THE CONSORTIUM
ACADEMY TRUST

# ICT Acceptable Use Policy

The Consortium Academy Trust (TCAT)
An Exempt Charity Limited by Guarantee
Company Number 07665828

| | |
|---|---|
| Status: | Live |
| Policy Owner (Position) | CEO |
| Statutory / Recommended | Recommended |
| Date Adopted | 21 May 2018 |
| Review Period | 12 months initially then 24 |
| Last Review Date | March 2019 |
| Revision | 2 |
| Next Review Date | March 2021 |
| Advisory Committee | ELG |
| Linked Documents and Policies | CCTV Policy,<br>Data Protection Policy and<br>Records Management Policy |

## 1. Scope of the Policy

1.1 This policy applies to all members of The Consortium Academy Trust ("**the Trust**") community. This includes but is not limited to every employee, governor, trustee, member, worker (including any agency, casual or temporary worker), volunteer and contractor who is employed or otherwise engaged at any academy operated by the Trust and are users of any of the ICT systems at any of the Trust's academies (whether inside or outside of school hours) (each a "**System User**").

1.2 Technological methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures. The Trust has prepared this policy in order to inform you of your obligations as a System User in respect of the use of the Trust's ICT systems.

1.3 This policy should be read in conjunction with the following related Trust policies:

- Data Protection Policy
- CCTV Policy
- Records Management Policy

## 2. Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the Trust in relation to ICT security:

### 2.1 IT Manager

Each academy has access to an IT Manager, who is responsible for ensuring that:

- the academy's ICT infrastructure is secure and is not open to misuse or malicious attack
- System Users at the academy may only access the academy's networks through a properly enforced password protection policy, in which passwords are regularly changed in accordance with good practice guidance
- the academy's filtering system is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- they keep up to date with technical information in order to effectively carry out their role and to inform and update others as relevant
- use of the academy's network, remote access facility and email is regularly monitored in order that any misuse/attempted misuse can be reported to the academy's senior leaders for investigation/action/sanction
- monitoring of software/systems is implemented and updated as agreed within Trust policies
- where possible, the academy-issued devices are enabled to allow the remote blocking or deletion of data in case of theft

### 2.2 System Users

Each System User is responsible for ensuring that:

- they have an up to date awareness of ICT security matters within the academy and of the current Trust ICT Acceptable Use Policy
- they have read, understood and signed to acknowledge their understanding of this ICT Acceptable Use Policy

- they report any suspected misuse or problem relating to any academy's ICT system to their line manager for investigation/action/sanction through the Whistleblowing Policy.
- digital communications with any person (including but not limited to learners) such as via email or any other electronic messaging system should be on a professional level and only carried out using official systems
- where specifically authorised by their academy, they monitor learners' ICT activity in lessons, extracurricular and extended school activities
- they are aware of security issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement the appropriate policies with regard to these devices
- where applicable, in lessons where internet use is pre-planned, learners should be guided to sites checked as suitable for their use. Any unsuitable material that is found in internet searches must be reported to the IT Manager immediately

### 2.3 Technical

Each academy will be responsible for ensuring that the technical infrastructure of its network is as safe and secure as is reasonably possible. It will also need to ensure that the relevant people named in the above sections comply with this policy, including but not limited to as follows:

- there will be regular reviews and audits of the safety and security of the academy's ICT systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- all System Users will have clearly defined access rights to the academy's ICT systems Details of the access rights available to groups of System Users will be recorded and maintained by the academy's IT Manager and will be reviewed, at least annually.
- all System Users will be provided with a username and password by the IT department, who will keep an up to date record of users and their usernames
- System Users will be made responsible for the security of their username and password and must not allow anybody else to access the ICT systems using their log-in details and must immediately report any suspicion or evidence that there has been a breach of security or that any password may no longer be secure
- The academy maintains and supports a managed filtering service
- In the event of there being any requirement for such filtering to be switched off for any reason (whether on an individual basis or otherwise), this must be expressly authorised and logged by the academy's senior leadership team
- any filtering issues should be reported immediately to the IT Manager (who will involve the senior leadership team where appropriate)
- requests from System Users for sites to be removed from the filtered list will be considered by the IT Manager in conjunction with the senior leadership team. If the request is agreed, this action will be recorded and logs of such actions shall be maintained
- each academy's IT department has the facility to monitor and record the activity of System Users on the academy's ICT systems. System Users will be made aware of this
- remote management tools are available to appropriately authorised staff to control workstations and view System User activity
- tapes and disks are cleansed or destroyed after use. Simply deleting information from them does not prevent the information from being recovered at a later date
- appropriate security measures are in place to protect the academy's servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the academy's systems and data

- guests (e.g. trainee teachers and visitors) may be given temporary access to academy wi-fi networks by authorised personnel providing them with the relevant password
- this policy is in place regarding the downloading of executable files by System Users (see 4.2)
- this policy is in place regarding the extent of personal use that System Users are allowed on academy-issued laptops and other portable devices (see 4.2)
- this policy restricts System Users from installing programmes on academy workstations and / or portable devices
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by System Users on academy workstations and / or portable devices
- the academy infrastructure and individual workstations are protected by up to date virus software and are backed up regularly in order that they can be restored in a timely manner in the event of a security incident
- personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured

## 3. Training

Where appropriate, System Users will receive additional training in respect of the Trust's ICT security procedures. This may include the following:

- all new staff will receive ICT security training as part of their induction programme, ensuring that they fully understand the contents of this policy and our related procedures
- each IT Manager will receive updates through attendance at training sessions and by reviewing related guidance documents
- this ICT Acceptable Use Policy and any updates to it will be presented to and discussed with System Users
- each IT Manager will provide advice/guidance/training on ICT security matters as required
- System Users will act as good role models in their use of ICT, the internet and mobile devices

## 4. Use of Digital and Video Images

4.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. Each academy will inform and educate their System Users about these risks.

4.2 Each System User must observe the following:

- System Users will only take digital/video images using an academy-issued camera or academy-issued portable device. Personal equipment of System Users must not be used for such purposes.
- System Users are allowed to take digital/video images to support educational aims, but must follow the rules below concerning the sharing, distribution and publication of those images.

- Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals, the academy or the Trust into disrepute.
- Learners must not be permitted to take, use, share, publish or distribute images of others without their permission.
- Written consent from the relevant learner's parent/carer must be obtained before any photograph or video of any learner is published internally or externally (e.g. on display boards and screens, or on the academy's or the Trust's website, Twitter and Facebook pages).
- Published photographs that include learners will be selected carefully and will comply with good practice on the use of such images.
- Learners' full names will not be used anywhere on any external publication (e.g. website or social media).
- When using digital images, staff should inform and educate learners appropriately about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet.

## 5. Use of ICT Systems by System Users

5.1 Each System User must:

- at all times take care to ensure the safe keeping of academy and Trust ICT systems to minimise the risk of loss or misuse
- store academy and Trust information on the central ICT network and not on individual computers
- ensure that any electronic device used is properly "logged-off" at the end of any session and initiate a password-protected screensaver when leaving their computer unattended to prevent anyone else accessing the network using their log-in identity
- only transfer data using encrypted and secure password protected devices
- not allow others to access academy or Trust ICT systems (including but not limited to by sharing usernames or passwords)
- not access or attempt to access academy or Trust ICT systems using another person's account
- not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised
- not install or download any hardware or software without approval from the academy's IT Manager
- where issued with an academy or Trust mobile telephone, laptop, tablet computer or similar electronic device, only use such a device in accordance with this policy and any other instructions given by the Trust or academy, and shall not use such a device for any unauthorised purpose.
- not use their personal laptops for processing personal or special category data. Such information should only be processed on a secure network using academy or Trust equipment. However, lesson planning and work of anonymised groups or any work of a non-personal nature may be performed on a staff member's own device. If the System User has any queries regarding this then they must seek the advice of the Academy Data Protection Link.
- take care when synchronising any portable device such as a tablet computer with any Trust or academy ICT systems in order that they only synchronise with those parts of the network which that System User is authorised to access
- not establish Internet or other external communications connections that could enable a third party to access our computer systems

- not access external networks or computers via academy or Trust networks without prior permission from the academy's IT Manager
- immediately report any damage or faults involving equipment or software to the academy's IT department (however caused)

5.2 When personal data is stored on any portable computer system, USB stick or any other removable media:

- the device must be encrypted and password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete
- the device must be kept in a locked filing cabinet, drawer or safe when not in use

5.3 Each System User must observe the following rules in relation to communication technologies when on any Trust academy site:

| | Allowed | Allowed at restricted times | Prohibited |
|---|---|---|---|
| Mobile phones may be brought to school | ✓ | | |
| Use of mobile phones in lessons | | ✓ (to access apps with the teacher's consent) | |
| Use of mobile phones in social time | ✓ | | |
| Taking photos on mobile phones or other camera devices | | | ✓ |
| Use of hand held devices e.g. PDAs, PSPs | ✓ | | |
| Use of personal email addresses on Academy networks | | | ✓ |
| Inappropriate use of school email for personal emails | | | ✓ |
| Use of chat rooms / facilities | | | ✓ |
| Use of instant messaging | | ✓ | |
| Use of social networking sites | | ✓ (only permitted on System Users own mobiles) | |
| Use of blogs | ✓ | | |

- Each academy's official email service may be regarded as safe and secure. System Users should therefore use only their academy's email service to communicate when using academy systems (e.g. by remote access).

- System Users should note that each academy's computer network and email system is the Trust's property. All uses of the internet and all emails sent and received, including by remote access, may be subject to access and monitoring by the academy at the academy's discretion. Each academy may also delete messages or prevent messages being sent from the email system at its discretion and may disclose details about System Users' use of email and the Internet as required to comply with legal and contractual obligations.
- System Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between System Users and learners or parents (e.g. via email or any other electronic messaging system) must be professional in tone and content. These communications may only take place on official academy systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Personal information must not be posted on any academy or Trust website or social media pages other than in accordance with Trust policies and procedures.
- Any System User who uses a tablet computer or other hand-held device away from Trust or academy premises must take appropriate additional precautions to safeguard the security of such equipment. Such precautions include but are not limited to keeping the device either with the System User or in a secure location at all times. Documents, tablet computers and other devices containing Trust or academy information should never be left unattended in vehicles (even when the vehicle is parked at the System User's home). In the event that any such device is lost or stolen, or a System User believes that it may have been accessed by an unauthorised person or otherwise compromised, they must report it to their academy's IT department immediately.
- Electronic copies of emails should generally only be retained in System Users' inboxes or elsewhere on the network for as long as they are needed for the purpose for which they were sent or received.
- Incoming emails that contain attachments could contain viruses. System Users must not open any attachment without first checking to ensure that it is virus-free unless they are certain that they originate from a safe source. All incoming emails are automatically scanned for viruses by the ICT system and the results of each anti-virus scan can be found at the footer of the relevant email. If no such results can be seen in any email received by a System User, they must contact their academy's IT department and not open any attachments to the email unless told by their academy's IT department that it is safe to do so.

## 6. Inappropriate Activities

6.1 System Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments which are offensive, obscene, demeaning, indecent, disruptive, discriminatory, including but not limited to material that contains or relates to:

- child sexual abuse images
- promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm

- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

6.2 System Users must not use any academy or Trust ICT systems for:

- running a private business
- excessive or inappropriate personal use
- accessing or using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy or the Trust
- uploading, downloading or transmitting files, commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- non-educational online gaming or video broadcasting
- online gambling
- accessing social networking sites
- file sharing (other than using any official file sharing system implemented by the Trust or the academy for use by System Users)
- corrupting or destroying the data of any other person or causing deliberate damage to hardware or software
- sending any email, text or instant message that is offensive, harassing or of a bullying nature, or sending any electronic chain mail, anonymous mail or material which infringes the intellectual property rights of a third party
- any action which could compromise the professional standing of that System User or anybody else
- accessing proxy sites or subverting any of academy or Trust filtering system
- breaching copyright or licensing regulations

## 7. Responding to Incidents of Misuse

Each System User has a duty to be a responsible user of ICT and to follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

- Any System User found to be in breach of this policy may be subject to disciplinary proceedings which in serious cases, or in cases of repeated breach, may result in dismissal. Any System User who is in any doubt about the terms of this policy or has any questions regarding this policy should contact their academy's IT Manager for further guidance.
- If any apparent or actual misuse appears to involve illegal activity including child sexual abuse images, adult material which potentially breaches the Obscene Publications Act or criminally racist material then the police will be contacted.

## 8. Additional Information

8.1 This policy does not form part of any employee's contract of employment and it may be amended by the Trust at any time. Any changes will be notified in writing.

8.2 This policy will be reviewed every two years to ensure it is achieving its stated objectives.