IT Acceptable Use, Security and Best Practice of I.T. and Telecommunications Equipment Policy for Staff and Students

GUILDHALL SCHOOL

This policy is of relevance to students, staff and visiting students/ staff

Approved on	June 2017
Approved by	Operations Board
Written by	Richard Antonel IT Department
Version No.	v3.2 July 2021
Last Reviewed	
Last Amendment	Minor amendments: DPA references updated to 2018; staff password policy updated; eduroam and DirectAccess laptops added
Date of last amendment	May 2021
Publication Status:	Sensitive – this policy contains excerpts and is derived from the School staff handbook which is not a public document.

Table of Contents

Table of Contents

0. Abridged Policy for External Use/ WiFi Usage for visitors

The Guildhall School's computer (information technology), telephone and other communications systems are provided to assist staff in the performance of their jobs and all eligible students at the School in the pursuance of their studies and research. All users of information technology at the School including *eduroam* visitors must abide by this policy and any related rules and standards.

0.1 End User Agreement (Abridged)

Accessing the IT systems or parts thereof assumes acceptance of the following Acceptable Use Policy:

This system may not be used for any of the activities described below:
Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
Creation or transmission of material with the intent to cause annoyance, inconvenience or anxiety.
Creation or transmission of material with the intent to defraud.
Creation or transmission of defamatory material.
Creation or transmission of material such that this infringes the copyright of another person or persons.
Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of a service to which the user or their user organisation has chosen to subscribe.
Deliberate unauthorised access to networked facilities or services.
Deliberate activities having, with reasonable likelihood, any of the following characteristics:
Wasting staff effort or networked resources, including time on end systems accessible and the effort of staff involved in the support of those systems;
Corrupting or destroying other users' data;
Violating the privacy of other users;
Disrupting the work of other users;
Denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment);
Continuing to use an item of networking software or hardware after the system administrators have requested that use cease because it is causing disruption to the correct functioning of this system;
Other misuse of the system or networked resources, such as the introduction of "viruses" or other harmful software.
Connecting any unauthorised hardware to the system not via the wireless system itself.

1. Full Policy - Definition of "Acceptable Use" and "Information Technology"

The Guildhall School's computer (information technology), telephone and other communications systems are provided to assist staff, students and eligible visitors in the performance of their jobs, studies and research. All users of information technology at the School must abide by this policy and any related rules and standards.

Information technology encompasses all computing and communications facilities and services provided by the School's I.T. department including voice-mail and telephone services, computers, networks, email, accounts and storage, software, web pages and websites and internet access.

In the use of information technology, Guildhall School students and staff are required to meet expectations and standards of professional and ethical behaviour that go beyond the requirements of law. These standards and an expectation of "acceptable use" are designed to help achieve both a positive teaching, learning and working environment in which all persons treat each other with dignity and respect and the effective and efficient operation of information technology resources so not to lead to performance problems, inconvenience to others and expense to the School, particularly in terms of lost productivity.

1.1. Applicable Laws

Laws that are applicable to the I.T. systems at the School are:

- Data Protection Act 2018 (GDPR)
- Copyright Designs and Patents Act 1988
- Human Rights Act 1998
- Computer Misuse Act 1990
- Regulation of investigatory Powers Act 2000
- Freedom of Information Act 2000
- Electronic Communications Act 2000
- Digital Economy Act 2017
- And any regulations made pursuant to these Acts

1.2. Eligibility to Use IT Services

1.2.1 Staff

Staff or contractors must not use a School system unless it is specifically part of their job. Neither should they assist anybody to make unauthorised access.

1.2.2 Students

Only students authorized by the School's Registry department are given access to the systems at the School. Students should not assist anybody to make unauthorised access to systems. I.T. privileges may be removed as a result.

1.3 Prohibited Use

Examples of prohibited use of the School's systems include, but are not limited to:

- Attempting access to systems for which the user is not authorised
- Sending messages or holding data which are illegal, likely to cause offence or to
- bring the School into disrepute
- Using vulgar or obscene language in that context
- Accessing, displaying or disseminating pornography
- Sending information that may tend to disparage or harass others, for example on ○ the grounds of sex or sexual orientation, race, nationality, ethnic origin, colour, ○ creed, disability, marital status, age, trade union or political beliefs
- Divulging confidential material to unauthorised third parties Distributing junk mail, fund raising requests or chain letters Loading or using unauthorised software:

    - You must not copy or take School software, including other licensed software for your own use. All software must be run within the terms of its license.
    - Examples of specific activities that are not permitted include…downloading, using or distributing software or executable programs without checking it with IT Staff.

- Soliciting or carrying out business activities for personal gain
- Excessive participating in non-work related chatrooms/ forums
- Downloading or playing computer games
- Connecting unauthorised equipment to the School's network for example wireless access points or routers or switches
- Using unauthorised screensavers or wallpaper

1.4 Occasional Non-employment related use – Staff

It is recognised that incidental and occasional use by staff not strictly on School business can be permitted to a small degree. Such use must not be habitual or frequent and must not contravene any aspect of the School's policies. It should not be done in working time and the cost of materials used (e.g. paper and other consumables) may be reimbursable to the School. In the event of any doubt, the user must confirm in advance with their departmental line management the permissibility of any such personal use.

Acceptable Use by staff therefore must not:

- Interfere with institutional business (i.e., teaching, learning, research, and administration);
- Detract from an employee's availability to carry out his or her assigned responsibilities;
- Damage the School or its reputation; or
- Compromise the integrity and efficiency of the institution's information technology facilities and services.

1.4.1 Use for Other Commercial Purposes

Use of School information technology systems and resources for commercial purposes or for the benefit of organizations not directly affiliated with the School is forbidden without the written consent of the Principal or Head of Finance and Business Administration. This includes, but is not limited to: any advertising on web pages or via e-mail or news postings; any solicitation of funds, goods, or services for any purpose; and processing or transmission of data on behalf of a third party whether a fee is charged or not.

All personal and approved commercial use of information technology resources has the same status as institutional use and is subject to the same expectations regarding legal and acceptable use.

1.5 Reporting possible illegal and unacceptable use

Employees and Students should report to their line manager or programme leader all suspected illegal or unacceptable use of information technology resources. Directors shall forward reports of possible illegal or unacceptable use to either the relevant Director (in the case students) or the Director of Finance and Resources or HR Manager (in the case of staff and contractors). In the interests of efficiency, tutors can report cases of possible illegal or unacceptable use of information technology by students directly to the Head of IT, with copies to the head of their department.

1.5.1 Obligations and Authority of Information Technology Staff

Employees who support the information technology infrastructure are expected to use information technology appropriately, respect the privacy of others and maintain the confidentiality of information that may come to their attention during the routine exercise of their duties.

Information technology employees will ascertain and release information that is normally confidential only when specifically requested to do so according to the provisions of this and other relevant policies.

In situations where there is an immediate threat to the integrity and availability of the School’s networks and data systems, information technology staff have the obligation and authority to take the measures that they, in their professional judgment, think are necessary to secure the networks and systems for general use, even if this means denying access and causing loss or inconvenience to some users.

The School’s Head of IT has the authority to take any measures pertaining to secure and protect the networks and systems, including imposing permanent user disconnections and bans.

2. Passwords

Users should follow good security practices in the selection and use of passwords. All users must adopt the following guidelines for allocating and managing their passwords:

- Only use your own password to access a system.
- Keep passwords confidential.
- Avoid obvious passwords e.g. family names, initials, days of the week and so on.
- Mix alpha and numeric characters, upper and lower case.
- Change passwords at regular intervals and avoid re-using or cycling passwords.
- Change passwords whenever there is any indication of possible system or password compromise.

2.1 Passwords for Staff

Staff may use the OneLogin portal to change and reset their passwords.

2.2 Passwords for Students

Students may use the OneLogin portal to change and reset their passwords.

3. Network Security

Unauthorised use of systems, equipment, internet and email

Only authorized persons are entitled to access, connect to, monitor, use, copy, modify (including encrypt), or destroy any of the School's data, passwords, computers, storage devices, programs, systems or parts of the network; if in doubt about your authority, contact the IT department. Contravention of these rules may amount to a criminal offence under the Computer Misuse Act 1990, and employees may also face disciplinary action.

The following are specifically prohibited: attempting to access restricted areas of the network; accessing information which you know or ought to know is confidential; accessing the communications or data of any other user without their authority; connecting unauthorized devices (i.e. anything not supplied by the School) to the School's equipment or its wired or wireless network including the in the Halls of Residence; introducing packet sniffing software, network discovery tools, any type of spyware or monitoring software; and using any software not supplied or authorized by the School; rebroadcasting a WiFi signal or connecting or disconnecting network equipment.

3.1 Saving Data

Data created or used on computer systems at the School should *never* just be saved to local disk drives or USB devices of any PC or computer workstation. Always save data on the designated network drive.

3.2. Unattended PCs

3.2.1 Staff:

Users should not leave PCs logged in while unattended for long periods. A standard, password protected screensaver is implemented to protect users from issues arising therein. This will automatically activate after 15 minutes of inactivity on staff systems. This

is a mandatory requirement and cannot be bypassed. Staff should always log out of their computers once a day when finished using them. Computers should not be left logged on at the end of the work day as this prevents security updates being applied to them.

3.2.2 Students

Conversely, students should not lock workstations such that other students cannot use them. However students should also remember to log out after their sessions are finished.

3.3. Viruses

Viruses are programs designed to destroy data and systems and are introduced via emails, the internet and disk drives.* The School has in place automated processes for regular virus checking, but you should never use a disk, access an internet site, or open an email attachment unless you are sure that it is work related and free from the risk of virus infection. If you suspect an infection you should report it immediately to the I.T. Helpdesk and take no further action unless instructed.

3.3.1 Terminology

*The term “disk drives” above now includes ’mobile devices’ such as mobile phones, Smart Phones, iPhones, laptops, memory sticks, flash drives and other mobile media as these are all capable of holding data.

3.3.2 Staff

Staff must not ordinarily accept flash drives or USB drives from students unless they are familiar with the operation of the anti-virus software on their PCs in respect of knowing how to scan the diskette for viruses and knowing what to do in the event of an issue. Failure to do so could lead to an infection of the staff systems here at the School and could render them liable for any occurring damages or data loss.

The School has identified USB drives and flash drives and other removable hard drives as a high virus risk. There is a risk to the corporate network when data is synchronised as it is not virus scanned. The issue of laptops and such drives to staff will therefore be kept to an absolute minimum.

3.4 Advice on Data Security

The term “sensitive data” is used in this document to refer to any data which if lost or disclosed inappropriately, would cause embarrassment to or damage to the reputation of the School or where such loss or disclosure would cause the School and/or individual responsible for the data to be in breach of any legislation applicable to it, notably the Data Protection Act.

The security of data is a critical factor for any organization and the transfer of data onto mobile devices or storage media such as discs is considered the “weakest link”. The consequences of losing such data could include harm to individuals and action under the Data Protection Act, financial loss and considerable reputational damage.

School data could be held on a range of mobile devices and the risks associated with such a device or media being lost or stolen includes: -

- Exposure of data which could cause damage or distress to individuals (e.g. children and vulnerable adults).
- Breach of regulatory rules (e.g. Data Protection Act 2018).
- Exposure of security information such as disaster recovery plans (e.g. held by key users on USB sticks).
- Exposure to social engineering / identity theft / hacking risks.
- Exposure of financial data (e.g. high level financial policy including grants, fees).
- Exposure of other confidential information (e.g. related to the formulation of policy)

The School has identified USB drives, flash drives and removable hard drives as a high security risk. Although such devices are in use by staff *they must not be used to store any data that could be commercially or legally sensitive* because loss or theft of the item could result in its data being stolen. To this end corporate laptops have their hard drives encrypted. Only School laptops are permitted to connect to the School's corporate data network. USB devices should also be encrypted when used with Staff PCs.

3.5 General Advice to be followed

- Wherever possible, avoid putting sensitive data onto removable media (both data in transit and mobile devices). Where this cannot be avoided, the data must be the absolute minimum necessary. Loading large databases on laptops or memory sticks should not be undertaken.
- Departmental management teams should consider the issue of mobile data security and have a clear understanding of their department's needs and practices.
- Users should keep abreast of School polices and training regarding mobile data security.
- A risk analysis should be conducted before the transfer of sensitive data to mobile devices or media are undertaken. Including: -

    - Does the user have legitimate access to the data?
    - Is the data judged too sensitive to risk leaving the physical confines of School premises?
    - What would the impact should the data be compromised?

    - What would be the impact on individuals (members of the public, or employees) should the data be compromised?
    - What is the likelihood of compromise occurring?

- The appropriate level of management agreement should be obtained prior to transfer of sensitive data to a mobile device or media. This should be done through drawing up a risk analysis document.
- Additional security measures will be required for high risk data where, for example, encryption of a laptop is mandatory.
- Users should not use USB drives or memory sticks which have no encryption protection applied to transport or store corporate data.
- Users should not email sensitive data to their personal email accounts.

- If you do work locally on a file, copy it back to the server it belongs on and then delete the local copy.
- Remember that as well as the copied file, Word and other applications will make and keep backup and temporary copies of the file - ensure that these are deleted as well. Users should not download or store sensitive data on their own personal devices.
- If a mobile device is shared, the user must ensure that his/her data is deleted after use.
- When a mobile device is no longer needed, it should be returned for all data to be removed.
- All media such as DVD discs and backup tapes which are no longer in use should be destroyed, so that data cannot be read from them.
- Users should ensure, as far as possible, the security of a mobile device when off site. For example, laptops should not be left in an unattended vehicle. When the laptop is in the user's home it should be stored in a secure place and out of sight. The loss of any media or device should be immediately reported.

3.5.1 A Quick List of Do's and Don'ts

- **DO** - Use the secure remote access facilities where possible as this avoids the need to remove data.
- **DO** - A risk assessment on all data you intend to remove.
- **DO** - Delete all copies of files held on local and removable storage.
- **DO** - Use encryption software on laptops where appropriate.
- **DO** - Use a secure USB or removable disk drive where appropriate.
- **DO** - Report any loss or compromise of data.
- **DO** - Return all IT equipment for secure disposal.
- **DON'T** - Email data to insecure personal email addresses.
- **DON'T** - Allow relatives or friends to access data held on your work computer.
- **DON'T** - Use a home wireless network unless it is securely configured.
- **DON'T** - Dispose of personal computer equipment without first securely erasing all data.
- **NEVER** - Remove high or very high risk data without first discussing with your Departmental Manager.

4. Email Usage Guidelines

4.1 General Guidelines

The School provides an e-mail facility for staff and students. It is recommended that all new staff are formally trained in the use of e-mail and to this end ad-hoc courses can be provided by the Guildhall School IT department though line manager request.

4.1.1 Security

Security, including protection from phishing emails and viruses, is a concern with e-mail use. Access to e-mail is restricted to authorised users. Staff are responsible for the security of their own passwords which protect against unauthorised access to their workstations.

4.1.2 Sending Mail

Use e-mail instead of sending a paper memorandum but bear in mind the requirements of your department for authorisation, the circulation of copies and record keeping.

Use e-mail instead of sending or leaving a message or note - an e-mail message is much less likely to get lost than a scrap of paper. Use e-mail instead of a phone call requesting or supplying straightforward information. The recipient will be able to deal with your enquiry when it's convenient and you will have a written record.

E-mail should be considered an insecure method of communication so think carefully before transmitting confidential information. Mail may be redirected without warning to someone else; the recipient may have divulged their password or left their PC active and unattended; others may see the item if it is printed out. If in doubt phone first or, in extreme cases, consider the use of encryption. Contact the School's IT Help Desk for further advice on using encryption. Assume that all e-mail can be read by anyone (see the section on Receiving Mail below).

Copy correspondence only to those people who really need to see it. Do not use the "reply all" function.

It is not necessary to send the actual document as an attachment to a number of users within your local area; you can send a short-cut instead provided that the document has been placed in a shared area that everyone can access. Note that if the location of the original document is changed, shortcuts will not work.

Never send a message to everyone in the School. In practice very few people have this ability. Non-urgent information can be disseminated via the Intranet or Staff and student e-zines or the digital marketing system. Consult the School's marketing and communications department for further advice on methods for wide scale distribution. Sending very large attachments, complex spreadsheets or artwork for instance, to a number of addresses simultaneously could cause similar problems.

Always include a meaningful subject line. Try and include the key words early in the phrase as not all of it may be displayed when the message is listed, e.g. use "Green Committee Meeting minutes 24/01/06" NOT "Agenda item 6, minutes of meeting".

4.1.3 Acceptable Use of Email

The School's e-mail systems are provided to assist staff and students in the performance of their jobs and courses of study. Examples of prohibited use of the School's e-mail system include, but are not limited to:

- Sending messages or holding data which are illegal, likely to cause offence or to bring the School into disrepute
- Using vulgar or obscene language
- Accessing, displaying or disseminating pornography
- Sending information that may tend to disparage or harass others, for example on the grounds of sex or sexual orientation, race, nationality, ethnic origin, colour, creed, disability, marital status, age, trade union or political beliefs
- Divulging confidential material to unauthorised third parties

- Distributing junk mail, fund raising requests, chain letters or jokes
- Soliciting or carrying out business activities for personal gain

However it is recognised that incidental and occasional use not strictly on School business should be permitted to a small degree. Such use must not be habitual or frequent, must not contravene any aspect of the School's policies and should not be done during your normal working hours.

4.1.4 Liability

Users must not enter into contractual commitments, represent or commit the School in any manner without obtaining specific authorisation. Please bear in mind the following points:

- Unless you are very confident of the effectiveness of your communication with another party, do not use e-mail for matters of contractual importance
- E-mail communications carry the same contractual implications as their paper equivalents. You should include the same specific disclaimers such as Without Prejudice or Subject to Contract, as you would for other written communication of a similar nature. If in any doubt, contact the Comptroller and City Solicitor's department at the Guildhall.
- If you are making an offer or commitment, e.g. placing an order, include a date and time on which the offer or commitment will lapse, to allow for the possible late delivery of the e-mail. Specify how the addressee should respond, e.g. in writing or whether e-mail is acceptable
- Paper copies of any significant e-mails should be placed on the relevant file to give others a complete view of the correspondence and to provide a record in case of dispute
- Where confirmation of receipt outside the School is required request an acknowledgement by return or use an alternative delivery method

4.1.5 Receiving Mail

- Check your email in-box regularly.
- If you cannot provide a reply within a few hours, send an acknowledgement indicating when you will be able to. However official emails from colleagues should be replied to in a reasonable time frame.
- Because of the risks associated with content, viruses and other malware do not open attachments from unknown or dubious sources. If in doubt delete the attachment immediately with SHIFT + DELETE (Microsoft Outlook).

- Always set up Out of Office messages or consider the use of Out of Office rules when away.
- Consider giving access to your mail to a trusted deputy to cater for unanticipated absence.

4.1.6 Filing Mail

- The filing systems provided with e-mail are not a substitute for full document management systems. If your message and/or reply is important ensure a printed

copy is taken or better still save the attachment somewhere else such as your file server storage.

- Set up your folder system as you would a paper system. Use many small folders rather than a few with a large number of messages. Frequently review their contents and delete material no longer required.
- Do not file mail unnecessarily
- Email is not an infinitely-sized filing cabinet. Delete mail and attachments that are not needed.

4.1.7 Monitoring

To ensure compliance with this policy, the School uses a full range of monitoring techniques to regulate and review the use of IT and communication systems.

NOTE: ALL EMAIL IN AND OUT OF SCHOOL SYSTEMS TO/ FROM THE OUTSIDE WORLD IS MONITORED

4.2 Viruses and Spam

As a user of the School's email systems you may receive many unsolicited email messages. A sizeable proportion of these messages may be what is commonly known as "spam" and many can be offensive in nature. Measures exist for detecting unwarranted "spam" messages, and also messages containing profane words.

Every email message that arrives at the School is analysed for tell-tale signs of spam or viruses. Viral infection is removed and the message released if possible, or the message rejected if this is not possible. Messages are also assigned a "score" on the basis of separate tests for spam -the more likely a message appears to be spam, the higher is the score. Those messages that score above a certain numerical value are "flagged" as suspicious, by tagging them (adding the characters [SUSPICIOUS MESSAGE] to the subject line of the message. Please note that there is no *absolute* way of identifying what is spam and what is not, so a small amount of spam will always come through. These are known as "false negatives."

4.2.1 Spam Scoring

Ambivalent (medium and low-scoring spam messages) may be held for review. The end user will receive a 2-hourly digest, listing the sender email address, subject and timestamp. The end user can then "Release", "Permit" or "Block" each individual email or all emails, though it is best to consider each email. The responsibility for deciding whether or not to open and read these messages must remain with the end user. All outgoing mail from the School is checked for the presence of viruses and mail is quarantined if a virus is detected. Outlook 2010 and above can also place suspected spam mail into a "junk mail" or "clutter" folder by the application of simple heuristics and it is the user responsibility to check this from time to time to ensure that no genuine messages are placed in here or missed.

It is possible to configure your email client to place similar patterned emails into a particular folder or message group other than your inbox, where you may examine it at your leisure. In Outlook, these are called "rules".

4.3. Spoofed Emails/ Phishing Emails

Spoofed emails are emails purporting to come from a user within the school to another school email user. It is another way spammers will try to get you to read their emails. They can be simply detected by looking at the sender address of the message which will have the external email address on it, for example “john.doe@school.ac.uk” as opposed to “john doe”. The external email address is not used when mails are sent internally. These should be checked and discarded. They may be detected by the system in which case they will be deleted before delivery. Another example of a spoofed email might ask you to reply with your account details such as username, email address and password. In no circumstances should emails ever contain passwords.

Phishing Emails encourage you to visit bogus websites. They usually come with an important-sounding excuse for you to act on the email, such as telling you your bank details have been compromised, or claim they’re from a business or agency and you’re entitled to a refund, rebate, reward or discount.

The email tells you to follow a link to enter crucial information such as login details, personal information, bank account details or anything else that can be used to defraud you. Alternatively, the phishing email may try to encourage you to download an attachment. The email claims it’s something useful, such as a coupon to be used for a discount, a form to fill in to claim a tax rebate, or a piece of software to add security to your phone or computer. In reality, it’s a virus that infects your phone or computer with malware, which is designed to steal any personal or banking details you’ve saved or hold your device to ransom to get you to pay a fee.

4.3.1 Protect yourself against Phishing

- Do not assume that anyone who has sent you an email is who they say they are.
- If an email asks you to make a payment, log in to an online account or offers you a deal, be cautious. Real banks never email you for passwords or any other sensitive information by clicking on a link and visiting a website. Never submit any personal details.
- If in doubt, check it’s genuine by asking the company itself. Never call numbers or follow links provided in suspicious emails; find the official website or customer support number using a separate browser and search engine.

4.3.2 Spot the signs of Phishing

- Their spelling, grammar, graphic design or image quality is poor quality. They may use odd ‘spe11lings’ or ‘cApiTals’ in the email subject to fool your spam filter.

- If they know your email address but not your name, it will begin with something like ‘To our valued customer’, or ‘Dear...’ followed by your email address.
- The website or email address doesn’t look right; authentic website addresses are usually short and don’t use irrelevant words or phrases. Businesses and organisations don’t use web-based addresses such as Gmail or Yahoo.
- Money’s been taken from your account, or there are withdrawals or purchases on your bank statement that you don’t remember making.

- Hyperlinks do not look right and do not pertain to the subject-matter in question.

4.3.3 Website Links

You may find a link to a website pretending to be a well-known company, organisation or service. The aim of these websites is to convince you that you're using a real online service so that you hand over your personal or banking details or send money.

4.3.4 Social media

Facebook, Twitter and other social media channels are also used to direct you to a spoof website. Fraudsters create accounts that have similar usernames and profile pictures to official accounts to trick you into thinking you're dealing with someone you can trust. Official accounts are 'verified' – they come with a checkmark icon next to their name, meaning they've proved themselves as the official company to the social media channel.

4.3.5 How to report it

Please report instances where action was erroneously taken to your IT Helpdesk. It is not necessary to report all instances of emails received that are believed to be fraudulent as many thousands are received and purged every day and it is inevitable that a few may get through. However we may need to know if you have compromised the School by giving away credentials or so on.

4.4 Email Attachments

4.4.1 Staff

Non-business email attachments are not allowed. Non-business attachments received from outside the School must be permanently deleted immediately with a SHIFT-DELETE (Outlook).

4.4.2 All Users

Attachments should not exceed 20MB in size – this is to stop possible Denial of Service of the email system by excessive message size. There is a 30 attachment limit per email providing the total size limit is not exceeded. However please note that the email system overhead itself adds significant size to email attachments.

<u>All executable attachments are prohibited from the system and are purged upon receipt.</u>
Executable attachments include EXE, COM and BAT files and HTML, VBS and LNK (shortcut) files amongst others. In addition to this Microsoft Outlook will not allow certain kinds of attachments to be received.

Encrypted emails cannot be virus scanned in the usual way and so must be considered a threat. You should consider carefully the use of encryption on emails sent, and see 9.2.4 below.

The internet email system as a whole must now be considered unsecure and you should consider the consequences of sending confidential or sensitive information by this method, regardless of whether messages have been encrypted or not.

5. Internet Access – Staff and Students

5.1 Permitted Internet Web Site Categories

In terms of internet access, two Acceptable Use policies (AUPs) apply to the School – the JANET acceptable use policy which applies to everyone including *eduroam* visitors (JANET is our internet service provider) and the School acceptable use policy which additionally applies to staff and students.

All internet access at the School on the Corporate, Student or Wireless networks is monitored.

All web sites are categorised by the web filter into one of the following categories (these are constantly under review). Web site categories are shown to be permitted or blocked an AUP: Please note the wireless policy is a little different because of its use by visitors.

Web Filter Category	**Access**	**Reason**	**Wireless**
Adult/Sexually Explicit	Blocked	JANET 9, 10 Staff Handbook	Blocked
Advertisements	Permitted		Permitted
Arts & Entertainment	Permitted		Permitted
Internet chat (not *including Skype)*	Permitted		Permitted
Computing & Internet	Permitted		Permitted
Criminal Skills	Blocked	JANET 8, 11, 13 Staff Handbook	Blocked
Drugs, Alcohol & Tobacco	Permitted		Blocked
Education	Permitted		Permitted

Finance & Investment	Permitted		Permitted
Food & Drink	Permitted		Permitted
Gambling	See policy	Staff Handbook	Blocked
Games	Blocked	JANET 16.5 Staff Handbook	Blocked
Glamour & Intimate Apparel	Permitted		Permitted
Government & Politics	Permitted		Permitted
Hacking	Blocked	JANET 8, 15; 16.2 Staff Handbook	Blocked
Hate Speech	Blocked	JANET 9, 10, 12 Staff Handbook	Blocked
Health & Medicine	Permitted		Permitted
Hobbies & Recreation	Permitted		Permitted
Hosting Sites	Permitted		Permitted
Job Search & Career Development	Permitted		Permitted
Kids Sites	Permitted		Permitted
Lifestyle & Culture	Permitted		Permitted
Motor Vehicles	Permitted		Permitted
News	Permitted		Permitted
Personals & Dating	See policy	JANET 16.1 Staff Handbook	Permitted
Photo Searches	Permitted		Permitted

Real Estate	Permitted		Permitted
Reference	Permitted		Permitted
Religion	Permitted		Permitted
Remote Proxies	See policy	JANET 8, 18, 19	Blocked

Search Engines	Permitted		Permitted
Sex Education	Permitted		Permitted
Shopping	Permitted		Permitted
Sports	Permitted		Permitted
Streaming Media	Permitted		Permitted
Travel	Permitted		Permitted
Usenet News	Permitted		Permitted
Violence	Blocked	JANET 9, 10 Staff Handbook	Blocked
Weapons	Permitted but see policy above		Blocked
Web-based Email	Permitted		Permitted

5.2 JANET Acceptable Use Policy

Found at: https://community.jisc.ac.uk/library/acceptable-use-policy

Version: 12, May 2016 – reproduced in part below

Unacceptable Use

8. Janet may not be used by a User Organisation or its Members for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities. (See **Note 3**.)

9. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material. (See **Note 4**.)

10. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.

11. Creation or transmission of material with the intent to defraud.

12. Creation or transmission of defamatory material.

13. Creation or transmission of material such that this infringes the copyright of another person.

14. Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.

15. Deliberate unauthorised access to networked facilities or services. (See **Note 5** and **Note 6**.)

16. Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:

16.1 wasting staff effort or Janet resources, including time on end systems on another User Organisation's network, and the effort of staff involved in the support of those systems;

16.2 corrupting or destroying other users' data;

16.3 violating the privacy of other users;

16.4 disrupting the work of other users;

16.5 denying service to other users (for example, by overloading of access links or switching equipment, of Janet services, or of services or end systems on another User Organisation's network);

16.6 continuing to use an item of software or hardware after the Janet Network Operations Centre or its authorised representative
has requested that use cease because it is causing disruption to the correct functioning of Janet;

16.7 other misuse of Janet, such as the introduction of "viruses" or other harmful software via Janet to resources on Janet, or on another User Organisation's network.

Access to Other Networks via Janet

17. Where Janet is being used to access another network, any deliberate or persistent breach of the acceptable use policy of that network will be regarded as unacceptable use of Janet. Any activity as described in clause 16 above, and where applied either to a user of that network, or to an end system attached to it, will also be regarded as unacceptable use of Janet.

18. Any deliberate or persistent breach of industry good practice (as represented by the current standards of the London Internet Exchange) that is likely to damage the reputation of Janet will also be regarded prima facie as unacceptable use of Janet.

Compliance

19. It is the responsibility of the User Organisation to take reasonable steps to ensure its Members' compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of Janet is dealt with promptly and effectively should it occur. The discharge of this responsibility includes informing all Members of the User Organisation with access to Janet of their obligations in this respect. (see **Note 7**.)

20. Where necessary, service may be withdrawn from the User Organisation, in accordance with the Janet Terms. Where violation of these conditions is unlawful, or results in loss or damage to Janet resources or the resources of third parties accessible via Janet, the matter may be referred for legal action.

Explanatory Notes

Note 1: The Acceptable Use Policy does not make any particular statement as to the acceptability of using Janet for activities resulting in commercial gain to the User Organisation, other than this is acceptable where lawful. However, it should be noted that there are legal constraints applying to a publicly funded User Organisation in such activities. Where the User Organisation is operating as an economic undertaking the issue of State Aid will need to be considered. There is also an issue of the status of both Janet and the User Organisation's network as private networks. Both are addressed in the Janet Eligibility Policy and more particularly in the Janet factsheets referenced therein.

Note 2: It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of Janet resources on the part of its users and appropriate disciplinary measures taken by their User Organisations.

Note 3: *The list of unacceptable activities in this section is not exhaustive*. The purpose is to bring as clearly as possible to the reader's attention those activities most commonly associated with the abuse and potentially unlawful use of a network.

Note 4: It may be permissible for such material to be received, created or transmitted where this is for properly supervised and lawful purposes. This may include, for example, approved teaching or research, or the reception or transmission of such material by authorised personnel in the course of an investigation into a suspected or alleged abuse of the institution's facilities. The discretion to approve such use, and the responsibility for any such approval, rests with the User Organisation. Universities UK has provided guidance on handling sensitive research materials.

Note 5: Implicit authorisation may only be presumed where a host and port have been advertised as providing a service (for example by a DNS MX record) and will be considered to have been withdrawn if a complaint from the provider of the service or resource is received either by the User Organisation or by Janet. For all other services and ports, access will be presumed to be unauthorised unless explicit authority can be demonstrated.

Note 6: Where a User Organisation wishes to commission or itself perform a test for vulnerabilities in its IT systems (for example, via "penetration testing") this, as an action authorised by the User Organisation, will not be a breach of clause 15. However, the User Organisation should inform the Janet CSIRT, in advance of the test, of the source, nature and timing of the test. This is to avoid wasting the time and resources of the CSIRT in investigating the perceived attack on the User Organisation, or automatically blocking it.

Note 7: In order to discharge this responsibility, it is recommended that each User Organisation establishes its own statement of acceptable use within the context of the services provided to its Members. This should be cast in a form that is compatible with the provisions of this Acceptable Use Policy. Such a statement may refer to, or include material from this document. If material is included, this must be done in such a way as to ensure that there is no misrepresentation of the intent of the Janet Acceptable Use Policy.

5.3 School Staff Internet Access AUP

The School Staff Handbook has many sections that relate to IT and data security and these are constantly under review so staff should familiarise themselves with the relevant parts.

6. Telephones and Faxes

6.1 Staff

School telephones and faxes should normally only be used for School business. Although certain types of usage may be restricted in line with specific local arrangements, the following general rules apply:

- Calls to the user's home and home area for domestic purposes are permitted without payment. Such calls must be kept short.
- Any personal calls other than to the user's home area must be reported to the operator and the user will be liable for the call charge.
- All personal faxes should be passed to the Telecommunications Section for transmission. The user will be liable for the call charge.
- All incoming and outgoing personal calls and faxes should be kept to an absolute minimum.

6.2 Students

Faxes may only be sent from designated fax machines but will be charged as appropriate by local administrative staff. Specially provided student phones (i.e. in student production

offices) may *not* call international numbers unless authorized by staff. Local and regional calls may be permitted in certain areas where necessary for the pursuance of coursework.

6.3 Mobile Telephones, Staff

If mobile telephones are provided for business use, private calls and text messages may be made provided they are not excessive and the cost of such calls is repaid to the School including any tax liability. Mobile telephones are issued at the discretion of a Head of Department who will have a mobile phone budget as appropriate. Note: these are not under the control of the IT department but responsibility and running of mobile phones is devolved to staff themselves.

6.4 SMS services

If SMS services (through a web account) are provided for business use text messages are monitored and may be made provided they are not excessive vis a vis purpose or for the purposes of marketing. The service may be withdrawn in the event of misuse at the discretion of the Head of IT.

7 School Laptops

School laptops and other computer equipment for use outside the office must:

- Be used mainly for business purposes although it is acknowledged that some private use is acceptable provided it falls within the terms of the rules given above
- Access the School's network only via authorised, secure routes.
- Run approved antivirus software. It is the responsibility of the user to ensure that the software is kept up to date using the method laid down by the I.T. Department.
- Have encrypted local storage/ hard disks.
- School-issued laptops with the "Always on VPN" or "DirectAccess" feature are further subject to *Remote working equipment - staff responsibilities (ST056)* policy.

7.1 regular Maintenance of Laptops

If a supplied laptop is not brought into work for some time (for over two weeks for example) such that the anti-virus software has therefore not been updated for that time, the approval of the IT Department should be sought before attempting to connect the laptop to the corporate network. However laptops with an internet connection can update across the internet in any event and are usually configured to do so.

8. Copyright

Users must not make or use unauthorised copies of software whether for business or personal purposes. Users must not download, copy or transmit to third parties the works of others without their permission as this may infringe copyright which can lead to personal and corporate liability and may constitute a criminal offence. Users should note that the CLA copyright guidelines are prominently displayed near all photocopiers. If unsure, the Head Librarian may advise on copyright issues.

9. Offensive Material

Users must not create, publish, circulate or display on computer monitors statements, images, information or sounds which are abusive, obscene, defamatory, discriminatory, or which could be regarded as harassment. This could give rise to personal or corporate liability and may constitute a criminal offence.

All offensive email and messages must be deleted immediately.

10. Contractual Commitments

Users must not enter into contractual commitments, represent or commit the School in any manner without obtaining specific authorisation.

11. Monitoring Activity

To ensure compliance with these rules, the School and the School uses a full range of monitoring techniques to regulate and review the use of IT and communication systems. This includes, amongst other things, monitoring telephone calls, logging traffic, recording Internet access and monitoring e-mail. User activity is reported as appropriate and abuse of these systems investigated.

12. Data Protection & Confidentiality

Users must take care when collecting, keeping or using personal, sensitive or confidential information. Users must adhere to the Principles and provisions of the Data Protection Act 2018. The Internet, e-mail and fax systems must all be considered non-confidential methods of communication and careful consideration should be given to using them for sending sensitive information.

12.1 The Limits of Confidentiality and Security

Privacy and confidentiality are important values for users of information technology at the School. Normally, users can expect that their communications and the contents of their accounts will be treated as private and confidential and that their files will not be accessed

without their permission. However, individuals have no right to absolute privacy when using information technology resources at the School. The School owns the information technology infrastructure and is therefore responsible for its use. The School reserves the right to take action to see that its information technology is used lawfully, appropriately, and efficiently in pursuit of the primary purposes of the institution.

12.1.1 Privacy does not extend to the following situations:

Aggregate statistics about user accounts are not confidential (for example, data that indicate the amount of storage being used by particular accounts or internet statistics while an employee is at work).

As a normal part of their system administration duties, information technology employees monitor levels of network traffic, use software that logs network activity, make copies of files, and maintain archives of these copies.

Information technology employees may access any file, data, program, or e-mail in order to gather sufficient information to diagnose and correct network, hardware, and software problems.

12.2.2 Information Release

Technology employees will compile and release otherwise confidential information when this is required but only when the request meets the following three conditions:

(a) The request is made by the appropriate officer in the institution. These officers are:

- The Principal of the School.
- The Senior Management team at the School or the Head of HR (in the case of employees and associates) with respect to an internal School investigation.
- The officer in charge of Information (or other person authorized by the Principal to execute the legal obligations of the School with respect to legislation concerning freedom of information and protection of privacy) with respect to Freedom of Information requests or requests from law enforcement agencies for assistance with investigations.

(b) The request is made in writing, is reasonably specific in terms of the information required, and specifies to whom the information is to be released. (The request to the Head of IT to gather and release information need not contain reasons why the information is required. The person and office issuing the request according to section has the obligation to establish and document these reasons and to ensure that the request and subsequent actions comply with the appropriate laws and policies under which they are acting.)

(c) The request is addressed to the Head of IT who shall be responsible for fulfilling the request, even though the actual work of gathering the requested information may involve other information technology employees.

The School assumes no liability for files and information that are stored on its systems. It has no obligation to maintain or destroy any or all physical representations of particular files.

In the cases of doubt please refer to the local AIN or refer to the School's data protection officers.

13. IT accounts of people leaving the School.

Once you leave the School you are no longer entitled to an IT account and the process of removing them is started.

13.1 Staff who leave School.

The IT department relies on the data received from either the HR department or from departmental heads to tell us which staff are automatically entitled to IT accounts. If we are notified by the same parties that someone is leaving on a particular date then we will purge the account after that date. It is the user's individual responsibility to take their data with them before they leave. After they leave, it is not obligatory to surrender any data to them and a charge may be made for retrieving data that has been lost in this way.

It is not acceptable for the account of someone who leaves the School to be used by someone else without following the correct procedure.

13.1.1 IT account and Email address of the Staff member who has left.

When someone leaves the School we normally "close" their IT account and email address. We cannot allow anyone else to use the account/ email address during this period unless we have permission from the leaver granting access. This is because we are legally obliged to protect the privacy of everyone's mailbox even after they have left and also because emails sent out from the leaver's email account can be represented as from them.

13.1.2 Someone using another person's IT account – Staff

If we have reason to believe that someone other than the leaver is using their IT/ email account without the correct permission we will disable the account immediately. If the leaver's email address is still required there are multiple possible courses of action to be selected by the (leaver's) line manager:

1. As above - obtain written permission from the leaver to reopen the account temporarily and/or reroute incoming mail to someone else's mailbox.
2. Remove the account. Mail sent to the leaver will not be delivered but will be returned to the sender with a standard mail message called a non-delivery report (NDR) suggesting that the intended recipient is no longer at the School.
3. Place an "out of office" message on the account for a short while asking the sender to re-direct enquiries to another staff member.

13.1.3 Generic email addresses.

Generally, individual email addresses should not be used on forms, posters, flyers, adverts etc. Generic email addresses based on a role rather than a person can be created and set to point to whoever is handling the mail. If that person leaves the address can then be redirected to whoever takes over the role without having to change the advertised details.

13.2 Students who leave School.

We rely on the data received from the Registry to tell us which students are automatically entitled to accounts. If we receive written (including email) information from Registry that someone is/ will leave, we will delete the account after the leaving date. It is therefore their (students) responsibility to copy their data to multiple backup locations during their time at the School and when they leave, take their data with them.

13.2.1 Students Final Term

IT Accounts are normally left open for two weeks after the end of their last term (date unless advised by Registry) before deletion. Accounts are not kept open over the summer unless requested by Registry. (This does not apply to postgraduate students who finish courses in September.) Please note that in some cases IT are not notified that students are continuing on to another course at the School after the completion of their current course in a timely fashion and therefore students should take steps to ensure that they have a backup of their data if they need it.

If you feel that you are still entitled to use the IT facilities but our records don't show you in the data we receive from Registry you need to contact the Registry to get your status clarified and to ensure that you do appear on the correct records.

13.3 Freelancers and other staff not on the salaried staff payroll

Persons falling under this category would not normally be entitled to an IT account under the HR rules. In these circumstances this can be authorized by a Head of Department if expedient to do so. However in some cases this may be limited to wireless access only.

14. Sanctions and Procedures in Cases of Alleged Misuse

14.1 Investigating alleged misuse of information technology

The School may undertake investigations of specific allegations of alleged misuse of information technology. These investigations may involve the collection and analysis of information that is otherwise considered private and confidential, subject to sections of this Policy. In the case of students or members of the general public, only the Vice Principals may authorize investigations of alleged misuse of information technology. In the case of employees and associates, only the Vice Principals or Human Resources Manager may authorize an investigation. In cases where the identity of the person of interest is unknown, either the Vice Principals or Head of IT may authorize the investigation, but the further conduct of the investigation will fall to the appropriate person once the identity is known. All investigations must comply with the Policy provisions under which they are conducted—for

example, notifying people that that their actions are under investigation and ensuring appropriate levels of confidentiality.

14.2 Processes for cases of alleged misuse

Within the School, the processes used to consider cases of alleged misuse of information technology will be those normally used for cases involving possible student or employee misconduct. Sanctions will include those allowed under various School policies or the Student Code of Conduct and disciplinary procedure. In addition to other sanctions, misuse of information technology may result in denial of access to the technology or specific limitations on its use. Any such denial or restriction must be reasonable in terms of time limits and extent. The Vice Principals, Human Resources Manager and Head of IT have the authority to order the temporary withdrawal or limitation of privileges to use information technology pending a fuller investigation of alleged misuse.

15. Incident Notification and Escalation Path

All actual or suspected security breaches or issues must be reported in the first instance to the School's IT Helpdesk who may refer the matter (or escalate it) to the Head of IT if necessary. Please contact the IT Helpdesk if further guidance is required.