Three Counties Academy Trust

Staff ICT and Electronic Devices Policy

#FI16

Last amended 13th March 2026 (v1.1)

Subject to periodic review. To be reviewed no later than 12th March 2029

Version history

Date	Version	Details	Actioned by	PDF to Websites	Word to Governor Hub
13.03.26	1.1	Formatted to house style and checked against model for updates	MF	✓	✓

Contents:

Common abbreviations and acronyms

AA	Admissions Authority	**GPA**	Government Procurement Arrangement
AAI	Adrenaline Auto-Injector (Epi Pen)	**HASH**	Herefordshire Association of Secondary Heads
ACM	Asbestos Containing Materials	**HBV**	Honour Based Violence
AFH	Academies Financial Handbook	**HR**	Human Resources
AHT	Assistant Headteacher	**H&S**	Health and Safety
AIR	Attendance Intervention Reviews	**HoS**	Head of School
APIs	Application Programme Interfaces	**HSE**	Health and Safety Executive
BAME	Black, Asian and Minority Ethnic Backgrounds	**ICO**	Information Commissioners Office
BCP	Business Continuity Plan	**IHP**	Individual Healthcare Plan
BFR	Budget Forecast Return	**IRMS**	Information and Records Management Society
CAMHS	Child and Adolescent Mental Health Services	**IWF**	Internet Watch Foundation
CEO	Chief Executive Officer	**KCSIE**	Keeping Children Safe in Education
CFO	Chief Financial Officer	**KS1/2/3/4**	Key Stage 1/2/3/4
CIF	Condition Improvement Fund	**LAC**	Looked After Child
CIN	Child in Need	**LADO**	Local Authority Designated Officer
CLA	Children Looked After	**LGB**	Local Governing Body
CMIE	Child Missing in Education	**LLC**	Low-Level Concerns

COO	Chief Operating Officer	**LSA**	Learning Support Assistants
COSHH	Control and Substances Hazardous to Health	**MASH**	Multi-Agency Safeguarding Hub
CP	Child Protection	**MAT**	Multi-Academy Trust
CPD	Continuing Professional Development	**MFA**	Multi-Factor Authentication
CSCS	Children’s Social Care Services	**MFL**	Modern Foreign Language
CSE	Child Sexual Exploitation	**NCSC’s**	National Cyber Security Centres
CTIRU	Counter-Terrorism Internet Referral Unit	**NPQEL**	National Professional Qualification in Executive Leadership
CWD	Children with Disabilities	**PA**	Persistent Absence
DBS	Disclosure and Barring Service	**PAN**	Published Admission Number
DDSL	Deputy Designated Safeguarding Lead	**PECR**	Privacy and Electronic Communications Regulations
DfE	Department for Education	**PEP**	Personal Education Plan
DHT	Deputy Headteacher	**PEEP**	Personal Emergency Evacuation Plan
DSE	Display Screen Equipment	**PEx**	Permanent Exclusion
DSL	Designated Safeguarding Lead	**PLAC**	Previously Looked After Child
DPO	Data Protection Officer	**PP**	Pupil Premium
EAL	English as an Additional Language	**PSHE**	Personal, Social and Health Education
ECT	Early Career Teacher	**PSED**	Public Sector Equality Duty

EHA	Early Help Assessment	**PTFA**	Parent, Teacher and Friends Association
EHCNA	Education, Health and Care Needs Assessment	**RIDDOR**	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
EHCP	Education, Health and Care Plan	**RHE**	Relationships and Health Education
EHE	Elective Home Education	**RSHE**	Relationships, Sex and Health Education
ELSA	Emotional, Literacy and Support Assistant	**SALT**	Speech and Language Therapist
ESFA	Education and Skills Funding Agency	**SARC**	Sexual Assault Referral Centre
EVC	Educational Visit Coordinator	**SBM**	School Business Manager
EWO	Education Welfare and Safeguarding Support Officer	**SCCs**	Standard Contractual Clauses
EYFS	Early Years Foundation Stage	**SDQ**	Strengths and Difficulties Questionnaire
FBV	Fundamental British Values	**SEMH**	Social, Emotional, and Mental Health
FGM	Female Genital Mutilation	**SENCO**	Special Educational Needs Coordinator
FOI	Freedom of Information	**SEND**	Special Educational Needs and Disabilities
FSM	Free School Meals	**SLA's**	Service Level Agreements
FTS	Find a Tender Service	**STEM**	Science, Technology, Engineering and Maths
GAG	General Annual Grant	**TA**	Teaching Assistant
GDPR	General Data Protection Regulation	**TCAT**	Three Counties Academy Trust
GIAS	Get Information about Schools	**VSH**	Virtual School Headteacher

Statement of intent

Three Counties Academy Trust (TCAT) believes that ICT plays an important part in both teaching and learning over a range of subjects, and the trust accepts that both TCAT-owned and personal electronic devices are widely used by members of staff. TCAT is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

TCAT has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the internet
- TCAT ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk
- Members of staff are protected from potential risks in their everyday use of electronic devices
- A process is in place for claiming financial payments when electronic devices are lost or damaged by members of staff

Personal use of ICT equipment and personal devices is permitted across the TCAT estate; however, this is strictly regulated and must be done in accordance with this policy, and the Social Media Policy and Online Safety Policy.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

Where legislation has been passed or updated during the shelf life of this policy, we will always apply the latest version available irrespective of the version quoted here.

This policy operates in conjunction with the following policies:

- Cyber Crash File
- Cyber Response and Recovery Plan
- Freedom of Information Policy (FI10)
- Records Management Policy (FI2)
- MAT Financial Procedures Policy (FI5)
- Loaning TCAT Equipment Policy (FI18)
- Data Protection Policy (FI20)
- Complaints Policy and Procedure (GN9)
- Disciplinary Policy and Procedures (HR3)
- Photography and Images Policy (SG9)
- Social Media Policy (SG24)
- Online Safety Policy (SG43)

2. Roles and responsibilities

The Trust Board has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The Executive Headteacher/CEO is responsible for:

- Reviewing and amending this policy in consultation with the ICT Technician and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures
- The overall allocation and provision of resources. This duty is carried out daily by the ICT Technician
- Informing staff that the school reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy

The Headteacher/Head of School is responsible for:

- The day-to-day implementation and management of the policy
- Handling complaints regarding this policy as outlined in the Complaints Policy and Procedures
- Ensuring all staff in their school are aware of, and comply with, the data protection principles outlined in TCAT’s Data Protection Policy

The ICT Technician is responsible for:

- Ongoing checks on internet activity of all user accounts and to report any inappropriate use to the Executive Headteacher/CEO
- Monitoring the computer logs on TCAT’s network and to report any logged inappropriate use to the respective Headteacher/Head of School
- Remotely viewing or interacting with any of the computers on TCAT’s network. This may be done randomly to implement this policy and to assist in any difficulties
- Ensuring routine security checks are carried out on all TCAT-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks

- Accessing files and data to solve problems for a user, with their authorisation
- Adjusting access rights and security privileges in the interest of the protection of TCAT’s data, information, network and computers
- Disabling user accounts of staff who do not follow this policy, at the request of the Executive Headteacher/CEO or the Chief Financial Officer
- Assisting Headteachers/Heads of School in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy
- Assisting staff with authorised use of the ICT facilities and devices, if required
- Immediately reporting any breach of personal devices to the Chief Financial Officer and if required the DPO
- Ensuring that all TCAT-owned and personal electronic devices have security software installed, to protect sensitive data in cases of loss or theft
- Ensuring that all TCAT-owned devices are secured and encrypted in line with the TCAT’s Data Protection Policy
- Ensuring that all devices connected to the TCAT network and internet are encrypted

Staff members are responsible for:

- Obtaining approval from their Headteacher/Head of School or ICT Technician, before using TCAT-owned devices for personal reasons during school hours
- Requesting permission to loan TCAT equipment and devices from the Headteacher/Head of School or Chief Financial Officer
- Ensuring any personal devices that are connected to the TCAT network are encrypted in a manner approved by the ICT Technician
- Reporting misuse of ICT facilities or devices, by staff or pupils, to the Headteacher/Head of School

The Chief Financial Officer supported by the Academy Business Manager and ICT Technician is responsible for:

- Maintaining a Fixed Asset Register to record and monitor TCAT’s assets
- Ensuring value for money is secured when purchasing electronic devices
- Monitoring purchases made under the MAT Financial Procedures Policy
- Overseeing purchase requests for electronic devices

3. Classifications

TCAT-owned and personal devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software
- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras
- Camcorders
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Pagers
- Fax equipment
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

4. Acceptable use

This policy applies to any computer or other device connected to any TCAT network and computers.

TCAT will monitor the use of all ICT facilities and electronic devices. Members of staff will only use TCAT-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc

- Researching any school-related task
- Tuition or educational use
- Collating or processing information for TCAT business
- Communicating with other members of staff, such as contacting the school office for assistance

Inappropriate use of TCAT-owned and personal devices could result in a breach of TCAT's Data Protection Policy.

Inappropriate use of TCAT-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

Any member of staff found to have breached the TCAT's Data Protection Policy or relevant legislation will face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

Since ICT facilities are also used by pupils, each school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

Pupils found to have been misusing the ICT facilities will be reported to the Headteacher/Head of School.

TCAT-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Any illegal, inappropriate or harmful activity will be immediately reported to the respective Headteacher/Head of School.

Members of staff will not:

- Open email attachments from unknown sources
- Use programmes or software that may allow them to bypass the filtering or security systems
- Upload or download large capacity files without permission from the ICT Technician
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised contact channels
- Take any allocated classroom mobile phone off the premises, unless permitted by the Headteacher/Head of School

All data will be stored appropriately in accordance with the Data Protection Policy.

Members of staff will only use TCAT-owned electronic devices to take pictures or videos of people who have given their consent.

TCAT-owned electronic devices will not be used to access personal social media accounts.

Personal electronic devices will not be used during working hours to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing TCAT or their school online
- Avoid disclosing any confidential information or comments regarding TCAT or their school, or any information that may affect its reputability
- Have the necessary privacy settings applied to any social networking sites

Images or videos of activities including pupils, staff or parents will only be published online after consent has been sought.

Copyrighted material will not be downloaded or distributed.

TCAT-owned devices will be taken home for work purposes only, after approval has been sought from the Headteacher/Head of School and ICT Technician. Remote access to the TCAT network will be given to staff using these devices at home.

TCAT equipment that is used outside the premises, e.g. laptops, will be returned to TCAT when the employee leaves employment, or if requested to do so by the Executive Headteacher/CEO or the Chief Financial Officer.

While there is scope for staff to utilise TCAT equipment for personal reasons, this will not be done during working hours unless approved by their Headteacher/Head of School or in the case of a personal emergency.

Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Use of a TCAT-owned phone for personal use will be permitted for necessary calls lasting less than 10 minutes. A charge may be requested as a result of calls exceeding this time.

Should staff need to use the telephones for longer than this, authorisation will be sought from their Headteacher/Head of School. This authorisation will be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls; however, staff will notify their Headteacher/Head of School after the call.

Personal use of TCAT-owned equipment can be denied by the Headteacher/Head of School or the ICT Technician at any time. This will typically be because of improper use or over-use of TCAT facilities for personal reasons. A charge may be made for using equipment if the values are significant.

Where permission has been given to use TCAT equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, will be reported to their Headteacher/Head of School.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. Emails and the internet

The TCAT and school email systems and internet connections are available for communication and use on matters directly concerned with TCAT business.

Emails will not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and should be proofread by the staff member sending the email to ensure this prior to sending.

Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.

TCAT will be liable for any defamatory information circulated either within a TCAT school or to external contacts.

The TCAT and school email systems and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. TCAT and school email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

All emails that are sent or received will be retained dependent on the information contained. More information can be found in the Records Management Policy. The timeframe will be altered where an inbox becomes full.

All emails being sent to external recipients will contain the TCAT or school standard confidentiality notice. That notice will normally be configured as a signature by the ICT Technician and will not be removed.

Personal email accounts will only be accessed via TCAT computers outside of work hours and only if they have built-in anti-virus protection approved by the ICT Technician. Staff will ensure that access to personal emails never interferes with work duties.

Staff linking work email accounts to personal devices, subject to their Headteacher/Head of School approval, will sign the Device and Technology Acceptable Use Agreement for Staff and submit their devices for routine security checks on a regular basis.

The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.

Contracts sent via email, or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or TCAT or any TCAT school, and the recipient. Staff will never commit TCAT or their school to any obligations by email or the internet without ensuring that they have the authority to do so.

Purchases for equipment will only be permitted to be made online with the permission of the Headteacher/Head of School who must check the funds are available prior to authorising. A receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase will be made for the purchaser and the Academy Business Manager. This is in addition to any purchasing arrangement followed according to the MAT Financial Procedures Policy and the Financial Scheme of Delegation.

Any suspicious emails will be recorded in the incident log and will be reported to the Executive Headteacher/CEO, the Chief Finance Officer and the ICT Technician. All incidents will be responded to in accordance with the Online Safety Policy.

6. Portable equipment

All data on TCAT-owned equipment will be synchronised with our server and backed up online regularly.

Portable TCAT-owned electronic devices will not be left unattended and instead will be kept out of sight and securely locked when they are not in use.

Portable equipment will be transported in its protective case, if supplied.

Where TCAT provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, only staff will use these devices.

Before any supplied mobile phones are used, the Headteacher/Head of School, DSL and the ICT Technician will assess and ensure that the necessary software is in place to meet data protection and safeguarding requirements.

Parents will be discouraged from calling the classroom mobile phones. In emergencies, parents will contact the relevant school's emergency contact number, not the classroom phone. Parents will be permitted to text the number for justified reasons, such as being late to collect a child at the end of the day.

Parents will be asked to consent to providing their phone numbers to TCAT and their children's school, which may be kept in a classroom phone address book. This will be used to identify the number, protecting against safeguarding risks as the caller can be easily identified and to track parents who may be abusing the system.

7. Personal devices

Staff members may use personal devices in line with TCAT's Cyber Response and Recovery Plan.

All personal devices that are used to access their school's online portal, systems or email accounts, e.g. laptops or mobile phones, will be declared and approved by the Headteacher/Head of School before use and submitted for the routine checks as requested.

Staff using their own devices will give assurances to their Headteacher/Head of School that they understand the requirement for routine security checks to take place and the possibility of their personal information being seen by the ICT Technician. They will be required to provide consent to their device being accessed – if consent is refused, they will not be permitted to use a personal device.

Approved devices will be secured with a password or biometric access control, e.g. fingerprint scanner.

Members of staff will not contact pupils or parents using their personal devices.

Personal devices will only be used for off-site educational purposes when mutually agreed with the relevant Headteacher/Head of School.

Inappropriate messages will not be sent to any member of the TCAT or school community.

Permission will be sought from the owner of a device before any image or sound recordings are made on their personal device. Consent will also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken.

Members of staff bringing personal devices into a TCAT site will ensure that there is not any inappropriate or illegal content on their device.

During lesson times, unless required for the teaching activity being undertaken, personal devices will be secured.

8. Removable media

Only recommended removable media will be used including, but not limited to, the following:

- USB drives
- DVDs
- CDs

All removable media will be securely stored when not in use.

Personal and confidential information should not be stored on any removable media.

The ICT Technician will encrypt all removable media with appropriate security measures.

Removable media will be disposed of securely by the ICT Technician.

9. Cloud-based storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential, and no data is copied, removed or adapted.

10. Storing messages

Emails and messages stored on TCAT-owned devices will be stored digitally or in a suitable hard copy file and disposed of securely.

Information and data on TCAT’s network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

If a member of staff is unsure about the correct message storage procedure, help will be sought from the ICT Technician.

Employees who feel that they have cause for complaint as a result of any communications on TCAT-owned devices will raise the matter initially with their Headteacher/Head of School, as appropriate, or for members of the Central Team with the Executive Headteacher/CEO. The complaint will then be raised through the grievance procedure in line with the Grievance Policy and Procedure.

11. Unauthorised use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the Executive Headteacher/CEO or the Chief Financial Officer
- Intentionally physically damage ICT and communication facilities or TCAT-owned devices
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the ICT Technician or their Headteacher/Head of School. Certain items are asset registered, and security marked; their location is recorded by the Chief Financial Officer for accountability. Once items are moved after authorisation, staff will be responsible for notifying the Chief Financial Officer of the

new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password will be changed regularly. User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
    - Online gambling
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else
- Install hardware or software without the consent of the ICT Technician
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any TCAT computers
- Use or attempt to use TCAT's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal
- Purchase any ICT facilities without the consent of the ICT Technician or Headteacher/Head of School. This is in addition to any purchasing arrangements followed according to the MAT Financial Procedures Policy and/or the Financial Scheme of Delegation
- Use or attempt to use TCAT's phone lines for internet or email access unless given authorisation by the Headteacher/Head of School. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff will not download or attempt to download any software of this nature
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the Headteacher/Head of School. This is in addition to any purchasing arrangement followed according to the MAT Financial Procedures Policy and/or the Financial Scheme of Delegation
- Knowingly distribute or introduce a virus or harmful code onto TCAT's network or computers. Doing so may result in disciplinary action, including summary dismissal

- Use the ICT facilities for personal use without the authorisation of their Headteacher/Head of School. This authorisation will be requested on each occasion of personal use
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member it is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of their Headteacher/Head of School
- Obtain and post on the internet, or send via e-mail, any confidential information about other employees, TCAT or a TCAT school, its customers or suppliers
- Interfere with someone else’s use of the ICT facilities
- Be wasteful of ICT resources, particularly printer ink, toner and paper
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils
- Share any information or data pertaining to other staff or pupils at TCAT or their school with unauthorised parties. Data will only be shared for relevant processing purposes
- Operate equipment to record an image beneath a person’s clothing with the intention of observing, or enabling another person to observe, the victim’s genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as “upskirting”

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of TCAT-owned devices, they will report this immediately to their Headteacher/Head of School, or for members of the Central Team and Headteachers/Heads of School, with the Executive Headteacher/CEO.

12. Loaning electronic devices

TCAT equipment, including electronic devices, will be loaned to staff members in line with the Loaning TCAT Equipment Policy.

Loans will be requested using the Loan Request Form and must give appropriate notice prior to the requested loan date.

Equipment and devices will only be loaned to staff members who have read, signed and returned the terms of use, as set out in the Device and Technology Acceptable Use Agreement for Staff.

By loaning TCAT equipment and electronic devices, staff members will be agreeing to act in accordance with the terms of acceptable use.

Once a request has been authorised, the staff member will be required to undergo any training required to use the requested equipment, including how to store, handle and undertake any maintenance, e.g. changing batteries.

The maximum loan period will be five working days; however, where required, this can be extended following discussion with the Executive Headteacher/CEO.

If the equipment or device is no longer required, staff members will return the equipment to the ICT Technician as soon as possible, allowing the equipment to be made available to someone else.

Devices allowed for loan will be encrypted and protected to ensure the security of any data they hold.

13. Purchasing

Funding for electronic devices, predetermined by the Trust Board, will be available each year on request from the Academy Business Manager.

Requests for equipment or electronic devices will be made in writing to the Academy Business Manager using the approved system.

Requests will be submitted in sufficient detail for an informed decision to be made.

Requests will be responded to as soon as reasonably possible. If sufficient detail is not provided or other conditions specified by the Academy Business Manager are not met, the request will not be processed.

Requests made for equipment or electronic devices that exceed the predetermined amount allocated will require discussion and authorisation by the Trust Board.

Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on TCAT’s behalf unless permission has been sought from the Executive Headteacher/CEO or the Chief Financial Officer.

The cost of any equipment or devices personally purchased by staff members will not be reimbursed by TCAT, unless otherwise specified by the Executive Headteacher/CEO or the Chief Financial Officer.

In relation to devices for a specific project, project budget holders will provide evidence and a written statement requesting the necessary funds for the equipment required.

The Chief Financial Officer and the Academy Business Manager will seek advice from the ICT Technician and professionals when purchasing equipment.

All equipment and electronic devices will be sourced from a reputable supplier.

The Chief Financial Officer will maintain a Fixed Asset Register which will be used to record and monitor TCAT’s assets. All equipment and electronic devices purchased using TCAT funds will be added to this register.

When devices are not fit for purpose, staff members may request new equipment. If their request is granted, the old equipment or electronic device will be returned to the ICT Technician, including any accessories which were originally included with the device. Any old devices will then be disposed of or wiped clear.

14. Safety and security

TCAT’s network will be secured using firewalls in line with the Cyber Response and Recovery Plan.

Filtering of websites, as detailed in the Cyber Response and Recovery Plan, will ensure that access to websites with known malware are blocked immediately and reported to the ICT Technician.

Approved anti-virus software and malware protection will be used on all approved devices and will be updated as required.

TCAT will use mail security technology to detect and block any malware transmitted via email – this will be reviewed as required.

Members of staff will ensure that all TCAT-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades as required.

Approved personal devices will also be submitted when requested, to the ICT Technician, so that appropriate security and software updates can be installed to prevent any loss of data. Consent for such access will be obtained before the approval of a device – if consent if refused, TCAT reserves the right to decline a request to use a personal device.

Records will be kept detailing the date and time, owner of a device and device type, on which the checks have taken place.

Programmes and software will not be installed on TCAT-owned electronic devices without permission from the ICT Technician.

Staff will not be permitted to remove any software from a TCAT-owned electronic device without permission from the ICT Technician.

Members of staff who install or remove software from a TCAT-owned electronic device without seeking authorisation from the ICT Technician, may be subject to disciplinary measures.

All devices will be secured by a password or biometric access control.

Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Devices will be configured so that they are automatically locked after being left idle for a set time. This will be no more than 10 minutes for mobile or other portable devices and 15 minutes for desktop computers or laptops.

All devices must be encrypted using a method approved by the ICT Technician.

Further security arrangements are outlined in the Cyber Response and Recovery Plan.

15. Loss, theft and damage

For the purpose of this policy, **"damage"** is defined as any fault in a TCAT-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT Technician
- Unreasonable use of force
- Abuse
- Neglect

- Alterations
- Improper installation

TCAT's insurance will cover TCAT-owned electronic devices that are damaged or lost, during school hours, if they are being used on TCAT premises.

Staff members will use TCAT-owned electronic devices within the parameters of TCAT's insurance cover – if a TCAT-owned electronic device is damaged or lost outside of school hours and/or off-site, the member of staff at fault may be responsible for paying damages.

Any incident that leads to a TCAT-owned electronic device being lost will be treated in the same way as damage.

The ICT Technician and Chief Financial Officer will decide whether a device has been damaged due to the actions described above.

The ICT Technician will be contacted if a TCAT-owned electronic device has a technical fault.

If it is decided that a member of staff intentionally caused the damage and deemed liable, they will be required to pay 50% of the total repair or replacement costs. A written request for payment will be submitted to the member of staff who is liable to pay for damages.

If the member of staff believes that the request is unfair, they can make an appeal to the Executive Headteacher/CEO, who will make a final decision.

In cases where the Executive Headteacher/CEO decides that it is fair to seek payment for damages, the member of staff will be required to make the payment within six weeks of receiving the request.

Payments will be made to the Academy Business Manager, and the member of staff will be issued with a receipt.

TCAT will accept payments made via credit and debit cards, cheques and cash.

A record of the payment will be made and stored by the TCAT Finance Team for future reference.

The Executive Headteacher/CEO may accept the payment in instalments.

If the payment has not been made after six weeks, the fee will increase by 5% and continues for a maximum of six months – at which point formal disciplinary procedures will begin.

The member of staff will not be permitted to access TCAT-owned electronic devices until the payment has been made.

In cases where a member of staff repeatedly damages TCAT-owned electronic devices intentionally or through avoidable neglect, the Executive Headteacher/CEO may decide to permanently exclude the member of staff from accessing devices.

If a TCAT-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to TCAT and the school, its staff and its pupils, and that the loss is reported to the relevant agencies.

TCAT will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

16. Implementation

Staff will report any breach of this policy to the Executive Headteacher/CEO, or in the case of the executive Headteacher/CEO to the Chair of the Trust Board.

Regular monitoring and recording of email messages will be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.

Use of the telephone system will be logged and monitored.

Use of the TCAT internet connection will be recorded and monitored.

The Chief Financial Officer and Academy Business Manager will conduct random checks of asset registered and security marked items.

The ICT Technician will check computer logs on the network on a regular basis.

Unsuccessful and successful log-ons will be logged on every computer connected to TCAT’s network.

Unsuccessful and successful software installations, security changes and items sent to the printer will also be logged.

The ICT Technician may remotely view or interact with any of the computers on TCAT's network. This may be used randomly to implement this policy and to assist with any difficulties.

TCAT's network has anti-virus software installed with a centralised administration package; any virus found will be logged to this package.

TCAT's database systems are computerised. Unless given permission by the ICT Technician, members of staff will not access the system. Failure to adhere to this requirement may result in disciplinary action.

All users of the database system will be issued with a unique individual password, which will be changed as required. Staff will not, under any circumstances, disclose this password to any other person.

Attempting to access the database using another employee's user account and/or password without prior authorisation will likely result in disciplinary action, including summary dismissal.

User accounts will be accessible by the ICT Technician.

Users will ensure that critical information is not stored solely within TCAT's computer system. Hard copies will be kept or stored separately on the system. If necessary, documents will be password protected.

Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved, TCAT or the school.

Monitoring and review

This policy will be reviewed in line with the published schedule at the front of this document and at any point material changes require it by the Executive Headteacher/CEO in collaboration with the Board appointed Trustee, the Trust Board and Executive and Senior Leadership.

Any changes made to the policy will be amended by the Executive Headteacher/CEO and will be communicated to Executive Leaders, the TCAT Central Team and to Headteachers/Heads of School, who, in turn, will alert school-based staff.

The next scheduled review date for this policy is 12th March 2029.

Signed by:

______________________________ Executive Headteacher/CEO Date: ______________________________

______________________________ Board appointed Trustee Date: ______________________________

Appendix A: Device and technology acceptable use agreement for staff

Whilst Three Counties Academy Trust (TCAT) promotes the use of technology or devices and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the Headteacher/Head of School, or for members of the Central Team and Headteachers/Heads of School to the Executive Headteacher/CEO in order for any necessary further action to be taken.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

TCAT may undertake monitoring activities of employees to ensure the quality and quantity of work. TCAT will ensure that any monitoring activities undertaken are lawful and fair to employees, as well as meet data protection requirements.

If any monitoring activities are undertaken, then TCAT will ensure that employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a clearly defined purpose, and that it is as unintrusive as possible to the employees.

Information which is gathered from monitoring activities must have a lawful basis. TCAT understands and respects the rights and the private lives of workers, particularly as remote working continues to become more common. TCAT acknowledges that excessive monitoring can have adverse impacts on data protection rights and the private lives of employees

TCAT will ensure that the monitoring of workers is necessary for the identified reasons. TCAT will also ensure that all suitable safety checks are carried out prior to monitoring activities.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR
- Follow TCAT's Data Protection Policy and any other relevant TCAT and TCAT school policies and procedures

I will not:

- Attempt to bypass any filtering, monitoring and security systems
- Share school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so

Using technology in school

I will:

- Follow the Staff ICT and Electronic Devices Policy
- Only use ICT systems which I have been permitted to use
- Ensure I obtain permission prior to accessing materials from unapproved sources
- Only use the internet for personal use during out-of-school hours, including break and lunch time, except in an emergency
- Only use recommended removable media and keep this securely stored

I will not:

- Install any software onto school ICT systems unless instructed to do so by the ICT technician or Headteacher/Head of School
- Search for, view, download, upload or transmit any inappropriate material when using the internet

Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information
- Use personal email accounts to contact pupils or parents

TCAT-owned devices

I will:

- Only use TCAT-owned devices for the purpose of carrying out my school responsibilities
- Only access websites and apps that have been approved by the Headteacher/Head of School
- Understand that the usage of my TCAT-owned devices will be monitored
- Keep my TCAT-owned devices with me or within my sight at all times
- Transport TCAT-owned devices safely
- Provide suitable care for my TCAT-owned devices at all times
- Only communicate with pupils and parents on TCAT-owned devices using appropriate channels
- Ensure I install and update security software on TCAT-owned devices as directed by the ICT technician
- Seek permission from the Headteacher/Head of School before using a TCAT-owned device to take and store photographs or videos of pupils, parents, staff and visitors
- Immediately report any damage or loss of my TCAT-owned devices to the ICT technician
- Immediately report any security issues, such as downloading a virus, to the ICT technician
- Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence
- Make arrangements to return TCAT-owned devices to the ICT technician upon the end of my TCAT employment

I will not:

- Permit any other individual to use my TCAT-owned devices without my supervision, unless otherwise agreed by the Headteacher/Head of School
- Install any software onto TCAT-owned devices unless instructed to do so by the ICT technician
- Use TCAT-owned devices to send inappropriate messages, images, videos or other content
- Use TCAT-owned devices to view, store, download or share any inappropriate, harmful or illegal content
- Use TCAT-owned devices to access personal social media accounts

Personal devices

I will:

- Only use personal devices during out-of-school hours, including break and lunch times, except in an emergency
- Ensure personal devices are either switched off or set to silent mode during school hours
- Only make or receive calls in specific areas, e.g. the staff room, except in an emergency
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom
- Understand that I am liable for any loss, theft or damage to my personal devices

I will not:

- Use personal devices to communicate with pupils or parents
- Access TCAT's Wi-Fi using a personal device unless permission to do so has been granted by the Headteacher/Head of School or ICT technician
- Use personal devices to take photographs or videos of pupils or staff
- Store any school-related information on personal devices unless permission to do so has been given by the Headteacher/Head of School

Social media and online professionalism

I will:

- Follow the TCAT's Social Media Policy
- Understand that I am representing TCAT and behave appropriately when posting on TCAT or TCAT's school social media accounts
- Ensure I apply necessary privacy settings to social media accounts

I will not:

- Communicate with pupils or parents over personal social media accounts
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts
- Post any negative comments or posts about TCAT or any TCAT school on any social media platforms or other online platforms which may affect TCAT or any TCAT school's reputability

- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised TCAT contact channels

Working from home

I will:

- Ensure I obtain permission from the Headteacher/Head of School and TCAT’s Chief Finance Officer (CFO) before any personal data is transferred from a TCAT-owned device to a personal device
- Ensure any data transferred from a TCAT-owned device to a personal device is encrypted or pseudonymised
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted
- Ensure my personal device has been assessed for security by the ICT technician before it is used at home
- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working

Training

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety
- Allow the ICT technician and DPO to undertake regular audits to identify any areas of need I may have in relation to training
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices
- Deliver any training to pupils as required

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the Headteacher/Head of School, or for the Central Team and Headteachers/Heads of School to the Executive Headteacher/CEO
- Understand that my use of the internet will be monitored by the ICT technician and recognise the consequences if I breach the terms of this agreement
- Understand that the Headteacher/Head of School may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement

Monitoring staff

I understand that:

- TCAT will notify employees when monitoring takes place and that TCAT will clearly explain what personal information of mine is collected and how it's utilised and maintained
- Monitoring can be used for security purposes, managing employees' performance, and monitoring sickness and attendance
- Monitoring technologies include, but aren't limited to, camera surveillance, webcams, technologies for timekeeping and keyboard activity, productivity tools, internet activity trackers, body-worn devices, and hidden audio recording
- Personal data relating to myself which is collected from monitoring activities is securely kept and protected and isn't kept for any longer than necessary by the school
- TCAT will factor in increased expectations of privacy if I work from home
- TCAT will conduct its monitoring activities in a way that's fair and reasonably expected
- TCAT will conduct its monitoring activities with transparency, clearly explaining how and why they process my information
- TCAT will conduct its monitoring activities in a way that's accountable and compliant with UK GDPR
- I can object to having my personal information collected and processed if the lawful basis which TCAT is relying on is a public task or legitimate interests based on my personal situation
- TCAT may refuse to comply with the objection if they can demonstrate that the monitoring is for legitimate interests which override my interests, rights, and freedoms, or that the monitoring is for establishment, exercise, or defence of legal claims

- Tools for monitoring workers continue to become increasingly sophisticated, and that TCAT will inform me if they choose to use solely automated processes for monitoring activities
- I can access the information collected by TCAT by making a subject access request (SAR)
- TCAT will carry out a data protection impact assessment (DPIA) prior to undertaking their monitoring activities. Completing a DPIA identifies and minimises any potential risks that come with monitoring activities

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Name	
Signature	
Date	

Appendix B: Loan Request Form

This form should be completed by staff members when requesting to loan TCAT-owned equipment. Staff members must detail the specific equipment or device which is requested, as well as provide a reason, and where necessary, evidence, as to why the equipment or device is required.

The completed form should be returned to your Headteacher/Head of School for authorisation or for the Central Team to the Executive Headteacher/CEO.

Name		**Department**	
Equipment required			
Reason			
First date of loan		**Return date**	
Authorised (if rejected, detail why)			
Signed			
Job role		**Date**	

Appendix C: Purchase Request Form

This form should be completed by staff members when requesting funds for the purchase of equipment or an electronic device.

Before submitting the form, any evidence supporting a purchase request or demonstrating the need for the equipment should be attached.

The completed form should be returned to the Academy Business Manager for authorisation.

Name:		**Department**	
Purchase requested			
Amount required			
For use by			
Reason			
Supporting evidence			
How it will benefit pupils			

Authorised (if rejected, detail why)			
Signed			
Job role		**Date**	