The Sutton Academy

Staff ICT Acceptable Use Policy

Status	**Non-Statutory**
Responsible Governors' Committee	**HR & Finance**
Date last approved by GB	**Not Applicable**
Responsible Person	**Mr P Blakemore**
To Review Date	**October 2020**
Last Amended Date	**October 2018**

Staff ICT Acceptable Use Policy

This policy covers the acceptable use of ICT systems to support learning, email and the internet by staff, and the use of online tools provided by The Sutton Academy.

Acceptable Use of ICT Equipment Principles

The Academy is committed to safeguarding its ICT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the academy's ICT infrastructure is the responsibility of all staff. The academy encourages staff to fully use the ICT infrastructure and to make use of portable ICT equipment offsite to support them in their work. The academy encourages this use in a responsible and professional manner. Portable computers include for example laptops, tablets and other portable ICT devices.

As a user of ICT services of the academy you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse academy computing facilities in a way that constitutes a breach or disregard of this policy, consequences associate with that breach and you may be in breach of other academy regulations.

Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements. Staff are advised of this policy during their induction and of the academy's requirement for them to adhere to the conditions therein.

For the purposes of this policy the term "computing services" refers to any ICT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the Internet). Staff who connect their own ICT to the Academy's network and the services available are particularly reminded that such use requires compliance to this policy.

Purposes

- To protect the academy's networks and equipment
- To protect the academy's data
- To protect the academy and its employees from activities that might expose them to legal action from other parties

Password Security Guidelines

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the Academy. Issuance and continued use of your User Account is conditional on your compliance with this policy. User ID's and passwords are not to be shared or revealed to any other party. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy.

Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords should be routinely changed (every 3 months is recommended) and should be changed immediately if the user believes or suspects that their account has been compromised.

General Conditions

In general, use of academy "computing services" should be for your study, research, teaching or the administrative purposes of the academy. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.

- Your use of the academy's computing services must at all times comply with the law.
- Your use of the academy's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the users' permission.
- You must not use academy computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use academy computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and special authorisation from the Principal).
- You must not use the academy's computing services to conduct any form of commercial activity without express permission.
- You must not use the academy's computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence, and which is not first authorised by the ICT Department for installation
- You must not use any peer-to-peer file sharing software
- You must not use any IRC or messenger software including, but not limited to AOL, MSN, Yahoo! or other "Messengers", IRC or "chat" clients unless expressly authorized to do so for work related purposes
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the academy's facilities, unless specifically related to academy activities
- You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Principal/Governing Board
- You must not play computer games of any nature whether preinstalled with the operating system or available online

Data Security

The academy holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law in the Academies Data Protection Policy which includes GDPR.

You should only take a copy of data outside the academy's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, memory sticks, cds/dvds or into emails. If you do need to take data outside the academy, this should only be with the authorisation of the academy's Data Protection Officer. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular using VPN and remote desktop) which allow you to work on data in-situ rather than taking it outside the Academy, and these should always be used in preference to taking data off-site. The ICT Department offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for advice.

Anti-Virus and Firewall Security

All personal computers are installed with current versions of virus protection and firewall software by the ICT Department. Users are not to alter the configuration of this software unless express permission has been obtained from the ICT Department. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files. Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, they should inform the ICT Department immediately. If the ICT Department detects a machine behaving abnormally due to a possible viral infection it will disconnected from the network until deemed safe.

Physical Security

The users of ICT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would
- Keep liquids away from ICT equipment
- Do not place heavy objects on ICT equipment
- Do not drop ICT equipment or objects onto it
- Any portable computer must be securely locked away when not in use.
- Portable computer security is your responsibility at all times.
- Do not leave the portable computer unattended in a public place or within the academy
- Do not leave the portable computer on view inside your car. It should be locked away in your car's boot out of sight.
- Extra reasonable care must be taken to prevent the loss of USB sticks which contain confidential academy data
- Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment

Remote Access

Remote access to the academy network is possible where this has been granted by the ICT Department.
Remote connections are considered direct connections to the academy network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy. All connection attempts are logged.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.

Such records and information are sometimes required, under law, by external agencies and authorities. The academy will comply with such requests when formally submitted.

E-Safety

The Academy has a duty of care to ensure that Information and Communications Technology (ICT) is used appropriately and does not compromise the safety of staff and students or the reputation of The Academy.

The Internet and other digital and information technologies are powerful tools which open up new learning opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. It is the Academy's intention to provide Students with an entitlement to safe internet access at all times.

The Academy is committed to ensuring that all our students are able to use the Internet and related communications technologies appropriately and safely in line with the Academies safeguarding policy.

Guidelines Use of Telephones

There will be occasions when employees need to make short, personal telephone calls on academy telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of academy telephones, which are unreasonably excessive or for academy purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

Where the academy has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the academy reserves the right to record calls.

Use of Email

E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication.

Employees should be careful that before they open any attachment to a personal e-mail they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the academy. Any other use of e-mail to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. Where the academy has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.

The academy also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of its staff to undertake their academy role.

Unauthorised use of the Internet, which is unreasonably excessive or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. The academy reserves the right to audit the use of the Internet from particular Personal Computers or accounts where it suspects misuse of the facility

Monitoring the use of Telephone, Email and the Internet.

It is not the academy's policy, as a matter of routine, to monitor an employee's use of the academy's telephone or e-mail service or of the Internet via the academy's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Principal may grant permission for the auditing of an employee's telephone calls e-mail or the Internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Principal.

These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Principal/Governing Body or their delegated representative to enable Human Resources to advise the appropriate line manager/head of faculty the actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

Computing Services Declaration

Please only agree if you have fully read the Acceptable Use Policy and have understood the terms and conditions and all the instructions of The Sutton Academy IT Services.

Please contact the IT Network Manager at The Sutton Academy if you are not sure of any policies and terms and conditions of use.