Monday to Friday 08:45 (vacations 09:00) to 18:00.

An *on-line request form* is available via the Computer and IT Support web pages. Otherwise you can send your queries by email to **helpdesk@st-andrews.ac.uk**

If you have problems with your computer account or if you need face-to-face help, please visit the Helpdesk. If you are unable to use the web form or email or to visit the Helpdesk, telephone (01334 46) 3333 – a voicemail system may be in use.

Email messages and messages left on voicemail will be dealt with as soon as possible.

A small number of laptops are available at the Helpdesk for presentation use.

Quick answers

Quick answers are a list of common problems and solutions on topics such as printing or using classroom computers; when the Helpdesk is closed they are displayed on a nearby poster, and are also available on-line via the Helpdesk section of Computer and IT Support web pages.

Technical support for your computer

Computers provided by the University for individual use are either PCs (running MS Windows) or Macs (running Mac OS). We provide support for both types of computer, including purchase, repair and software provision. We have trained technicians who are able to repair University staff computers – please contact the Helpdesk.

Service status

The status of various aspects of the computer service in St Andrews is indicated on a web page (which is updated automatically).

Academic support

We also provide specialised support for research computing, data creation, students with disabilities or special needs, audio-visual and videoconferencing services, etc. See later sections for further information.

University computer account

Your **username and password** give you access to the following services:

- **Unimail:** your **University email** and **calendar** facility
- **password-controlled pages** on the University website, including **administrative material** such as student records, online learning facilities, etc.
- your network **filespace** (also referred to as your *home directory*) held in the University's **central filespace**
- your own **web space:** if you want to create a website for yourself or a research group you can apply for space on the University's main web server
- **iSaint:** a portal giving you access to a variety of University and personal information, such as your Library record, University dates and timetables, student records, online exam papers, etc, as well as 'live feeds' about the computer service
- an increasing number of **external information resources** (previously requiring a separate ATHENS username and password)
- the local **wireless network service** and *eduroam* services elsewhere.

You must keep your password secret. Do not give away or share your password. If you forget it, go to the Helpdesk to get a new one: you will need to provide proof of identity, such as your ID card. If you have given your password away or you think someone else has discovered it, you must change it immediately using the 'password changing page' on the Computer and IT Support web pages, or go to the Helpdesk.

Advice on creation of strong passwords can be found via the Computer and IT Support web pages.

You will sometimes receive 'phishing' emails *pretending* to come from St Andrews, asking you to supply your username and password (for instance to 'update our records' or to avoid 'losing your account'). ***You must not answer these emails!***

We will never ask you for your password.

Using a computer at the University

Almost everyone working at the University today uses a computer on his or her desk and, if you need to use a computer to do your job at the University, one will be provided for you. This may be a new machine or one inherited from a previous member of staff.

The predominant type of computer used by staff in the service units is the Microsoft Windows-based PC. In schools it is a much more mixed situation with a fair number of Macintosh and other systems. During your time at the University you will obtain, use, and dispose of one or more computers. Whether you are starting a job at the University, moving office or department, or leaving the University, there are recognised practices for dealing with the acquisition, moving and disposal of your computer.

The basics

This section summarises the following topics:

- *Hardware* (new or inherited) and *software* (operating system and applications)

- *Network connectivity* (Local Area Network, wireless, etc)
- *Printing*
- *Dealing with data* (backup and archive)
- *Disposal of the computer* (to a new user or for recycling).

Hardware and software

In consultation with Procurement, we have specified a “**standard build**” computer for use in the University, including utilities such as an internet browser, email client and anti-virus software. The standard build allows the computer to be restored quickly to a defined configuration. It can also make use of a central server to update anti-virus software automatically.

We have also developed a “**managed build**”, which is a tightly controlled configuration similar to the set-up in the PC classrooms. In this mode you have little flexibility to change the machine’s set-up but, in return for the lack of flexibility, you see an advantage from increased central management, which improves support for the PCs (by reducing the local effort required) and also security.

If you require a **laptop computer**, we can also recommend a number of suitable laptop PCs; we buy through the national agreement for portable computers.

For further information on all these, please see the Computer and IT Support web pages.

A range of commonly used software is available for installation under site licence: information is available on the Computer and

IT Support web pages. Please see also the later note regarding licences, in the section *Legal*.

For further information on hardware and software options, please see the Computer and IT Support web pages.

Network connectivity

Direct connection: All computers connected directly to the University of St Andrews data network *must* be registered with our systems. Connecting to our data network without proper registration and configuration will lead to unexpected consequences, some of which could adversely affect other users. Any computer with an unauthorised connection will be removed from the network without warning.

Wireless connection: There is a *wireless access* service in most University locations, which you can use if you have a wireless-enabled device. Most facilities are accessible via wireless connection but some are not, notably the public printers. See later main section on *Wireless connections*.

Printing

Printers are, of course, most usefully available locally, and you may find that your school or unit provides local network printers for your use. Contact the Helpdesk if you need help with setting up your computer to access local network printers. A personal printer may be available, connected directly via USB.

Dealing with data

You will have two types of data on your University computer: work-related and personal. While you are working at the University, the data on the computer is your responsibility; so

you should regularly backup and archive your data to ensure its safety and integrity.

- **backup** means taking a copy for *short-term storage* (used to restore data in the event of its loss from your disk)
- **archive** means *long-term storage* (the main intent being to preserve data when it is no longer on current systems)

For further details, see the later sections in *Managing your data*, especially *Central filespace* and *Backing up and archiving your data*.

Disposal of the computer

You should ensure that personal and work-related data are not lost: see also *Dealing with data* above.

- **disposal to another user** (see also the sections above on *Hardware and software* and *Network connectivity*)
When you no longer require the use of a particular computer it must be processed before it is reused. Personal data must be removed from the computer and any existing work-related data must be scrutinised to see if it is required for future use. The computer must then be prepared for the next person's use. Contact the Helpdesk if you require this service.
- **disposal for recycling**
If the computer is to be recycled, and the data present on the computer is required for future use, the data must be copied to some intermediate backup or suitable archive medium. The hard disk drive should then be securely erased prior to the computer being sent to Estates for safe disposal. Contact the Helpdesk if you require this service.

Starting work at the University

Your University computer

Your school or unit will arrange for your computer to be prepared prior to your arrival. The procedures vary depending whether the computer is new or inherited, but in either case your computer will be configured for connection to the University data network and your email client and other relevant software will be set up for your use.

Your own computer

If you have to connect your own computer directly to the University's systems by plugging it into a network socket, the procedure remains the same as stated previously; you must inform us, and your computer must be configured correctly *prior to any attempt at connection*. For occasional or *ad hoc* use on the University network, wireless connection is recommended – see later section on *Wireless connections*.

Moving to a new office or department

Moving office

If you are moving office within the same department you will probably take your University desktop computer with you. If this is the case it is unlikely that the computer will require a rebuild, etc. However you must inform us, and we will visit to reconfigure your computer for connection to the network at its new location. Also, remember to contact the Telephone Office to have your telephone handset and extension number transferred to your new location.

Moving department

If you are moving department it is unlikely you will take your University desktop computer with you. You will probably have a “new” computer provided for you. If so, the procedure is as explained in the section *Starting work at the University*. And it will be your responsibility to *back up or archive any personal data* present on your present University desktop computer prior to your move, just as for *Leaving the University* (see below).

Leaving the University

When you leave the University it will be your responsibility to back up or archive any personal data present on your University desktop computer prior to your departure. The University is not responsible for your personal data, and we will not back it up for you. Whether the computer is reissued or recycled *its hard disk will be securely erased prior to reassignment*.

For further information on ensuring that personal and work-related data are not lost, see the later section (in *Managing your data*) on *Backing up and archiving your data*.

Visitors to the University

From time to time you may need to provide computer facilities for a guest, such as a visiting research colleague: there are special arrangements available, for visiting members of other academic institutions (including special local computer accounts) and also for access to local wireless networking (see later section on *Wireless connections*). Conference accounts are also available.

See also the section on *Videoconferencing*.

Email arrangements for University staff

Your colleagues will assume that you read your email regularly, and students expect (and are expected) to communicate with staff by email. You are allocated an individual email account, access to which is controlled by your personal username and password.

The University provides an email and calendar system (Unimail) based on a remotely hosted Microsoft Exchange server, which can be accessed in full using the Outlook client (currently version 2010 for PCs and 2011 for Macs). There is also an Outlook web-based client, Outlook Web App (OWA), allowing access to your University email and calendar from anywhere in the world; see the later section on *Remote access to University network facilities*.

Email addresses

Your email address is in the form: *xxx@st-andrews.ac.uk* – use your own username in place of *xxx*.

You can find out other University users' email addresses from the University directory. In Outlook this is accessible via the Address Book or Contacts Search facility (this may be triggered automatically when you're composing an email and type a contact name).

Storage of email

Unimail provides you with 3GB of filespace, to hold a mailbox for incoming messages and folders where you can store messages after reading them – you are advised to organise your messages in suitably named folders within this filespace.

For your own sake you should keep your incoming mailbox as small as possible, otherwise it will become unwieldy and likely to cause problems for you. You can keep it small by reading your mail frequently, deleting unwanted messages and filing the rest in folders.

The Outlook email client is configured to use Microsoft Exchange. Your mail folders are automatically backed up centrally, and will also be easily accessible from different locations – for example, from home or elsewhere, via a web browser using the Outlook Web App.

Shared email accounts

In addition to your personal email account you can arrange to have a non-personal account. This should be used when more than one person needs to be able to access the messages. In some cases the mailbox is shared regularly, for example when several people share a job. In other cases only one person regularly accesses the email, but others need access when the usual recipient is absent. Sharing of email is eased by central storage of messages, which enables them to be accessed from more than one location or by more than one user.

When messages are sent to you as the holder of a particular post rather than in your personal capacity it is important that such messages should not languish in your personal mailbox

when you are absent. They should therefore be sent to one of these shared, non-personal email accounts. You can encourage this by advertising the address associated with your post or function, and by using it as the “return address” when sending mail.

In emergencies, where messages of importance to the University are believed to be held in an absent staff member’s personal mailbox, the Principal’s Office may, *exceptionally*, authorise us to give other members of staff access to the absentee’s mailbox.

Spam and viruses

MailScanner and SpamAssassin software is used to check all incoming and outgoing email for spam and viruses.

The University inevitably attracts a huge quantity of unsolicited email (*spam*). Many staff users now opt to discard all messages identified and marked as {Spam?} by the mail server, accepting the small risk of losing genuine messages. This can be done using the filtering function in Outlook.

If you receive a message that MailScanner believes contains a *virus*, the infected file will be stripped out of the message and placed in quarantine. When this happens you will receive a warning message. Sometimes (very rarely) MailScanner wrongly identifies a genuine message as containing a virus. If this happens and you want to re-claim the file that has been wrongly quarantined, you should forward the *entire warning message* to the Helpdesk.

Email etiquette

Be tactful when composing messages; be aware of the possibilities for misunderstanding. Sending abusive emails is regarded as a serious offence and may lead to disciplinary action.

Think twice before forwarding an email to a third party; would the writer be willing to have it forwarded? If you reply to a message and copy your reply to a third party you are in effect forwarding the original message.

Avoid sending very large attachments by email. Be aware that they can cause inconvenience for the recipient and may even be blocked en route. If you need to send a file of more than a couple of megabytes it is worth checking with the recipient beforehand. Within the University, you should instead consider uploading the file to a place (such as shared filespace) where the recipient can download it conveniently – this is particularly true if you are intending to send the same large file to several recipients.

Do not send mass unsolicited emails except to a mailing-list established for a specific purpose; in that case, the message must be relevant to the mailing-list and *must not contain attachments*.

Managing your data

Different members of staff have widely different data-storage requirements. How you manage your data depends on what sort of data it is, how volatile it is, how important it is, how sensitive it is and how long it needs to be kept. Any general advice must be adapted to fit your specific needs.

The University's Freedom of Information Officer is available for consultation on both the legal and practical aspects of records management, and on matters such as file-naming conventions. The Arts Computing Adviser is able to advise on matters relating to the long-term sustainability of research data. If you have queries that go beyond the general advice given in this booklet, please contact the Helpdesk, who will refer you to the relevant expert.

As a general rule, information (in email or in documents of any kind) should not be retained longer than necessary. You should develop a retention and deletion plan for different categories of information.

Central filespace

Members of staff have a quota of at least 5 GB (gigabytes) on the University's Central File Store (CFS). This is to accommodate documents or data that you keep on the CFS. *You are recommended to keep all your important University data in your filespace on the CFS.*

Remember that *your email is stored separately* in your mail folders in filespace within Unimail (with a limit of 3GB).

To put a gigabyte in more manageable terms, it will accommodate 10,000 reasonably sized (100KB) Word

documents, or 500 medium sized (2MB) image files. If you regularly create very large documents (for example documents containing images or equations) or if you deal with high quality, very large image files, then naturally the number of documents and images that you can store will be reduced. Many academic staff will also need to store large datasets in connection with their research.

It is recognised that many members of staff will require a larger allocation of space on the CFS, and an increase to 10GB can be had on demand. If you require substantially more than 10GB you should contact the Helpdesk to make a case for a larger quota.

You can check your quota and your current usage via a page available on the Computer and IT Support web pages.

Accessing the Central File Store

Your space on the Central File Store can be accessed from your own computer – or from elsewhere – in the following ways, all of which require you to enter your username and password. You will need to be *connected within the University network*, either directly or via a Virtual Private Network (VPN) – see later section on *Remote access to University network facilities*:

- *map a network drive* (Windows) or *connect to a server* (Mac OS), using the *samba* protocol (here xxx is your username):

Windows: \\nexus\xxx

Mac OS: smb://nexus/xxx

- use FTPES (Explicit FTPS or secure File Transfer Protocol over TLS/SSL) to log in to ftp.st-andrews.ac.uk by means of an FTP client that supports TLS/SSL (such as FileZilla or Fetch): this

method may be used also for accessing your own web space (see later section on *Web space*).

Backing up and archiving your data

You are responsible for ensuring that your email, documents and other University data are all securely backed up. If your data is on your local hard disk you will need to make a copy onto some secure media, such as CD, DVD, tape or external hard drive. Of these, CD and DVD are recommended only for short- or medium-term backup (up to two years).

Backup: Backing up your data means to take a copy for *short-term storage*. You should use this method to ensure that working copies of your current (or active) files are kept safely. There are a number of ways to do this: copy to recordable CD or DVD, copy data to a network drive, or use the standard Windows or Mac OS utilities supplied for backing up.

Data held on the Central File Store is backed up daily by us. This means that files in your home directory are secured against any disk failure or corruption that may occur. You are recommended to keep all important University data in your network filespace on the CFS. If you map your filespace as a network drive (as described above) you can use it as the primary location for saving your work, using the **Save** or **Save As** command in MS Word or other applications. On the whole this is the easiest way of ensuring that your documents are backed up. Alternatively you can work on your local hard disk, and then copy documents across to your network filespace as a secondary location.

Archive: Archiving is used for *long-term storage*. You must take into account the archive medium and the methods used for

writing the archive. Proprietary backup software can change over time, so you should use tried and tested archival methods and avoid using data compression. Similarly, careful thought should be given to the archive medium. Recordable CDs and DVDs may be convenient but, because they degrade with usage and time, they should not be considered as suitable media for long-term storage: *checks and copies should be made on a regular basis, to ensure that the data remains readable.*

If you need advice on any of the above please contact the Helpdesk.

Use of central filespace

When you use your network filespace, bear the following points in mind:

- Although you can have a large allocation of space on central filespace there will always be a limit: you can't expect to back up everything from your computer's hard disk onto central filespace. Keep an eye on your disk quota.
- Don't back up your applications or operating system software: if software is deleted or corrupted you should re-install it from the original installation media.
- If data is no longer 'live' you should consider removing it to an archive medium such as magnetic tape or optical media (CD or DVD). Note that data stored on optical media will need to be refreshed (copied onto fresh disks) every year or so, and that all media formats become obsolete and eventually impossible to read.

Files that you accidentally delete or modify can be restored, subject to certain important provisos:

- *Restoring files from backup is a time-consuming business, and you should only ask for files to be restored if they are of importance for your work. Don't ask to have a file restored from backup if you can easily recreate it or if you have another copy or if it is easily downloadable from elsewhere.*
- *The backup tapes are only kept for four to six weeks, so if data in your network filespace was lost or corrupted longer ago than that it will not be possible to restore it from backup.*
- *You may be able to restore a file if you have overwritten it with a more recent version, but not if you have both created and deleted it between daily backups.*

Shared space

Schools and units can apply for **shared filespace** ("share") on the Central File Store (CFS). This can be divided up into a main group share plus a number of sub-groups. Every group and sub-group share must have a designated "responsible" person who will be the point of contact in dealings with us, and who will also ensure that their group and/or sub-groups are used responsibly, and that requests for changes are sent through them. This filespace will usually be accessed by mapping the shared space as a network drive on your PC or Mac, as described above in *Accessing the Central File Store*. Further details are available on the Computer and IT Support web pages.

Web space

Institutional web pages are managed centrally using Terminalfour's Site Manager software. Each school and unit has one or more staff members who are responsible for the school or unit's web presence, and if you have questions about your

school or unit's web presence you should address them first to these colleagues.

In addition, staff are entitled to create web pages for themselves or for groups with which they are associated. You can apply to the Helpdesk for space on the University web server for yourself or for a group. This space may be accessed using a suitable program, with a secure FTP (File Transfer Protocol) facility such as FTPES (see earlier section on *Accessing the Central File Store*). The integration of your personal or group web pages within your school or unit's web representation is something you should discuss within your school or unit.

Wireless connections

There is a *wireless access* service in most University locations, which you can use if you have a wireless-enabled device. Most facilities are accessible via wireless connection but some are not, notably the public printers.

Wireless connections use the *eduroam* service: when you visit a participating institution, using eduroam you can log in to that institution's wireless network with your St Andrews username and password. Software and instructions for setting up your laptop to use eduroam are available via an open wireless network (*uos-connect*). See also later section *Other access to network services*.

Remote access to University network services

Home broadband, and Internet connections in hotels (as well as wireless facilities in airports, trains, etc) now make it much easier to access the University network and facilities remotely. We cannot guarantee to support every form of remote working, but there are a number of things that have been tried and found to work. Please check Computer and IT Support web pages for current on-line information about broadband support.

Remote access to email and calendar

Since your University email and calendar are centrally stored, you can access them from any network computer with a web browser, via Unimail using the Outlook Web App (OWA). Instructions for using Unimail and the OWA are available on the Computer and IT Support web pages. You can also read and send your mail from any computer with a suitably configured IMAP (Internet Message Access Protocol) email client, but that doesn't give you access to your calendar.

If your hand-held device can connect via Microsoft Exchange ActiveSync you may be able to access your University mailbox and calendar by this method. Failing that, you should be able to reach your mail and calendar via your device's web browser using the OWA, or connect to your mailbox (but not your calendar) via IMAP.

Other access to network services

If you connect to the Internet from another institution or by using a commercial Internet Service Provider (whether by broadband or wireless or dial-up) then your access to the University facilities will be restricted and controlled, for obvious security reasons.

If you connect to the University wirelessly from another participating institution via *eduroam*, similar restrictions will apply.

Special steps are required if you want to access the following services from outside the University network, as follows:

- **Sending email from your St Andrews email address using an email client other than Outlook Web App (as above):**

You should configure the email client to use our secure SMTP server and you may need VPN access – see section below on *Virtual Private Network*. *If you attempt to use the secure SMTP server without VPN access, then:*

— *use of secure SMTP may not be permitted by your ISP*

— *your attempts to connect (and so relay email) via our secure server may be rejected; blacklists of spam sources supplied to us (under contract from JANET) include IP address ranges that ISPs use for broadband and dial-up.*

- **Access to your network filesystem:** this requires VPN access – see below.
- **Access to the University's web cache:** this also requires VPN access – see below.

If you set up a VPN (see the section below on *Virtual Private Network*) you will be able to access most licensed Library material through the University's web cache without needing a password; you will also be able to send email through our main mail servers.

Virtual Private Network (VPN)

A VPN connection is equivalent to a *direct* connection to the University network. To set up a VPN, you need to download, install and configure the Cisco VPN client. You can download the installation file from the Computer and IT Support web pages, where you will also find full instructions. We support versions of the VPN client for Windows and Mac OS.

When you need to access a service requiring a VPN connection you should run the Cisco client and connect using your username and password. The Cisco client has been found to work with most common broadband providers. There are compatibility issues with some firewall and anti-virus software.

The University's dial-up service (SARA)

When you don't have access to a broadband or wireless or other ISP connection, you can connect remotely to the University's network using a modem, via a dial-up telephone connection to the St Andrews Remote Access (SARA) service. Dial-up access is limited to a maximum speed of 56Kbps, or 9.6Kbps if connecting to SARA using a mobile phone. SARA gives you unrestricted connection *directly* into the University network, and so *Virtual Private Network (VPN) facilities are not required in this case.*

Mobile services

If you have a need to communicate using University systems while on the move, we can offer support for a range of mobile communications solutions, including the use of mobile phones and smartphones. Using these devices you can keep up to date with your calendar, email accounts, web browsing via *eduroam* networking and the Internet, etc.

*Not all mobile devices will interface successfully with our systems, so it is important to discuss your needs with us **before** making any purchases.* Likewise, it may not be possible to use your own mobile device with our systems. More information is available on the Computer and IT Support web pages.

Research computing

The Arts and Humanities computing team provides a liaison service to all schools in the Faculty of Arts and provides advice on all aspects of electronic resource creation. This includes assistance with technical aspects of applications for public funding, project management, digitisation issues, hosting and electronic archiving.

We are providing dedicated hosting service and are currently developing an electronic archive for the long-term preservation of local publicly-funded electronic resources in the Arts and Humanities. University of St Andrews Arts and Humanities computing projects, along with advice on this area of computing, are located on a dedicated server, the Arts Research and Teaching Server:

<http://arts.st-andrews.ac.uk>

Videoconferencing

Videoconferencing may be described as a method of holding a meeting or conference between two or more geographically separate locations where both sound and vision are conveyed electronically so as to enable simultaneous interactive communication.

We maintain a number of videoconference facilities in the University, with one in St Mary's College available for booking by any member of staff via the JANET Videoconferencing Service (JVCS) where it is identified as `marys-lr3@st-and.ac.uk`. For further details about the JVCS see:

<http://www.ja.net/services/video/jvcs/>

First-time users should contact the Helpdesk for further information and help.

Students with disabilities

The IT disabilities support advisor can be contacted via the Helpdesk. We provide a reserved computer room for the exclusive use of students with disabilities and other special needs. An Alternative Format Suite (AFS) facility is able to produce learning material in a form suitable for such students. For these facilities, students should be referred to Student Services (in the Students' Association).

Good working practices

These are guidelines and advice on good working practices, some of which are practical and some legal or standards-based; most are liable to change over time. For latest information and advice on-line check the Computer and IT Support web pages, and also the University's Policy and Governance web pages.

Support that we offer

We do not have the resources to support everything computer-related: whenever possible, you must use the hardware, software and network services supported by us.

If you install hardware or software other than that recommended by us on your own equipment *you must be prepared to manage and support this yourself.*

Network services

For security and efficiency, our network infrastructure and servers require central management, which we provide: *you must not set up unauthorised servers or connect unauthorised equipment to our network.*

Email

See the earlier section on *Email arrangements for University staff*, and note in particular the section there on *Email etiquette*.

Keeping your computer safe

Physical security

If you leave your computer unattended you should try to secure it from unauthorised access. If possible lock your room when

away from it. If you share a computer you should always log out of your account before your colleague uses the computer.

Electronic security

- Never open an attachment you do not recognise
- Always be vigilant when downloading files
- Never visit disreputable websites
- Set a secure password on the administrator account on your PC

You should always keep your system up to date by downloading *security patches* from your operating system supplier (eg, Microsoft or Apple). If you have no anti-virus software on your PC, you should download and install a copy of F-Secure, for which we hold a site licence. Virus definition databases are regularly updated and must be downloaded frequently (every one or two days).

Mac users may obtain a copy of Norton anti-virus from Symantec; there is also a free anti-virus tool for protecting Intel Macs running at least MacOS 10.5: PC Tools iAntiVirus from <http://www.iantivirus.com>

Passwords

Your **University username and password** allow you to access your email via SaintMail, your *home directory* on the University's central filespace, and certain restricted University web pages and systems. You are responsible for the use and security of this account.

You must keep your password secret. Do not give away or share your password. If you forget it, go to the Helpdesk

to get a new one: you will need to provide proof of identity, such as your ID card. If you have given your password away or you think someone else has discovered it, you must change it immediately using the 'password changing page' on the Computer and IT Support web pages, or go to the Helpdesk.

Make your passwords as difficult as possible to crack: do not use real names, car registration numbers, etc.

On your own computer, never use your University account password for your personal or administrator-level computer logins and, wherever possible, do not set administrator privileges on your own computer account.

Advice on creation of strong passwords can be found via the Computer and IT Support web pages.

You will sometimes receive 'phishing' emails *pretending* to come from St Andrews, asking you to supply your username and password (for instance to 'update our records' or to avoid 'losing your account'). ***You must not answer these emails!***

We will never ask you for your password.

Saving and backing up

While working on a document, save your changes frequently. Unless you are saving the document in your home directory you must make a backup copy at the end of each day's editing session. Avoid overwriting the previous day's version by giving each day's version a different filename. See the section on *Managing your data* for more advice on backups.

Data creation

Data standards: text, images, video, sound

If you are creating research, teaching or administration data, it is essential that such data conforms to accepted standards that we support.

Sustainability of (research) data

If you or others need access to your data in years to come, the data must be created in a manner that is sustainable. This involves the use of open standards, proper documentation, suitable storage media and appropriate data management at all times.

This consideration is particularly important for research data. For further information, contact the Helpdesk.

IT training

There are a number of IT training courses that are open to University students and staff. Some of these courses are taught by our staff; other courses are available on-line and you can work through them in your own time.

To find out more, see the section on training in the Computer and IT Support website, or email **it-training@st-andrews.ac.uk**

Legal

The University has policies and guidelines to ensure that it complies with all current legislation: see the University's Policy and Governance web pages. When creating *printed* or *on-line* documents or other media, you must not use copyright material (whether text, images, video or audio) *without licence or **written** permission from the copyright-holder*. Any documents, web pages, etc. must comply with current legislation, e.g. Copyright, Designs and Patents Act, Freedom of Information (Scotland) Act, Data Protection Act, Special Educational Needs and Disability Act (SENDa), etc. Refer to the University's Policy and Governance web pages for further information.

Software licensing

All software used on University-owned computers must be fully licensed for use in an educational environment. Many software manufacturers have concessionary prices for staff while employed by the University. We can advise on this, but purchases usually have to be made by individual staff through commercial re-sellers.

Conditions of use

The conditions governing the use of computers in the University are published on-line: see the University's Policy and Governance web pages. The terms relating to copyright, data protection and freedom of information are particularly important.

You must use your computer account responsibly. *Your computer account may be withdrawn either temporarily or permanently if you do any of the following:*

- divulge your University computer password
- fail to keep your anti-virus software, operating system and application patches up-to-date
- send abusive emails or unsolicited mass emails ('spam')
- generate excessive network traffic by downloading music or movie files
- probe or otherwise attempt to hack into any computer either within or outwith the University network
- download or disseminate pornographic or racist material unless it is *authorised* as part of your academic study
- copy or distribute copyright material without the authorisation of the copyright owner
- set your own computer up as a server offering web, file-transfer, file-storage or other services, whether or not this is done for profit, unless you have explicit permission from the University's Chief Information Officer.

The above list is not an exhaustive statement of the conditions for using the University's computer network. A full statement is available on University's Policy and Governance web pages. Apart from infringing the University's rules, **some of the activities listed may also incur a legal penalty.**

Help and support summary

On-line help:

<http://www.st-andrews.ac.uk/staff/itsupport>

Web pages on other topics (such as the Helpdesk) are available via this page.

The **iSaint** portal displays 'live feeds' about the computer service, such as current availability of computers in public rooms, system status, etc:

<http://isaint.st-andrews.ac.uk>

IT Helpdesk:

On-line request form available via Computer and IT Support web pages – see above.

Email: helpdesk@st-andrews.ac.uk

Telephone: (01334 46) 3333

Quick answers:

Available on-line via the Helpdesk web page – see above.



University of
St Andrews

IT Services, University of St Andrews,
St Andrews KY16 9AL

The University of St Andrews is a charity registered
in Scotland. No: SC013532.