ICT Policy

Policy Owner:	Matt Moody
Ratified by:	QAT Board
Date:	April 2019
Next review date:	January 2020

Q3 Academies

ICT Security Policy

Contents

Background

The Q3 Academy ICT Support Department aims to support the development of communication and information tools and systems for research, learning and management within each Academy, between Academies and the rest of the world. These policies are intended to facilitate the smooth and consistent running of systems and services in support of this aim.

The term "Information and Communications Technology" (ICT) can be interchanged with the term "Information Technology" (IT) in much current documentation, this policy uses the term IT. Most of the tools of communication and information technologies: audio and video, telephones and faxes, copiers and printers, computers and network infrastructure, are included in the department's remit. This broad definition of "IT" has been used throughout the policies and should be kept in mind when interpreting them.

Typographic convention: *italicized text* indicates explanatory notes rather than policy.

A. TRUST POLICY STATEMENT

A.1 Scope of IT Policies

The Q3 Academies Trust (QAT) IT policy and its supporting policies apply to:

1. All staff and students within the Trust and its Academies and all other users authorised by the Trust, whether at QAT premises or elsewhere. *This includes visitors to the Trust from other organisations (Please see Appendix 2).*
2. Users from other institutions under arrangements covered by location independent networking (LIN).
3. The use of QAT-owned, on-loan facilities. They also apply to all private systems, whether owned, leased, rented or on-loan, when connected to the Trust's network directly or indirectly.
4. All QAT/Academy-owned or licensed data/programs, be they on QAT systems or private systems, and to all data/programs provided to the Academy by sponsors or external agencies.

The IT systems covered include servers, workstations, desktop computers, laptop/notebook/handheld computers, communications equipment, photocopiers, telephones, facsimile machines and audio visual equipment installed anywhere within the QAT, or operated on behalf of the Trust at another location.

This policy is to be used in conjunction with AUP (Acceptable Use Policy), which has to be signed by all students and staff.

A.2 Objectives

The objectives of IT policy and its supporting policies are to:

1. Provide systems that are suited to their purpose.
2. Provide and maintain safe IT equipment in a suitable environment, and to ensure safe working practice in the operation of IT equipment.
3. Ensure that the Trust achieves best value in its IT provision.
4. Ensure that QAT IT facilities are adequately secure.
5. Ensure that users are aware of and fully comply with the relevant legislation, policies, procedures, guidelines and standards.
6. Ensure safe, and socially and environmentally responsible disposal of equipment in line with the Waste Electrical and Electronic Equipment (WEEE) regulations;
7. Ensure that QAT and its Academies play an active and responsible part in the wider higher education community in its use of information technology.
8. Ensure that all students, as children, are safeguarded as much as possible against external threats using appropriate technologies and instruction through learning consultant guidance.

Definitions of terms used in this Policy Statement can be found in Appendix 1.

A.3 Responsibilities for IT Policies

The Group IT Manager and the Executive Group have responsibility for initiating and drafting IT policies and for delegating the production of supporting documentation.

The Group IT Manager, Executive Group and ICT Network Supervisors have responsibility for arranging the consultation process as appropriate for each policy.

The Group IT Manager and the Executive Group have responsibility for arranging approval of IT Policies.

The Group IT Manager and the Executive Group have responsibility for maintaining IT policies in an up-to-date and accessible form.

The Group IT Manager and the Executive Group have responsibility for arranging the dissemination of IT policies in an appropriate and accessible way.

It is the responsibility of each individual, defined in paragraph A.1 above, to ensure their understanding of and compliance with this and associated policies. Such responsibility is part of a member of staff's contract of employment and a student's Acceptable Use Agreement (AUP). All other users are required to sign the agreement in Appendix 2.

A.4 Compliance with Legislation

The Trust has an obligation to abide by all relevant legislation. This policy and supporting policies, procedures, guidelines and standards must satisfy all applicable legislation. This obligation formally devolves to all users defined in A.1 above, who may be held personally liable for any breach of the legislation.

If anyone finds an inconsistency between policies and legislation, or between individual policies, they must bring this to the attention of the Group IT Manager, ICT Network Supervisor or the Executive Group.

A.5 Health and Safety

The Trust will provide and maintain equipment that is safe in the context of its intended use. Individual users have a responsibility to operate these systems safely and report any defects. Managers with responsibility for health and safety should follow recognised guidelines in assessing risk, and should consult the relevant Health and Safety Officer when advice is needed.

All users must follow manufacturer's instructions or handbooks in the installation and operation of IT systems, and should consult the relevant Health and Safety Officer when advice is needed.

A.6 Environmental responsibility

All systems within the scope of this policy will be acquired, operated and disposed of in an environmentally responsible manner and in line with the WEEE regulations.

A.7 Policy Awareness

All IT policies and guidelines will be made freely available electronically on the relevant Academy web site to everyone to whom they apply (see A.1 above) and these will form the up-to-date official version. Policies and guidelines will also be published in Staff handbooks, Student handbooks and contractors' guidelines, and will be available as paper copies for issuing to users as required.

Anyone responsible for authorising the use of facilities within the scope of this policy and its supporting policies is responsible for informing new users of IT policies.

All IT procedures and standards will be published electronically wherever possible, however where publication could compromise safety or security, procedures and standards will be restricted.

A.8 Changes to IT Policies

The normal process for changing IT Policies will be for a request to be made to the Group IT Manager and Executive Group, who will arrange for suitable approval from the relevant Local Governing Body. At this point the published IT Policies will change.

In the event of a need for urgent change, this may be approved by the Group IT Manager and implemented immediately, pending formal approval from the Executive Group and MAT Board. Any urgent changes will be published immediately with the changes highlighted as provisional.

A.9 Status of IT Policies

It is a condition of employment that staff will abide by QAT Rules and Policies of which IT Policies are a part. Where a member of staff does not abide by these, then dependent on the severity of the misconduct, the CEO, Head of School, or a designated member of the Senior Team, will deal with incident in accordance to the QAT Disciplinary Policy.

The Trust's Rules and Policies, including IT Policies, are an integral part of the Student Agreement.

IT policies are an integral part of the Trust's Policies to which contractors must adhere.

B. COMPLIANCE WITH LEGISLATION.

B.1 Introduction

Users must comply with current British legislation in all respects when using IT systems and equipment. *Legislation which applies particularly to these circumstances are: The Health and Safety at Work etc. Act and the work of the Health and Safety Executive, The Computer Misuse Act 1990, The Data Protection Act 1998, General Data Protection Regulation (GDPR) and the work of the Information Commissioner's Office, The Regulation of Investigatory Powers Act 2000, The Communications Act 2003, The Copyright, Designs and Patents Act 1988 and the work of the Copyright Licensing Agency.*

Data Protection Act

Users must comply with the Trust's Data Protection Policy as published on http://www.q3mat.org.uk/trust-policies.

Intellectual Property Right, Licenses etc.

No user may copy programs or information to paper, removable media (such as USB hard drives or flash drive), non-removable media (such as hard disks) or to portable devices, except where explicitly allowed by the license agreement/contract and where no copyright or intellectual property right is infringed.

Theft and misuse

Unauthorised removal of QAT-owned, leased, rented or loaned IT equipment, software or data from the Trust's premises constitutes a theft.

No user may interfere with protection systems. *This includes: any device which is provided to prevent removal or theft of equipment; any software or configuration that detects or prevents virus infection; any software or configuration that prevents the running of non-approved software.*

No user may install or use software or systems which are not licensed for use.

QAT systems may not be used to transmit, store or access text, images, recordings, scripts, programs or telephone calls that contain:

- ✓ Material likely to contravene current legislation such as sexist, racist, homophobic, xenophobic, pornographic, paedophilic or discriminatory material, except in the legitimate pursuit of valid pre-authorised research authorised by the CEO, Group IT Manager or Head of School in delegation with the Local Governing Body or MAT Board.
- ✓ Text, images or recordings to which a third party hold copyright or other intellectual property right, without the written permission of the right holder.
- ✓ Material that is defamatory, libellous, slanderous or threatening.
- ✓ Material that could be used to breach computer security or to facilitate unauthorised entry into computer systems.
- ✓ Material that is likely to prejudice or seriously impede the course of justice in UK criminal or civil proceedings;
- ✓ Material containing personal data as defined by the Data Protection Act 1998 and/or GDPR unless the subjects' permission has been explicitly given in writing.

The Regulation of Investigatory Powers Act 2000

The Trust's systems may intercept any communication transmitted across or stored on its systems provided that this is within the framework of the Regulation of Investigatory Powers Act 2000 (RIP). In particular, it may monitor, but not record, communications:

1. To anonymous helplines.
2. To determine whether communications are for personal or business purposes, except where personal use contravenes the staff conduct policy.

The QAT may monitor and record communications for the following purposes:

- ✓ To ensure that users are complying with Trust policies, Conditions of Use, procedures and guidelines and with British legislation, or AUP, except that recording may not take place the criteria above.
- ✓ To monitor standards of quality, performance and security.
- ✓ To prevent or detect crime.
- ✓ To investigate unauthorised use of systems.

When an external agency requests information under the RIP Act, Head of School or local senior leader will be the point of contact. In their absence, the ICT Network Supervisor or Group IT Manager shall be the point of contact.

The Trust routinely logs transactions on its systems. This logging covers the transmission of e-mails, access to web pages, the placement of telephone and fax calls and logging in and out of user network accounts. Some administrative systems also have transaction logging enabled. Electronically recorded messages and logs may be automatically backed up; these backups will also be covered by the RIP Act 2000.

All other interceptions must be authorised by the ICT Network Supervisor responsible for the system on which the interception is to take place. In this person's absence, responsibility will be assumed upwards through the line management, and ultimately to the Executive Group. The Group IT Manager will act as the compliance officer and is responsible for ensuring that policies and procedures are implemented in accordance with the RIP Act.

Accessibility

Where electronic information is provided with the intention of being generally accessible, this information should be in a suitable form for those with disabilities to gain access to the information wherever practicable. *This particularly applies to information on the World Wide Web where internationally recognised Accessibility Guidelines should be used when authoring material.*

The QAT will, wherever possible, make suitable provision for legitimate users with disabilities to access relevant information using appropriate information technology.

B2. Conditions of Use for IT Systems

Principles

QAT IT assets must be safeguarded, and operated and administered in the best interests of the Trust and its community as a whole. The interests of individuals or sections should not override the requirements for provision and continuity of service for the remainder of the QAT.

Access to equipment and information

Only those within the scope of the IT Policy, A.1, may use QAT IT systems.

No user may read/view/listen to, modify or delete any file or information without authorisation from the owner of the file. The Trust reserves the right to remove material from its systems which it deems to be unsuitable. Criteria for suitability are given later in this section. Removal of material may be governed by the **Data Protection Policy** or this policy. Where this is not applicable, the authority is vested in the Group IT Manager or ICT Network Supervisor. *Where information is clearly provided for other users to access (such as on the Internet or intranet), authorisation to read/view/listen to is implicit.*

Shared access to file space must be managed through the use of operating system services. It is not normally permitted for users to allow someone else to log in under their username in order to make use of their file space or for any other purpose. If temporary access needs to be given to someone else, the usual practice would be for the normal user to perform the login process. If, for legitimate operational or training reasons and with the approval of the ICT Network Supervisor, Group IT Manager or Head of School, a password is divulged to someone else, the password must be changed as soon as possible. *See below:* security of passwords.

A user must login to a shared system only under a username which he or she has been allocated. Logging in to a machine using someone else's username, password, or PIN number is an offence unless it is for legitimate operational or training reasons and with the approval of the ICT Network Supervisor or higher authority. *The CEO, Head of School, or member of the Senior Leadership Group/Team may consider it necessary to access an absent member of staff's files or email messages in order to maintain continuity of service. Where the absent member of staff's password is not known, the IT Support Department should be contacted in order to gain access. However, procedures should not normally require a user seeking assistance to divulge his or her password to anyone else.*

Security of passwords and PIN numbers

It is the responsibility of all users to maintain the security of their own passwords and PIN numbers. Any user who fails to take reasonable steps to do so breaches this policy and may be liable for any consequences which follow if another person makes use of one of them. *It is good practice to periodically change your password, and if you suspect that your password has become known to someone else you should change it immediately. Passwords should be chosen with care: do not use a dictionary word or a name, and include a number if possible. Passwords should not be made readily accessible: treat passwords as you would a credit card - safe and secure.*

QAT systems have a minimum requirement in terms of password length and security. In some cases, as per best-practice guidance, account lockout (after multiple failed attempts), password lifespan (a password can be no older than a certain number of days) and password complexity are applied across QAT systems. Further details may be obtain from the ICT Network Supervisor.

Use and security of equipment and information

IT resources are only available to users as defined in policy A.1. Additionally, the resources must have been allocated and/or approved by the Trust for their use.

IT resources may only be used for the purpose they are intended and in the way these systems are configured. Only QAT-appointed ICT Support Professionals, approved contractors or others with approval from the Group IT Manager or ICT Network Supervisors are permitted to change the use or system configuration of QAT IT equipment and software. Users are permitted to change user preferences to suit their working practice or style provided the settings do not compromise security or alter operability for others.

No user may use a computer system in any way which puts files or information belonging to someone else at risk of damage. In particular, knowingly introducing a computer virus is a serious offence which may result in disciplinary action where appropriate.

Users must cooperate with the ICT Support Department in preventative or remedial action concerning equipment and data security.

Publishing, or communicating without the authority of either the Group IT Manager, CEO, Head of School of any information which allows someone else to breach the security of the computer systems is an offence. *Examples are user's passwords or loopholes in system security which a user may come across accidentally whilst making legitimate use of the facilities. All users must inform the ICT Support Department when they find evidence of failures or weaknesses in security. The Group IT Manager and ICT Network Supervisor have the authority to give information which allows a breach of security, but this would normally be confined to testing and detection purposes only.*

When requested to do so by the staff or other responsible persons, anyone using QAT communication and information technology equipment must be prepared to identify himself or herself by presenting their QAT-issued identity card.

Users are required to treat IT equipment with care, and other users and ICT Support Department staff courteously.

QAT access to the Internet is governed by respective Acceptable Use Policies (AUPs), which allows for education, research and institution business. All users must comply with this policy.

QAT systems may not be used to transmit, store or access text, images, recordings, scripts, programs or telephone calls that:

1. Will consume sufficient network or server resource as to impede the effective use of systems by other users.
2. Is likely to incur unwarranted costs on the Trust.
3. Is likely to involve users or support staff in wasted time.
4. Contain misleadingly out-of-date information.
5. Contain inaccurate or deceiving information.
6. Seeks to unreasonably trivialise, insult or degrade other individuals, groups or bodies, or infringe others' human rights.
7. Use techniques that capture or otherwise display third party information is such a way as to give the impression that they come from anywhere other than the original source.

No material may display the Trust’s logos or names, or otherwise give the impression that they are official documents, except in accordance with approved QAT policy.

No material may imply or form a contract on behalf of the Trust, except in accordance with approved QAT policy.

The Group IT Manager and other authorised staff can read any file stored on the system and, if it is necessary to safeguard the integrity of the system, to delete any file without warning.

B3. Academy IT Security Policy

Scope and Purpose

The purpose of this policy is to ensure the availability, confidentiality and integrity of IT systems which support the academic and administrative activities of the Trust. Effective security is achieved by working with a proper discipline, in compliance with legislation and QAT Policies, and by adherence to approved procedures and standards.

Objectives

The objectives of this policy are to:

- Ensure that QAT IT facilities are adequately protected against loss, misuse or abuse.
- Raise awareness of IT security issues throughout the Trust and to ensure that they are considered at every stage of an IT system life cycle.
- Ensure that users understand their responsibilities for protecting the data they handle.

Responsibilities for Information Systems Security

The Group IT Manager, ICT Network Supervisors and Executive Group are responsible for implementation of this policy and related projects.

Proposals for IT Security Projects should be made to the Group IT Manager.

The Group IT Manager and ICT Network Supervisors have the authority to take any action in the event of an ICT emergency deemed necessary to protect the Trust's systems and information within the scope of this policy.

Compliance with Legislation

The Trust has an obligation to abide by all relevant legislation. This policy and supporting policies, procedures and standards satisfy the requirement under the Data Protection Act 1998 and GDPR for a formal statement of the Academy's security arrangements for personal data. The requirement formally devolves to all users defined in Policy A.1 above, who may be held personally liable for any breach of the legislation.

Risk Assessment and Security Review

Individual users have a responsibility to identify the value of the systems and information under their control and to make provisions for their safety.

Provision of Network Services

The ICT Network Supervisor is responsible for authorising standard and non-standard services on the QAT network.

B4. Policy for Use of Information Servers

An Information Server is classified a web server, VLE or Portal, which must have an owner who is authorised by the ICT Network Supervisor or Group IT Manager.

The Information Server Owner (ISO) is responsible for compliance with all relevant Academy Policies and current legislation. *This makes the ISO responsible to different people or groups for their actions, for example, to the Data Protection Officer for compliance with Data Protection legislation, to the Group IT Manager for network functioning, for audit availability and to users for the quality of the data.*

Each ISO is responsible for the availability, accountability, authenticity, confidentiality, integrity and reliability of their systems and data.

The ISO will assess the value to the QAT of the information served, identify threats to that information and arrange safeguards which are commensurate with the identified risk.

The ISO is responsible for monitoring changes to the value of information, or the threats to it and making appropriate changes to the safeguards.

The ISO will regularly review the operation of the above safeguards to identify attempts to compromise the server. All "successful" compromises must be reported immediately to the relevant local ICT Support Team. All attempts, whether successful or not, should be reported to the ICT Network Supervisor or Group IT Manager.

The ISO will take all possible precautions to ensure that system does not interfere with the operation of any of the Trust’s IT systems.

Information Servers must be available at any time for a security audit by the QAT’s ICT Support Teams or auditors.

The ISO must ensure that it is possible to disconnect the server immediately at all times.

B5. Equipment and Software used by groups and/or individuals

The following policies apply to equipment and software which is used by an individual or shared by a group of users and are additional to the Acceptable Use Policy (AUP) and other appropriate policies. *Examples of equipment to which this policy applies are telephone handsets, AV equipment, desktop and laptop computers, individual and shared printers, photocopiers/MFDs.*

Specification and selection of IT equipment must be done by or in consultation with the ICT Support Department.

Purchase of equipment and software must be in accordance with the finance guidelines for each Academy.

The ICT Support Department will maintain a record of the current location of QAT IT equipment. Movement of normally fixed equipment should be supervised by a member of the ICT Support Team wherever possible. Where this is not possible, the ICT Support Department should be notified of all changes.

The ICT Support Department will maintain a record of all software license purchases. *All software purchases and valid license must be presented to the ICT Support Team before installation on to the Trust's network.*

Installation and upgrading of individual and workgroup equipment and software will be undertaken by the ICT Support Department or an approved contractor.

No user may install additional hardware, software or alter the configuration of any equipment except:

1. ICT Support Department staff and other authorised personnel may install hardware, software or alter equipment configuration for testing and evaluation.
2. Where hardware or software has been procured via the ICT Support Department and is accompanied by adequate instructions for installation, the hardware or software may, by mutual agreement, be given to the user for them to install. This shall be deemed as authorisation to install only this item.
3. Auto-updating software (e.g. virus signature files) originally installed and configured by the ICT Support Department may continue to install updates under the authority of the ICT Support Department.
4. Periodic updates to software may be undertaken by a member of staff provided the member of staff has adequate instructions, appropriate skill and legitimate access to the equipment involved.
5. If hardware or software, other than updates to existing software, is to be acquired by an academic member of staff other than via the ICT Support Department (e.g. by personal purchase or download from the Internet), the academic member of staff must consult with a member of the ICT Support Department for known issues concerning that hardware or software.

6. Portable computers belonging to users or their employers may be connected to the QAT network, provided that the software is adequately patched and it is protected from infection by malicious software and from transmitting malicious software to other systems. Notes of Guidance for connecting to the Trust's network will be available but no support for non-QAT equipment will be provided by the Trust. Non-QAT users, such as those from other institutions using location independent networking (LIN), must operate within the IT Policy and at the discretion of the ICT Network Supervisor or Group IT Manager.

Any installation will ensure that data is backed up before adding additional hardware or software.

No license agreement may be entered into if the consequences or potential consequences will adversely affect performance or incur direct or indirect costs on the Academy unless authorised by the Network and Systems Manager.

All installations and upgrades must be within the terms of the license agreement and must be deleted in accordance with the license.

Every user must ensure the correct use and adequate safeguarding of data for which they are responsible. This includes suitable backups of the data.

No equipment may be used to serve information except where authorisation from the Group IT Manager has been gained. *Examples of serving information include creating a Web or ftp server; allowing other computers to connect to your computer or obtain remote access.*

All portable equipment and software shall have a designated user. The designated user is the person with whom the equipment is normally lodged and this person is responsible for the security of the equipment and software. The designated user, the designated user's line manager, and the ICT Support Department have the ability to authorise the use of that portable equipment and software outside of the Trust's premises.

Equipment on temporary loan must be recorded in the relevant equipment log as being on loan to a named individual who will be responsible for the security, correct operation and condition of the equipment, and for its return in good condition within the agree period of the loan. In some cases, the loan will authorise the individual to remove the equipment from QAT premises for the period of the loan. Failure to return the equipment by the end of the loan period will be considered as theft.

No equipment may be taken off QAT premises (unless covered by a loan agreement) without the permission of the Group IT Manager or ICT Network Supervisor.

The ICT Support Department may make arrangements for the temporary provision of equipment to individuals or workgroups. Temporary provision of equipment to a student will only be made with written authorisation from the student's Personalising Learning Director or Lead Inclusion Professional. This equipment is available on a first come, first served basis.

All redundant equipment and software must be passed to the ICT Support Department for redeployment or for disposal in accordance with 'WEEE' regulations.

B6. Maintenance and support of IT equipment and software

Resources for the maintenance and support of IT equipment and software will be managed based on the needs of the Trust as a whole. Priority will be given to maintenance and support of equipment and software that is widespread or critical in nature. Lower priority will be given where equipment or software is older, less widespread or non-critical to the Trust or its Academies.

The ICT Support Department provides maintenance and support for IT equipment and software provided that it is owned, licenced or leased by the Trust.

The Trust will designate information storage formats and media that it supports. Older formats that were supported will have an obsolescence period during which the format will no longer be actively used but can be transferred to a supported format.

B7. Connection to and from accounts on QAT Systems

Health and safety

All equipment connected to the Academy network must conform to the Trust or local Academy's Health and Safety Policy.

Connections to the Academy network

Only approved equipment may be connected to or used to access the QAT network. *In particular, no wireless access points may be connected to the Trust's network without approval.* Approval is given by the Group IT Manager. Approval will not normally be given for the temporary connection of non-Q3 Academy owned or leased equipment in connection with conferences except where the user is operating in accordance with location independent networking (LIN) arrangements. *Conference use requiring Internet access should be via QAT-provided equipment, "Guest" network access or via an alternative connection to an external Internet Service Provider (such as a 4G "dongle").*

Operating procedures and conditions for all connected equipment must be approved by the Group IT Manager.

Connection of equipment to the QAT network shall only be performed by staff from the ICT Support Department or approved contractors, except that:

- Users may connect their own or their employer's laptop computer to the network provided they follow the latest guidelines available from the ICT Support Department and in accordance with LIN policies.
- All equipment connected to the QAT network must be registered with the ICT Support Department either prior to, or for the purpose of, connection. Network configuration and registration information about the network is maintained centrally by the ICT Support Department.

Remote access to the QAT network

Remote access for users to the Trust’s network will normally be via the Internet using a secure user “portal”. For details of these servers contact the ICT Support Department. Users are responsible for their own equipment and connection outside the Trust’s premises.

The Academy will not provide or maintain external connections into the QAT network except:

Where an approved contractor or service requires a dial-up link for the purposes of maintaining specific systems or services. Such connections must be set up and maintained in accordance with procedures agreed with the Group IT Manager or ICT Network Supervisor.

No user may set up or maintain a private dial-up connection into the Trust’s IT resources.

QAT Sites will be connected by a secure “VPN Tunnel” to each other. This connectivity can only be leveraged from one of the Trust’s sites. Requests outside of a Trust site to access the networks using this method will be denied.

Approved services

Only approved services may be used on the Academy network. Current approved services are determined by the Group IT Manager.

Accounts on the network

All staff whether full-time, part-time, permanent or temporary, academic guests and enrolled students may have an account on the Academy network. Temporary accounts for academic purposes may be obtained when a request is supported by a member of the Executive Group, ICT Network Supervisor or Group IT Manager. Requests must be made to the ICT Support Department.

Academic staff who retire but continue their academic association with the Trust may retain their account on the network. Periodic checks will be made on the use of the account and the account will be expired in accordance with policy when the account is no longer in use.

Every account will be set as "expired" when a member of staff's contract is ended in SIMS.Net (MIS Software) and no later than four months after the account holder leaves the employment of the Trust. *An "expired" account remains on the system and will process e-mail messages. It will not allow the account holder access to the Trust's systems.*

Every account will be deleted no earlier than 6 months and no later than 12 months after the account holder leaves QAT, unless disciplinary or investigative circumstances warrant a different course of action. *When an account is deleted, the contents of all network directories (including email directories) associated with the account will also be archived in the first instance and deleted after a <u>maximum</u> period of 12 months.*

Staff account holders may have a grace period exceeding these limits in on request to and at the discretion of the ICT Support Department.

B8. Use of e-mail

QAT e-mail systems are provided for the conduct of Trust-related business. Incidental and personal use of e-mail is permitted so long as such use does not disrupt or distract the individual from Academy business (due to volume, frequency or time expended), does not incur unreasonable cost to the Academy, and/or does not restrict the use of those systems to other legitimate users. *Users are reminded that the Academy can access their e-mail messages for operational and security purposes.*

A user's e-mail account will be assigned and named by the relevant QAT email address policy.

The facility to alias an account is available to all users on request to the ICT Network Supervisor or Group IT Manager. Domain names <u>will not</u> be aliased. Aliases must be unique and will be allocated on a first-come first-served basis. Aliases must be non-trivial and must comply with QAT policies as decided by the Group IT Manager, who has the right to refuse an alias request.

Contact e-mail addresses for sections of the Trust will be provided by an alias, in preference to a separate account, on request to the ICT Network Supervisor or Group IT Manager.

Anonymous accounts for users will not be allowed on QAT systems. *Anonymous accounts do not allow proper management, accountability or traceability and would inherently contravene IT Policies.*

Essential information may be provided to users using e-mail. Users are responsible for reading and responding as appropriate within the time limit specified in the message subject.

Trade Union representatives and members may use QAT e-mail systems for related Trade Union communications.

QAT network and e-mail systems may not be used to transmit:

- ✓ Material unrelated to Academy business including bulk e-mail transmissions (SPAM).
- ✓ Messages requesting the recipient to continue forwarding the message to others, where the message has no educational or Academy-relevant value.
- ✓ Messages with forged addresses (spoofing) or otherwise purporting to come from a source other than the true sender.

The Trust (generally at a per-Academy level) will provide the following classifications of distribution list:

- ✓ Staff classification lists. (e.g. Associate Staff, Teaching Staff, Senior Leadership Group/Team)
- ✓ Class groups. (for student messaging)
- ✓ Year groups. (for student messaging)
- ✓ Subject groups. (for staff messaging)
- ✓ Staff initiative groups. (such as Quality Assurance, Enirchment, Trip leaders)
- ✓ Governor/Trustee list

E-mail lists and their operation will be regulated by the Group IT Manager.

The Trust will designate and regulate distribution lists. Users cannot opt out of these lists. *Core announce lists are used as essential communication mechanisms between the Trust and users, so it is important that the Trust regulates their membership.*

B9. Use of the Internet

Access to the Internet (Web) is provided for research, teaching, learning and other legitimate Trust-related business. Incidental and personal use of the Internet is permitted so long as such use does not disrupt or distract the individual from QAT business (due to volume, frequency or time expended), does not incur unreasonable cost to the Academy, and/or does not restrict the use of those systems to other legitimate users.

Website pages published using QAT systems must comply with the Policy for Information Servers and the data protection guidance set out in our **Data Protection Policy**.

The Trust will provide a default home page for all browsers on its owned or leased equipment. Users must not alter this home page without legitimate reason.

Essential information may be provided to users by the QAT using the Web. Users are responsible for reading and responding as appropriate within the time limit specified at the top of the page.

It is the responsibility of the member of staff authoring the pages to comply with QAT policies regarding content, presentation, accessibility, data protection and security.

Pages containing dynamic content must have the involvement of the Group IT Manager or “Web-lead” in their development and approval for their compliance with policies. “*Dynamic content" means that the page's content may change either by user interaction or by changes in the source data used in the page. Examples of dynamic pages are: pages that rely on an element of programming for their content; pages that accept input from users; pages that use a database as their source of information.*

Students will not have access to public space, in-house web space provision will be provided by the ICT Support Department.

Only designated users by the Group IT Manager or “web-lead” may have access to the Trust’s web sites, control panel and content management pages.

B10. Use of Telephones

The telephone systems provided by QAT are provided for research, educational and other legitimate business. Incidental and personal use of the telephones is permitted so long as such use does not disrupt or distract the individual from QAT business (due to volume, frequency or time expended), does not incur unreasonable cost to the QAT, and/or does not restrict the use of those systems to other legitimate users. *Short calls of a personal nature that are required as a result of changed Academy circumstances (such as having to work late at short notice) are considered to be in support of QAT-related business and may be legitimately made. Users wishing to make private calls should normally do so using a personal mobile phone.*

Where exceptional personal circumstances may lead to infringement of this policy, users should agree with their line manager the acceptability of their telephone usage.

Each mobile phone shall have a registered user and that user will be responsible for the use and security of the phone. The registered user must report the loss of or any damage to their phone to the Group IT Manager, Director of Finance and Operations or local Finance Manager/Officer.

Where technically possible and no cost is incurred, individuals should retain their existing internal telephone number when moving to another location within an Academy of the Trust. Where this is not possible or an additional charge is associated with the provision, the old number will normally be disconnected immediately on vacating the old location. Where redirection, rather than disconnection of the old number is deemed organisationally desirable, old numbers will be redirected using the telephone management system, so that callers are informed of the new number. The period for redirection should not exceed 3 months.

Trade Union representatives and members may use QAT telephone systems for QAT-related Trade Union communications.

B11. Use of Fascimile (Fax) Machines

The Trust provides facsimile machines for research, educational and other legitimate Trust-related business. Incidental and personal use of fax is permitted so long as such use does not disrupt or distract the individual from QAT business (due to volume, frequency or time expended), does not incur unreasonable cost to the Trust, and/or does not restrict the use of those systems to other legitimate users.

The Trust's facsimile machines may not be used for the bulk distribution of commercial or non-commercial material unrelated to QAT activity.

B12. Use of photocopying and printing equipment

The QAT provides photocopiers and printers for research, educational and other legitimate Trust-related business. Incidental and personal use of photocopiers and printers is permitted so long as such use does not disrupt or distract the individual from Trust business (due to volume, frequency or time expended), does not incur unreasonable cost to the Trust, and/or does not restrict the use of those systems to other legitimate users. *In practice copying and printing will incur a cost to the Trust, however the QAT provides facilities for payment for copier and printer charges, and these should be used when appropriate.*

The Trust will make a charge for all photocopying and networked printing. The charges and waivers will be set by the QAT from time to time.

B13. IT Purchasing Policy

The Trust's Financial Guidelines and Procurement Guidelines will be followed in the purchase or lease of IT Equipment.

All procurement of IT equipment, software and services for the QAT must be made either through the ICT Support Department or in full consultation with the relevant personnel in the IT Support Department. The ICT Support Department may veto a purchase or lease if it believes that IT policies have been breached.

The QAT will abide by the EU Tendering framework, if applicable.

IT equipment, software and services for the QAT will be purchased on the basis of best value for money over the complete life cycle of the goods. *Initial cost is not the* *only criterion to be considered: support requirements, warranties, reliability of goods as well as suppliers, longevity, and disposal costs must also be considered.*

Where a non-ICT Support Department budget is being used to fund a purchase or lease, it is the budget-holder's responsibility to ensure that sufficient funds are available for the purchase and that all relevant information is supplied to the ICT Support Department to facilitate the purchase/lease.

Where existing QAT suppliers make favourable arrangements available to staff or students for equipment or software purchase, these discounts will be made available either directly between supplier and individual or via the IT Department. In the latter case, the Trust reserves the right to apply a charge to cover administration costs.

B14. Disposal of IT Equipment

All equipment will be disposed of in compliance with current legislation and with due regard for social and environmental considerations.

Disposal shall not expose the Trust to continuing commitment to support or maintain any systems.

Disposal of equipment shall constitute best value to the Trust.

Where equipment has no residual value, recycling of materials or components shall be done in as economical a way as possible.

B15. The Community beyond QAT

QAT will play a responsible role in the UK academic community in support of information technology by participating in and contributing informally to appropriate networks of contacts.

QAT should maintain formal membership of appropriate organisations in support of IT and its application in the academic community.

B16. Non-compliance with these policies

Illegal Activities

Infringements of the relevant legislation, summarised in Section B1, will result in legal and/or disciplinary action. All such infringements must be reported to the Group IT

Manager or Head of School, who have the authority to deal with minor breaches and to escalate more serious offences.

Breaches of Academy Policies

Correcting problems caused by a breach of IT policies will be done at minimum effort and cost to the Trust. QAT reserves the right to pass on some or all of the cost involved to those causing the breach.

Consequences of violations of QAT IT Policies, will depend on the intent, the seriousness of the offence and the damage caused. All such violations must be reported to the Group IT Manager or Head of School, who have the authority to deal with minor breaches and to escalate more serious offences.

ICT Support Department staff, with authorisation from the Group IT Manager, may disconnect equipment without notice if it is believed that IT Policies are breached while an appropriate investigation is carried out.

Breach of Policies by students may result in:

1. Suspension of access to IT equipment and services for minor breaches.
2. Formal disciplinary action, which may result in expulsion from an Academy or the Trust, for more serious offences.

Breach of Policies by staff may result in:

1. Suspension of access to IT equipment and services for minor breaches.
2. Formal disciplinary action which may result in expulsion from the Trust for more serious offences.

Redress

If any user believes that the action taken by QAT is disproportionate to the alleged breach of policy, they may appeal through the Academy's Grievance Procedure. *The Trust’s Human Resources department determines grievance procedures for staff use.*

Appendix 1 – Definition of Terms Used

Accountability The property that ensures that the actions of an entity may be traced uniquely to the entity. (ISO 7498-2: 1989) e.g. an audit log in a database server.

Distribution lists E-mail lists that send a single message to multiple users. Only designated editors may send to an Announce list.

Authenticity The property that ensures that the identity of a subject or resource is the one claimed. Examples of infringement include impersonation and IP spoofing.

Availability The property of being accessible and usable upon demand by an authorised entity (ISO 7498-2:1989)

Confidentiality The property that information is not made available or disclosed to unauthorised individuals, entities or processes (ISO 7498-2: 1989)

Information Server Any computer system which may be used to store and make available information. The information may be text, images, video and sound and examples of server systems include Web, E-mail, VLE, Database, Portal and FTP. Networking equipment is also considered to fall within this definition: routers, switches and hubs. The system may be operated by employees of the Trust or by a third party on behalf of the Trust.

Integrity Data Integrity is the property that data has not been altered or destroyed in an unauthorised manner (ISO 7498-2: 1989), and System Integrity is the property that a system performs its intended function free from deliberate or accidental unauthorised manipulation.

Private discussion lists E-mail lists that allow members to send a message to a list and that message gets sent to all members of that list. One person controls the list of recipients; the list is therefore "private" rather than "open" for anyone to subscribe.

Private Information Any information which has not been officially approved by a relevant QAT committee.

Reliability Consistent, intended behaviour and results.

QAT/Academy Information Information officially approved by a relevant party committee.

QAT/Academy-related business Any activity or function that directly or indirectly supports or contributes to the Trust’s core business of education.

User Any person authorised to use QAT IT systems including staff, students, visitors and contractors.

Appendix 2 – Agreements and Disclaimers

Staff Acceptable Use Policy (AUP)

ACADEMIES

Staff - Acceptable Use Policy (AUP)

In order to allow you to use the Q3 Academies Trust (QAT) ICT System; including computer equipment, video-conferencing/teleconferencing equipment, software, network(s), and Internet access; the following Acceptable Use Policies have been established:

1. The Trust dedicates the property comprising of the network and grants access to it by users only for the educational activities authorised under the Trust's Policy and Procedures.
2. The Member of Staff agrees not to use any part of the Trust's systems to harm or disrupt other people, their work, any network, hardware, software, or data. The Member of Staff will not knowingly send, install, or create a computer virus or use the Trust's systems in a way that violates the Trust policy.
3. The Member of Staff will keep their Username and Password confidential and will not reveal it to others.
4. The Member of Staff understands and agrees that their electronic mail (e-mail) and/or data on any QAT computer or media is not private and that the QAT has access to all mail and other data, including internet logs, and these may be reviewed by the QAT at any time.
5. The Member of Staff may not use the Trust's systems for financial gain or to support or oppose political candidates, groups, or ballot measures.
6. The Member of Staff will not access, submit, publish, display, and/or install on or through the Trust's systems any defamatory, harassing, obscene, sexually explicit, threatening, or illegal material or other material that is disruptive to the educational environment.
7. The Member of Staff will not use the Trust's systems to encourage use of alcohol/controlled substances or violence against others or access sites that do so.
8. The Member of Staff will treat the files of others as private and will not access anyone's folders, work, or files without that person's permission.
9. The Member of Staff will not attempt to use another person's login or password.
10. The Member of Staff understands and consents to the fact that actions taken on or through the network may be recorded and replayed, including, but not limited to, audio and video recordings through teleconferencing, videoconferencing, and/or creation of multimedia projects.
11. The Member of Staff will not install any software on Trust equipment, any software required must be authorised and installed by the ICT Support Department only.
12. The Member of Staff will not install or transmit copyrighted material through the Trust's systems illegally.
13. The Member of Staff will not attempt to bypass any of the filtering or security software. When accessing other networks or systems through the Trust's systems, the Member of Staff will abide by all rules of that network or system.
14. The Member of Staff is aware that some sites accessible through the Trust's systems may contain defamatory, inaccurate, abusive, obscene, sexually oriented, threatening, offensive, or illegal material and the Member of Staff understand that QAT does not condone the use of such materials. Members of Staff should be aware that the filtering software used by the Trust is not infallible and that users may be able to access inappropriate materials. In the event any material is accessed, the ICT Support Department must be notified immediately.
15. The Member of Staff understands and agrees that use of the QAT systems is at their own risk and QAT is not liable for harm suffered by any party as a result of using the Trust's systems.
16. The Member of Staff agrees to be accountable for their actions. If the Member of Staff intentionally or recklessly inflicts any damage or harm on any portion of the QAT's systems or to any party through the QAT's systems, the Member of Staff may be subject to discipline and restitution. If the Member of Staff observes other users violating these terms and conditions, violators will be reported to a member of the QAT Executive Group or local senior leadership group (SLG).
17. The Member of Staff may not use the Trust's systems to participate in any activities that violate UK laws, Academy policies, or these Terms and Conditions. The Member of Staff will abide by all terms listed in the QAT ICT Policy.
18. Attaching network-capable equipment to the QAT network, unless authorised by the Group IT Manager or ICT Network Supervisor, is strictly prohibited.
19. It is your responsibility to ensure that if you are to connect any QAT equipment to your home broadband connection that it is adequately secured and protected. For example, ensure that any wireless connection is encrypted using WEP or WPA encryption.

I agree to and will abide by the above Terms and Conditions. I understand that if these terms and conditions are violated, appropriate disciplinary action may be imposed, legal action may be taken, and the violation may be forwarded to the authorities for prosecution.

User Signature:		Date:	
Print Name:		Department:	

Please Tick Appropriate Box:

I have read and understand the above Terms and Conditions and I agree to be bound by them.	
I have reviewed the above Terms and Conditions and I understand each and agree to the above Terms and Conditions	

Student Acceptable Use Policy (AUP)

Acceptable Use Policy (AUP)

In order to allow you to use the Academy's ICT Systems; including computer equipment, video conferencing/ teleconferencing equipment, software, network(s), and Internet access; the following Acceptable Use Policies have been established:

The Academy dedicates the property comprising of the network and grants access to it by users only for the educational activities authorised under Q3 Academies Trust (QAT) Policy and Procedures;

1. The student agrees not to use any part of the Academy's System to harm or disrupt other people, their work, any network, hardware, software, or data. The student will not knowingly send, install, or create a computer virus or use the Academy's System in a way that violates the Academy's Policy;
2. The student will keep their Username and Password confidential and will not reveal it to others;
3. The student understands and agrees that their electronic mail (e-mail) and/or data on any Academy computer or media is not private and that the Academy has access to all mail and other data, including internet logs, and these may be reviewed by the Academy at any time;
4. The student may not use the Academy's System for financial gain or to support or oppose political candidates, groups, or ballot measures;
5. The student will not access, submit, publish, display, and/or install on or through the Academy's System any defamatory, bullying, harassing, obscene, sexually explicit, threatening, or illegal material or other material that is disruptive to the educational environment;

6. The student will not use the Academy's System to encourage use of alcohol/controlled substances or violence against others or access sites that do so;
7. The student will treat the files of others as private and will not access anyone's folders, work, or files without that person's permission;
8. The student will not attempt to use another person's username or password;
9. The student understands and consents to the fact that actions taken on or through the network may be recorded and replayed, including, but not limited to, audio and video recordings through teleconferencing, videoconferencing, and/or creation of multimedia projects;
10. The student agrees not to install any software on Academy's equipment;
11. The student will not install or transmit copyrighted material through the Academy's System illegally;
12. The student will not attempt to bypass any of the Academy's filtering or security software. When accessing other networks or systems through the Academy's System the student will abide by all rules of that network or system;
13. The student and parent are aware that some sites accessible through the Academy's System may contain defamatory, inaccurate, abusive, obscene, sexually oriented, threatening, offensive, or illegal material and the student and parent understand that Q3 Academies Trust does not condone the use of such materials. Parents of minors should be aware that the filtering software used by the Academy is not infallible and that users may be able to access inappropriate materials. In the event any material is accessed, the ICT Support Department must be notified immediately;
14. The student understands that the Academy has the right to reformat any system's drives and/or remove/relocate any given data or computer at any time and is not responsible for any loss of data;
15. The student understands and agrees that use of the Academy's System is at their own risk and Q3 Academies Trust is not liable for harm suffered by any party as a result of using the Academy's System;
16. The student agrees to be accountable for their actions. If the student intentionally or recklessly inflicts any damage or harm on any portion of the Academy's System or to any party through the Academy's System, the student will be subject to discipline and restitution. If the student observes other students violating these terms and conditions, violators will be reported to a member of the Trust's staff;
17. The student may not use the Academy's System to participate in any activities that violate UK laws, Academy or QAT policies, or these Terms and Conditions. The student will abide by all terms. A copy of which is available on request;
18. Any network-capable equipment attached to the Academy's network, unless authorised by the ICT Network Supervisor or Group IT Manager, is strictly prohibited;
19. It is your responsibility to ensure that if you are to connect any Academy equipment to your home broadband connection that it is adequately secured and protected. For example, ensure that any wireless connection is encrypted using WEP or WPA encryption.

I agree to and will abide by the above Terms and Conditions. I understand that if these terms and conditions are violated, appropriate disciplinary action may

be imposed, legal action may be taken, and the violation may be forwarded to the authorities for prosecution.

User Signature: ______________________________________ Date: ____________

User's Full Name (Please Print): ____

The parent or guardian must complete the following:
I have read and understand the above Terms and Conditions and I agree to be bound by them. I wish for my child to have access to the Academy's IT Network, including Internet access and video-conferencing opportunities.
I have reviewed and explained the above Terms and Conditions to my child and he/she understands each and agrees to the above Terms and Conditions.

Parent/Guardian Signature: ____________________________ Date: ____________

Staff Loan Laptop Agreement Example Text

(Name of Venue, i.e. Q3 Academy Langley/Great Barr varies based on issuing site)

Manufacturer:
Laptop Model:
Serial Number:
Asset Tag:
Network Name:
Staff Name:

STAFF LOAN LAPTOP AGREEMENT

This laptop will be loaned to you while you remain employed by the Trust.

Please indicate your acceptance of the conditions below by signing one copy of this form and returning it to the ICT Support Department.

Whilst the device is in your care the following conditions should be noted:

1. The device remains the property of Q3 Academies Trust and is only for the use of the person to which it is issued. The device should not be loaned to other individuals or other staff (e.g. family members or friends).
2. Insurance cover provides protection from the standard risks but excludes accidental damage and theft outside of the Trust's premises. For example, if the laptop is stolen from an unattended vehicle, you (or your own insurance) will be responsible for the cost of its replacement.
3. Only software licensed by the Trust, or its Academies, authorised by Group IT Manager or ICT Network Supervisor and installed by a member of the Trust's ICT Support Department may be used. Under no circumstance should you install any software yourself.
4. Anti-Virus software is installed and must be updated on a regular basis. The device must be connected to the Trust's network or the internet at least once per week when in use so as to allow the software to update itself.

5. In the event of a problem, do not attempt to repair the device or have it repaired yourself. The device <u>must</u> be returned to the ICT Support Department, who will take appropriate action.
6. Any charges incurred by accessing the Internet from outside Q3 Academies are not chargeable to the Trust.
7. Q3 Academies Trust policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by all users of the device.
8. You must return the device to the ICT Support Department in good condition, before you leave the Trust, or at the request of the ICT Support department staff. If you fail to do so, you agree to pay for its replacement. The Trust will invoice you for the full cost of its replacement.
9. If we ask you to return the device to the Academy/QAT for any reason, you must do so. You will be given reasonable notice of this.
10. Q3 Academies Trust is not responsible for the purchase of peripheral devices (printers etc.), software, consumables or internet costs from home.
11. The device MUST be kept in the bag/sleeve/case provided when not in use.
12. Any breach of this agreement <u>*could*</u> result in the following actions:
    A. Written warning.
    B. Confiscation and interview.
    C. Confiscation without return.
    D. You will pay costs incurred for repair or replacement.

Manufacturer:
Laptop Model:
Serial Number:
Asset Tag:
Network Name:

Staff Name:

<u>Collected by staff:</u>

Signature…………………………………………………………………………Date………………………………

<u>Returned to:</u>

Technician……………………………………………………………………Date………………………………

Student Loan Laptop Agreement Example Text

(Name of Venue, i.e. Q3 Academy Langley/Great Barr varies based on issuing site)

Manufacturer:
Laptop Model:
Serial Number:
Asset Tag:
Network Name:
Name of Student:

STUDENT LOAN LAPTOP AGREEMENT

This laptop will be *loaned* to you while you remain at the Academy.

Please indicate your acceptance of the conditions below by signing one copy of this form and returning it to the ICT Support Department.

While the laptop is in your care the following conditions should be noted:

1. The Laptop **remains the property of Q3 Academies Trust** and is only for the use of the student to which it is issued. The laptop should not be loaned to other individuals or other students (e.g. family members or friends).
2. Insurance cover provides protection from the standard risks but excludes accidental damage and theft from an un-attended car. If the laptop is stolen from an un-attended car, you (or your own insurance) will be responsible for the cost of its replacement.
3. Only software licensed by the Trust, authorised by the Group IT Manager or ICT Network Supervisor and installed by a member of the ICT Support Department may be used. Under no circumstance should you install any software yourself.
4. Anti-Virus software is installed and must be updated on a regularl basis. The laptop must be connected to the Academy network or the internet at least once per week when in use so as to allow the software to update itself.
5. **In the event of a problem, do not attempt to repair the computer or have it repaired yourself.** The computer must be returned to the ICT Support Department, who will take appropriate action.
6. Any charges incurred by students accessing the Internet offsite are not chargeable to the Trust.
7. Q3 Academies Trust (QAT) policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by all users of the laptop.
8. You must return the laptop to the ICT Support Department, in good condition, before you leave the Academy or at the request of the ICT Support department staff. If you fail to do so you agree to pay for its replacement. The Academy will invoice you for the full cost of its replacement.
9. If we ask you to return the laptop to the Academy for any reason, **you must do so**. You will be given reasonable notice of this.
10. The Trust is not responsible for the purchase of peripheral devices (printers etc.), software, consumables or internet costs from home.
11. The laptop MUST be kept in the bag provided when not in use.
12. At the end of your time at the Academy, your examination results will be withheld until your laptop is returned or the appropriate payment made to replace it.
13. If your laptop is damaged in **any way**, for example, a broken display and the ICT Support Department assesses that this is the not the result of normal wear and tear then you will be liable for a **minimum repair charge of £50.00**. In exceptional circumstances this may be increased due to the level of damage.
14. Any breach of this agreement could result in the following actions:

a. Written warning;
b. Confiscation and interview;
c. Confiscation without return;
d. You will pay costs incurred for repair or replacement.

Manufacturer:

Laptop Model:

Serial Number:

Asset Tag:

Network Name:

Name of Student:

Collected by student:

Signature..Date..............................

Returned to:

Technician...Date..............................

Receipt of laptop S/N (Serial Here) return:

Signature..Date..............................

Technician...Date..............................

Trust Email Disclaimer Used

ICT Monitoring Statement (used pre-logon to QAT devices)