Three Counties Academy Trust

Cyber-Security Policy

#FI15

Last amended 6th November 2026 (v1.0)

Policy lifespan: 3 years. Subject to annual compliance check. Next full review 5th November 2029.

Version history

Date	Version	Details	Actioned by	PDF to Websites	Word to Governor Hub
06.11.26	1.0	Formatted to house style and checked against model for updates	MF	✓	✓

Contents:

Version history

Policy abbreviations and acronyms

Statement of intent

Member, Trustee, Local Governor and Staff Summary

Parent and Pupil Summary

1. Legal framework
2. Types of security breach and causes
3. Roles and responsibilities
4. Secure configuration
5. Network security
6. Malware prevention
7. User privileges and passwords
8. Monitoring usage
9. Removable media controls
10. Home working and remote learning
11. Backing up data
12. Avoiding phishing attacks
13. Social media and website data
14. User training and awareness
15. Cyber-security incidents
16. Assessment of risks
17. Consideration of further notification

Monitoring and review

Trust Glossary

Policy abbreviations and acronyms

CEO	Chief Executive Officer
CFO	Chief Financial Officer
ICO	Information Commissioner's Office
MFA	Multi-Factor Authentication
NCSC	National Cyber Security Centre
TCAT	Three Counties Academy Trust
UK GDPR	UK General Data Protection Regulation
USB	Universal Serial Bus

NB. Where the term "parent" or "parents" is used this includes those who act as carers or have parental responsibility.
NB. Staff roles noted within this policy may also include those staff performing that role in an 'Acting' capacity.

Statement of intent

Three Counties Academy Trust (TCAT) is committed to maintaining a secure, resilient and responsible digital environment across all of our schools and central operations. TCAT recognises that effective cyber-security is fundamental to safeguarding pupils, staff and other stakeholders, protecting sensitive and confidential information, maintaining public confidence and ensuring the continuity of educational provision and essential business functions.

TCAT is committed to protecting the confidentiality, integrity and availability of its information, systems and digital infrastructure. We will implement proportionate and robust technical, organisational and procedural safeguards to prevent unauthorised access, misuse, loss, disclosure or disruption of information and services. These measures will include appropriate access controls, secure authentication, effective system maintenance, regular data backups, monitoring of potential threats and the responsible management of digital devices, networks and cloud-based services.

TCAT acknowledges that cyber-security threats are continually evolving and may arise through malicious activity, technological vulnerabilities, human error or deliberate misuse. Particular attention will be given to emerging risks, including phishing, ransomware, social engineering, identity theft, data breaches and the misuse of artificial intelligence. TCAT will promote a culture of cyber-security awareness and shared responsibility, ensuring that staff, Trustees, Local Governors and other authorised users understand their obligations and receive appropriate guidance and training to recognise, prevent and report potential threats.

Recognising that no organisation can eliminate cyber-security risks entirely, TCAT will maintain appropriate arrangements for identifying, assessing and managing vulnerabilities, responding promptly to security incidents and minimising disruption to teaching, learning and Trust operations. Effective incident response, business continuity and disaster recovery procedures will support the timely restoration of essential systems, the protection of affected individuals and compliance with relevant statutory reporting and notification requirements.

TCAT will ensure that its approach to cyber-security is consistent with applicable legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and takes account of relevant guidance issued by the Department for Education, the National Cyber Security Centre and the Information Commissioner's Office.

Through effective governance, clear accountability, regular review and continuous improvement, TCAT will seek to embed cyber-security within our organisational culture, ensuring that digital technologies are used safely, securely and effectively in support of its educational responsibilities and wider strategic objectives.

Member, Trustee, Local Governor and Staff Summary

Purpose

- Ensures TCAT protects its systems, data and digital services from cyber threats
- Supports safeguarding, business continuity, data protection and operational resilience
- Promotes a culture of cyber-security awareness and shared responsibility across TCAT

Governance and Oversight

- Trustees and Local Governors provide strategic oversight of cyber-security arrangements and risks
- Schools must maintain effective cyber-security controls, recovery plans and risk assessments
- Trustees and Local Governors should receive regular cyber-security training

Key Expectations for Staff

- Follow cyber-security procedures and acceptable use requirements
- Keep passwords secure and use multi-factor authentication where required
- Remain vigilant to phishing, malware and other cyber threats
- Report suspected cyber incidents, data breaches or security concerns immediately
- Complete mandatory cyber-security training and updates

Protecting Systems and Data

- Access to systems and information is restricted to those who need it for their role
- Networks, devices and software are securely configured and regularly updated
- Data is backed up and recovery arrangements are tested regularly
- Monitoring and filtering systems help identify and prevent threats

Managing Cyber Risks

- Cyber risks are assessed regularly and incorporated into business continuity planning
- Schools maintain response and recovery plans for cyber incidents and attacks
- Lessons learned from incidents are used to strengthen future security arrangements

Key Messages

- Cyber security is everyone’s responsibility
- Good cyber-security practice helps protect pupils, staff, information and TCAT operations
- Prompt reporting, staff awareness and strong governance are essential to reducing cyber risk and maintaining resilience across TCAT

Parent and Pupil Summary

Why this Policy Matters

- TCAT works to keep pupils, staff and families safe when using technology
- Strong cyber-security helps protect personal information, school systems and learning resources
- TCAT takes steps to prevent cyber-attacks, data breaches and online scams

How TCAT Keeps Information Safe

- School networks, devices and online systems are protected through security controls and regular updates
- Information is only accessible to authorised users who need it for their role
- Data is backed up regularly to help schools recover quickly if systems are disrupted
- Activity is monitored to identify security risks and protect users

What Parents and Pupils Can Do

- Use strong passwords and keep them private
- Be cautious about unexpected emails, messages, links or requests for information
- Report anything suspicious, worrying or unusual to the school as soon as possible
- Take care when sharing personal information online
- Follow school expectations for the safe and responsible use of technology

If a Cyber Incident Happens

- TCAT and each of our schools have plans in place to respond to cyber-security incidents and minimise disruption
- Serious incidents are investigated and managed appropriately
- Where necessary, affected individuals and relevant authorities will be informed

1. Legal framework

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

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre 'Small Business Guide: Cyber Security'
- National Cyber Security Centre 'Cyber Essentials'
- ICO 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE 'Academy trust handbook'
- DfE 'Meeting digital and technology standards in schools and colleges'
- DfE 'Plan technology for your school'

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 and school documents:

- Behaviour Policy
- Cyber Crash File
- Cyber Response and Recovery Plan
- Device & Technology Acceptable Use Agreement for Pupils
- Device & Technology Acceptable Use Agreement for Staff
- Remote Learning Policy
- Staff ICT and Electronic Devices Policy (FI16)
- Data Protection Policy (FI20)
- Business Continuity Plan (GN22(A))
- Business Continuity Policy (GN22)

- Disciplinary Policy and Procedure (HR3)
- Social Media Policy (SG24)
- Online Safety Policy (SG43)

Central TCAT policies have the policy number identified, e.g. “SG1”. Where no policy number is identified this indicates the policy is a school specific policy available from an individual TCAT school’s website.

2. Types of security breach and causes

Unauthorised use without damage to data – involves an unauthorised person accessing TCAT devices, network, systems, services or data without necessarily altering or deleting information. This includes unauthorised people within the school, e.g. schools where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where users are given administrator-level access that is not required for their role.

Malware and ransomware attacks – involve malicious software being introduced to a device, network or system. Malware may be used to damage, disrupt, access or steal data, while ransomware may prevent access to data or devices and demand payment to restore access.

Denial of service attacks – involve attempts to make a network, system or service unavailable by overwhelming it with traffic or requests, which may disrupt TCAT’s operations.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in TCAT’s ICT systems, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence, as outlined below:

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow
- Malicious breaches can occur where an individual or organisation deliberately attempts to access, disrupt or damage TCAT's devices, network, systems, services or data, including through malware, ransomware, phishing or other forms of social engineering
- Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school policies and procedures or allowing pupils to access data without authorisation and/or supervision

Cyber security incidents may also arise from technical vulnerabilities or system issues, including incorrect installation or configuration, unsupported or outdated software, inadequate security controls or operational errors:

- Anti-malware software that is incorrectly configured, not actively monitored or not kept up to date can leave devices, systems and data vulnerable to malware and other cyber attacks
- Incorrectly configured or outdated firewalls, or inappropriate firewall rules, can expose TCAT's network, systems and data to unauthorised access and cyber attacks
- Operational errors or inadequate backup arrangements can result in data being lost, overwritten, corrupted or unavailable when it is needed

3. Roles and responsibilities

The Trust Board, and where delegated, Local Governing Bodies are responsible for:

- Ensuring TCAT and our schools have appropriate cyber-security measures in place, including any cyber response and recovery plans
- Ensuring TCAT and our schools have an appropriate approach to managing data breaches in place
- Supporting the Executive and Central Team, Executive Headteachers, Headteachers and Heads of School and other relevant staff in the delivery of this policy
- Ensuring TCAT and our schools meet the relevant cyber-security standards
- Providing oversight of cyber security and strategic cyber risk management, including considering significant cyber risks and issues escalated by SLT digital leads and the Senior ICT Technician
- Ensuring at least one current Local Governor per TCAT school and one current Trustee undertakes cyber-security training at least annually

The CEO will be responsible for:

- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including TCAT's Online Safety Policy

Executive Headteachers, Headteachers and where delegated, Heads of School will be responsible for:

- Being accountable for ensuring their schools create and implement an effective cyber awareness plan for pupils and staff
- Ensuring all of their staff members and pupils are aware of their responsibilities in relation to this policy
- Ensuring appropriate user access procedures are in place within their schools
- Responding to alerts for access to inappropriate content in line with TCAT's Online Safety Policy
- Ensuring appropriate cyber-security training and awareness activities are provided for pupils, staff and other relevant users
- Ensuring a log of cyber-security incidents and attacks is maintained for their schools
- Appointing a cyber recovery team and SLT Digital Lead, who is responsible for implementing TCAT's and the school's procedures in the event of a cyber-security incident in line with the school specific Cyber Response and Recovery Plan and Cyber Crash File

SLT Digital Leads will be responsible for:

- Ensuring their school is meeting the core cyber security standards as outlined in the DfE's 'Meeting digital and technology standards in schools and colleges'
- Leading on the strategic oversight of cyber security across their school
- Working with the support of the Senior ICT Technician and CFO to plan, prioritise and review cyber security controls and improvements
- Coordinating their school's annual cyber-security risk assessment and Cyber Crash File, ensuring they are reviewed every term, and following any significant technology or process change or cyber incident or attack
- Collecting relevant information from key staff to identify their school's greatest cyber risks, their likelihood and potential impact
- Ensuring cyber-security incidents and attacks are recorded and reviewed to identify common themes, vulnerabilities and areas for improvement
- Ensuring that cyber risks, vulnerabilities and incidents are escalated appropriately
- Working with their Executive Headteacher, Headteacher, Head of School, Local Governing Body, DPO, DSL and other relevant staff to ensure their school's approach is effective and proportionate

- Ensuring that acceptable use, training, incident reporting, access controls, anti-malware, firewall protection and backup arrangements are reviewed regularly
- Overseeing the maintenance of up-to-date documentation relating to their school's network and digital technology
- Coordinating the development and implementation of acceptable use agreements and cyber-security training and awareness activities
- Working with relevant business, finance and estates staff to ensure cyber risks are reflected in TCAT's risk register and their school's Business Continuity Plan, physical risks to digital technology are identified, and appropriate resources are planned for

DSLs will be responsible for:

- Monitoring online safety incidents which could result in data breaches and reporting these to the DPO
- Acting as the named point of contact within their school on all online safety issues

The DPO and where required, the CFO will be responsible for:

- Advising TCAT and our schools on data protection risks and compliance in relation to their cyber-security arrangements
- Ensuring the plans and actions of TCAT and our schools relating to data and cyber security are compliant with data protection laws
- Advising on and supporting TCAT and our schools response to personal data breaches, including determining whether notification to the ICO or affected individuals is required
- Assessing the risks to TCAT and our schools in the event of a cyber-security breach
- Working with the Senior ICT Technician, Online Safety Coordinator and school leaders after a data security breach to determine where weaknesses lie and improve security measures
- Advising on data protection training requirements, including where more frequent training is appropriate for staff with access to higher-risk data
- Working with SLT Digital Leads to ensure records of processing activities are completed and maintained for systems that store or process personal and sensitive personal data

The Senior ICT Technician will be responsible for:

- Maintaining accurate and up-to-date registers of TCAT and our schools digital technology, software and systems

- Ensuring digital technology and software is appropriately licensed, supported and kept up to date, and that unnecessary or unsupported software is removed
- Ensuring all software is kept up to date including running security updates and patches
- Implementing, securely configuring, maintaining and actively monitoring appropriate firewalls in accordance with the DfE's technical requirements
- Installing, monitoring and reviewing filtering systems for the TCAT or school network
- Setting up user privileges in line with recommendations from the CEO, CFO, Executive Headteachers, Headteachers or where delegated Heads of School
- Maintaining appropriate records of user accounts and access privileges
- Maintaining up-to-date network documentation, including network diagrams, changes, settings and IP addressing information
- Managing user accounts and access privileges, including implementing appropriate processes for joiners, movers and leavers and removing access when it is no longer required
- Performing a secure back-up of all electronic data held by TCAT and our schools, ensuring detailed records of findings are kept
- Ensuring appropriate, current and supported encryption standards are used where encryption is required
- Ensuring appropriate anti-malware software, including antivirus protection, is centrally managed, actively monitored and kept up to date on relevant devices and TCAT-managed cloud-based servers
- Recording any alerts for access to inappropriate content and notifying the appropriate school leader
- Monitoring TCAT and our schools digital technology for potential cyber-security incidents and attacks and investigating relevant security alerts
- Checking and approving applications and software before installation or use to ensure they do not present an unacceptable security risk
- Maintaining a current list of approved applications
- Configuring the network to minimise the potential spread of malware to critical systems
- Working with digital technology suppliers and outsourced IT providers, where applicable, to ensure relevant cyber-security requirements are met

The Online Safety Coordinator will be responsible for:

- Supporting SLT Digital Leads and DSLs in delivering training and resources relating to online safeguarding risks and preventative measures

- Taking responsibility for online safety across TCAT and promoting online safety measures to parents
- Liaising with relevant members of staff on online safety matters, e.g. the DPO, DSLs, CFO, Senior ICT Technician, and school leaders

DSLs will be responsible for:

- Assessing whether there is a safeguarding aspect to any cyber-security or other data breach incident and considering whether any referrals need to be made
- Working with their SLT Digital Lead, DPO and the Senior ICT Technician to ensure cyber-security training, acceptable use agreements and relevant security arrangements appropriately reflect safeguarding requirements

All staff members will be responsible for:

- Understanding their responsibilities in regard to this policy
- Undertaking appropriate training as and when directed
- Following TCAT and their school's procedures for the secure use of digital technology and not installing software or applications without appropriate authorisation
- Complying with the Staff ICT and Electronic Devices Policy
- Keeping login details secure and following TCAT and their school's requirements for passwords and multi-factor authentication
- Remaining vigilant to cyber-security risks, including phishing and social engineering
- Reporting suspected cyber-security risks, incidents or attacks promptly in accordance with TCAT and their school's reporting procedures

4. Secure configuration

TCAT and our schools will ensure that all devices, systems and software are securely configured to reduce vulnerabilities and minimise the risk of unauthorised access or cyber-attack.

An up-to-date inventory will be maintained of the digital technology, software and systems used throughout TCAT. The inventory will be reviewed regularly and updated when changes are made. All digital technology will be appropriately licensed, supported and kept up to date.

The Senior ICT Technician will regularly review TCAT's digital technology to ensure software and operating systems remain supported and up to date.

TCAT will ensure that security updates and patches are applied in a timely manner across all TCAT systems and schools. High-risk vulnerabilities will be prioritised and addressed as soon as possible in line with recognised best practice. Unsupported or outdated systems will be replaced or upgraded wherever possible. Where this is not immediately possible, they will be isolated or have restricted access to reduce risk.

Default configurations on devices and systems will be reviewed and securely configured to remove or disable unnecessary features, services and access points. Default administrator passwords will be changed before devices or systems are put into use.

Only applications approved by the Senior ICT Technician will be installed or used on TCAT's networks. All current and future applications, including cloud-based services, will be checked to ensure they do not pose an unacceptable security risk. Applications will only be installed where they can be verified as coming from a known supplier.

The Senior ICT Technician will maintain a current list of approved applications and remove unnecessary software in line with TCAT and our schools organisational needs.

Custom-built or commissioned applications will be developed securely and in line with the UK Software Security Code of Practice.

The Senior ICT Technician will configure and manage browser settings to ensure the highest appropriate level of protection is enabled, and users cannot change settings to install unauthorised browser extensions or bypass security features. Email systems will be securely configured to reduce the risk of third parties sending imitation emails.

The Senior ICT Technician will document how digital technology is configured, including which security features have been enabled or disabled and whether there are any conflicting security features.

The Senior ICT Technician will:

- Protect digital technology with a correctly configured boundary firewall or software firewall, including protection against denial-of-service attacks
- Change the default administrator password and restrict remote access on each firewall to only those who require access for maintenance purposes

- Protect access to the firewall's administrative interface with multi-factor authentication (MFA), where available, and prevent access from the internet except for those who need to maintain the firewall
- Keep boundary firewall firmware up to date and on supported versions, checking this at least termly
- Ensure all external connections to TCAT and our schools networks run through the firewall
- Actively monitor firewall traffic and enable firewall alerts to help detect suspicious activity, using firewall logs to support this monitoring
- Block inbound unauthenticated connections by default
- Document and review the reasons why inbound traffic has been permitted through the firewall at least termly
- Keep firewall rules to an absolute minimum, ensuring each rule is documented and subject to a risk assessment
- Enable a software firewall for digital technology used outside TCAT, including when used at home or on public Wi-Fi
- Consider the use of a virtual private network (VPN) to encrypt data sent and received by devices used outside TCAT

5. Network security

TCAT will ensure that our network and digital infrastructure are secure using appropriately configured firewalls, monitoring, and secure configuration controls to prevent unauthorised access and reduce the risk of cyber incidents and attacks.

In line with the UK GDPR, TCAT will appropriately test, assess, and evaluate any security measures put in place on a regular basis to ensure these measures remain effective.

TCAT will ensure that:

- All external connections to the network pass through a properly configured boundary firewall
- Unauthenticated inbound connections are blocked by default
- Firewall rules are kept to a minimum, documented, risk assessed and reviewed at least termly
- The reasons for permitting particular inbound traffic are documented and reviewed at least termly
- Boundary firewall firmware is kept up to date and on supported versions, with this checked at least termly
- Appropriate protection is in place against denial-of-service attacks

Access to firewall administration will be restricted to authorised personnel only. Where available, MFA will be used to protect access to firewall management interfaces. Remote access will be restricted to those who require it for maintenance purposes. Default administrator passwords will be changed.

TCAT will ensure that firewall activity is actively monitored. Alerts and logging will be enabled to detect suspicious activity, and logs will be reviewed regularly by ICT support.

All firewall arrangements, whether centrally managed or locally deployed, will meet the minimum-security requirements set out in this policy.

TCAT's firewalls will be deployed centrally, which means the broadband service connects to a firewall that is located within a data centre or other major network location.

As TCAT's firewall is managed by a third-party provider, the firewall management service will be thoroughly investigated by the Senior ICT Technician to ensure that:

- Configuration changes requested by authorised users are implemented promptly by the provider
- Security patches, firmware updates and fixes are applied in a timely manner
- The service meets the firewall security and monitoring requirements set out in this policy

The Senior ICT Technician will maintain up-to-date documentation of the school's network, including network diagrams, settings, configuration changes and IP addressing information.

Network documentation will be updated whenever a significant change is made to the network.

TCAT will ensure that our digital technology and software is appropriately licensed, supported and kept up to date.

TCAT will ensure that software firewalls are enabled on devices used outside of the TCAT network, including those used at home or on public Wi-Fi.

Unsupported digital technology and software will be replaced or upgraded as soon as practicable. Where this cannot be done immediately, the Senior ICT Technician will take appropriate measures to reduce the associated risk, including isolating affected technology or removing its access to the internet where appropriate.

Where appropriate, TCAT will consider the use of a virtual private network (VPN) to encrypt data transmitted between devices and TCAT networks.

6. Malware prevention

TCAT understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media.

SLT Digital Leads will be accountable for ensuring that appropriate anti-malware controls are in place and are effective. They will work with the Senior ICT Technician to review risks, monitor effectiveness and ensure that malware protection arrangements meet their school's needs.

The Senior ICT Technician will ensure that anti-malware software, including antivirus protection, is installed on all TCAT devices, including cloud-based servers managed by TCAT. Anti-malware software will be centrally managed, actively monitored and kept up to date with the latest security updates and definitions.

Anti-malware arrangements will be reviewed at least termly to ensure they continue to meet TCAT's needs.

SLT Digital Leads will ensure that filtering and monitoring arrangements are effective and aligned with safeguarding and cyber security requirements.

TCAT's filtering provider will be:

- A member of Internet Watch Foundation (IWF)
- Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- Effective at blocking access to illegal content

The filtering system will be able to identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them, and provide alerts when any web content has been blocked

Filtering of websites will ensure that access to websites with known malware are blocked immediately and reported to the Senior ICT Technician.

TCAT will use mail security technology, which will detect and block any malware that is transmitted by email. Anti-malware software will scan attachments on both incoming and outgoing emails. This will also detect any spam or other messages which are designed to exploit users. The Senior ICT Technician will ensure that mail security technology is actively monitored, maintained and kept up to date to detect and block malicious content and phishing attempts.

Only approved applications from trusted sources will be installed on school devices. This will be subject to appropriate approval and oversight. Where apps are installed, ICT support will keep up to date with any updates, ensuring staff are informed of when updates are ready and how to install them.

TCAT will use anti-malware software that:

- Is set up to scan files upon access, when downloaded, opened, or accessed from a network folder
- Scans web pages as they are accessed
- Prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement
- Alerts the Senior ICT Technician when malware is detected so that appropriate action can be taken, including removing the malware or isolating the affected device where necessary

The use of USB storage devices will be prohibited by default unless there is a specific need for their use, e.g. where required by an examination board. Where USB storage devices are permitted, they will be scanned for malware before their contents are made available to staff or pupils.

TCAT will configure our network and systems to minimise the spread of malware and protect critical systems from infection.

7. User privileges and passwords

TCAT and our schools will ensure that user accounts and access privileges are controlled effectively so that pupils, staff and third parties only have access to the systems, services and data they need.

TCAT and our schools will ensure that all users are authenticated through unique user accounts and credentials before being granted access to devices, systems or services.

TCAT and our schools will apply the principle of least privilege. Access to systems, data and administrative functions will be granted only where it is necessary for the user's role. Access rights will be proportionate, documented where appropriate, and reviewed regularly.

TCAT will ensure that the Senior ICT Technician works with Executive Headteachers/Headteachers/Heads of School, SLT Digital Leads, the CFO and other relevant staff to operate a clear process for joiners, movers and leavers. This process will ensure that:

- Accounts are created only where authorised
- Access rights are appropriate to role and responsibility
- Changes in role lead to a review of access permissions
- Accounts are disabled promptly when a user leaves or no longer requires access
- Unused, dormant, guest and unnecessary administrator accounts are removed or disabled

TCAT will ensure that privileged or administrative access is more tightly controlled than standard user access. Administrative accounts will:

- Only be provided to authorised users who need them
- Not be used for routine day-to-day activities such as email or general browsing
- Be separate from standard user accounts wherever possible
- Be subject to enhanced monitoring and stronger security controls

Changes to administrative privileges will be approved through an appropriate process. Emergency access arrangements will be documented so that critical systems can still be accessed if the Senior ICT Technician is unavailable. A dedicated administrative account will be available to the SLT for use only in an emergency where the Senior ICT Technician is unavailable.

TCAT and our schools will ensure that passwords are managed securely. The Senior ICT Technician will:

- Enforce password strength at system level
- Use measures such as deny lists or technical controls to prevent use of common or easily guessed passwords
- Ensure passwords are protected by restricting repeated failed login attempts
- Require passwords to be changed immediately where compromise is suspected or confirmed
- Ensure default passwords on devices, systems and services are changed promptly

TCAT will not rely on routine password changes unless there is a specific security reason to do so. Password resets will instead be driven by risk, compromise, technical need or account management processes.

Where younger pupils, pupils with SEND, or users with accessibility needs require alternative login arrangements, TCAT and our schools will implement proportionate solutions that support security while enabling access.

TCAT will ensure that MFA is enabled for all staff accounts with access to cloud services or remote access to on-site systems, and for all ICT administrative accounts. Enhanced security, such as MFA, will always be used where staff handle confidential, personal or sensitive personal data.

Where MFA is not available, a more complex password will be used in line with TCAT's password security requirements.

TCAT will ensure that remote access is only enabled where required and is restricted to authorised users. Remote access arrangements will be secured appropriately and reviewed regularly.

TCAT will review user accounts and access privileges at least termly to identify:

- Accounts that are no longer required
- Inappropriate access levels
- Missed joiner, mover or leaver changes
- Privileged access that is no longer justified

TCAT will keep arrangements for password security, authentication and access control under regular review to ensure that they remain effective and proportionate to risk.

8. Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. TCAT and our schools will inform all pupils and staff that their usage will be monitored, as well as how it is being monitored and why, in accordance with TCAT's Online Safety Policy.

The Senior ICT Technician will determine and implement an appropriate level of logging for TCAT's network and systems to support the identification and investigation of cyber-security incidents, attacks and network issues.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the Senior ICT Technician. Alerts will also be sent for unauthorised and accidental access. Alerts will identify the user, the activity that prompted the alert, and the information or service the user was attempting to access.

The Senior ICT Technician will record relevant alerts using an incident log and escalate cyber-security incidents in accordance with TCAT's reporting procedures. The CFO, acting for the DPO, will be informed where an incident involves, or may involve, a personal data breach. All incidents will be responded to in accordance with the Cyber-security incidents section of this policy, and as outlined in TCAT's Online Safety Policy.

The Senior ICT Technician will ensure appropriate filtering is in place to prevent access to inappropriate and potentially malicious websites and resources. Any member of staff or pupil that accesses inappropriate or malicious content will be recorded in accordance with the monitoring process in the cyber-security incidents section of this policy.

All data gathered by monitoring usage will be kept on a secure drive for easy access when required. This data may be used as a method of evidence for supporting a not-yet-discovered breach of network security. In addition, the data may be used to ensure TCAT, and our schools are protected and all software is up to date.

9. Removable media controls

TCAT and our schools understand that pupils and staff may need to access the school network from outside the school premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The Senior ICT Technician will encrypt all TCAT-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Before distributing any TCAT-owned devices, The Senior ICT Technician will ensure that manufacturers' default passwords have been changed. A set password will be chosen, and the staff member will be prompted to change the password once using the device. The Senior ICT Technician will check TCAT-owned devices on a regular basis to detect any unchanged default passwords.

When using laptops, tablets and other portable devices, the Senior ICT Technician will determine the limitations for access to the network, as described in the 'Network security' section of this policy.

Staff who use TCAT-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off TCAT premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any TCAT-owned laptops, tablets or other devices, or when accessing TCAT networks.

The Senior ICT Technician will ensure that appropriate filtering and security controls are maintained on TCAT-owned devices, including when they are used outside TCAT premises.

TCAT will use tracking technology on TCAT-owned devices where possible to support retrieval if they are lost or stolen. Users will be made aware that this means the location of the device may be tracked.

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The use of USB storage devices will be prohibited by default unless there is a specific need for their use, e.g. where required by an examination board. Where USB storage devices are permitted, anti-malware software will scan the device before its contents are made available to staff or pupils.

TCAT Wi-Fi networks will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless agreed prior to usage. A separate Wi-Fi network will be established for visitors at each TCAT school to limit their access to school networks and any other applications which it is not necessary for them to access.

10. Home working and remote learning

Staff and pupils will adhere to data protection legislation and TCAT's related policies when working remotely.

Staff will receive annual training regarding what to do if a data protection issue arises from any home working or remote learning.

Wherever possible, personal data will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach.

Staff and pupils may be required to use their own devices for the duration of the remote working or learning period. Where appropriate, TCAT will consider the use of a VPN to encrypt data sent and received by devices used outside TCAT premises. Using a shared personal or household device for school purposes should be avoided where possible; however, TCAT understands that this may not always be possible.

Staff and pupils are not permitted to let their family members or friends use any TCAT equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be disciplined in line with TCAT's Disciplinary Policy and Procedure. This may also result in a data breach that TCAT would need to record and potentially report to the Information Commissioner's Office (ICO).

Staff who require access to personal data to enable them to work from home will first seek approval from their Executive Headteacher, Headteacher or Head of School, and it will be ensured that the appropriate security measures are in place by The Senior ICT Technician and the CFO acting for the DPO, e.g. including appropriate authentication and anti-malware controls. MFA will be used for staff accounts with remote access to on-site systems.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked. TCAT devices will automatically lock within two minutes of inactivity as a maximum to avoid an unauthorised person gaining access to the device. Where staff are using a personal device, they will be advised that a similar function should be implemented.

Personal data will only be transferred to a personal device where necessary, authorised by TCAT and subject to appropriate security measures. When sending confidential information, staff must never save confidential information to a personal or household device. Data that is transferred from a work to a home device will be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives
- Sending work emails to and from personal email addresses
- Leaving logged-in devices and files unattended
- Using shared home devices where other household members can access personal data
- Using an unsecured Wi-Fi network

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off TCAT premises to allow staff to work from home, it will be transported in a lockable bag or container. TCAT's procedures for taking data off the school premises will apply to both paper-based and electronic data.

Staff will be expected to exercise particular vigilance when using TCAT ICT equipment outside the workplace. Appropriate precautions will be taken, as required from time to time, to prevent the importation of viruses or the compromise of system security.

The system may contain information that is confidential and/or subject to data protection legislation. Such information will be managed with the utmost care and in strict accordance with TCAT's Data Protection Policy.

All staff working remotely will be required to comply fully with this policy and the Data Protection Policy at all times.

Staff should avoid taking physical copies of data, e.g. paper documents, off TCAT premises unless absolutely necessary, such as when a digital version of the data does not exist. When taking physical copies of data off TCAT premises, staff will sign out the documents at their school office. The physical data will be signed back in when staff return it.

Pupils will not be permitted to use TCAT-owned devices or software for activities that do not pertain to their online education, e.g. use of social media, gaming, streaming or viewing content that is not applicable to their curriculum. Pupils will also not be permitted to download any software onto TCAT devices, unless instructed to and approved by their teacher.

Pupils will not alter the passwords or encryptions protecting school documents and systems put in place by TCAT and/or their school. Pupils will not alter or disable any security measures that are installed on TCAT devices, e.g. firewalls, malware prevention or anti-virus software. Pupils will not share any confidential and/or personal information made accessible to them, e.g. VPN passwords, with anyone who is not authorised to view that information.

Pupils that do not use TCAT devices or software in accordance with this policy will be disciplined in line with their school's Behaviour Policy.

Pupils must report any technical issues to their teacher as soon as possible. Parents and pupils will be encouraged to contact their DSL if they wish to report any concerns regarding online safety.

Any devices that are used by staff and pupils for remote working and learning will be assessed by the Senior ICT Technician prior to being taken to the home setting, using the following checks:

- System security check – the security of the network and information systems
- Data security check – the security of the data held within the systems
- Online security check – the security of any online service or system, e.g. the school website
- Device security check – the security of the personal device, including any 'bring your own device' systems

The Senior ICT Technician will provide staff and pupils with details and instructions for accessing their school network that they will be using throughout the duration of the remote working and learning period.

In the event that a staff member or pupil decides to leave a TCAT school permanently, all data in any form will be returned on or before their last day. The Senior ICT Technician will then ensure that the said staff member or pupil no longer has access to any TCAT network.

11. Backing up data

TCAT and our school's will maintain a documented backup and recovery approach to ensure that important systems and data can be restored in the event of accidental loss, corruption, system failure, cyber incident or attack.

TCAT will ensure that its backup arrangements support business continuity, disaster recovery and safeguarding requirements.

SLT Digital Leads will oversee their school's backup strategy and Cyber Crash File and will work with the Senior ICT Technician, the CFO acting for the DPO, their DSL, and relevant business staff to identify which systems and data are most critical to the continued operation of the school.

Each school will identify:

- What data and systems need to be backed up
- Which systems and records are critical to safeguarding, teaching, finance, operations and statutory duties
- How quickly systems and data need to be restored following an incident
- How current restored data needs to be in order to support school operations
- How long different categories of backed-up data should be retained in line with statutory requirements and retention schedules

The Senior ICT Technician will ensure that TCAT and our schools maintain at least three copies of important data, on at least two separate devices or platforms, with at least one copy held off-site.

The Senior ICT Technician will ensure that at least one backup is immutable so that it cannot be altered once created. This will help reduce the risk of ransomware, malicious interference or accidental corruption affecting backup integrity.

The Senior ICT Technician will ensure that backups are protected appropriately. This will include:

- Restricting access to backups to authorised personnel only
- Securing backup systems and storage locations
- Encrypting backup data where appropriate
- Ensuring that physical backup media is stored securely
- Ensuring that physical backups are never taken to a private home

The Senior ICT Technician will maintain records of backup arrangements, including what is backed up, where it is stored, how often backups run, how long data is retained, and when restoration testing has been completed.

TCAT will assess backup and restoration arrangements at least termly, and more frequently where there is a significant service or systems change. Testing will confirm that data can be recovered successfully and within an appropriate timeframe.

The Senior ICT Technician will keep a record of restoration tests and any issues identified. Where weaknesses are found, TCAT will take remedial action promptly.

TCAT will review its backup strategy annually, and sooner if there is:

- A major change to systems, services or infrastructure
- A significant cyber incident or attack
- A change to legal, safeguarding or operational requirements

TCAT will ensure, wherever possible, that backed-up data can be restored to a wide range of supported devices and systems and is not dependent on a single item of hardware.

TCAT will also ensure that unnecessary data is deleted or archived in line with retention requirements so that backup sets remain manageable and recovery processes remain effective.

Where cloud services are used, TCAT will ensure that backup arrangements are understood clearly and do not rely solely on supplier defaults where these are insufficient to meet the school's operational, safeguarding or compliance needs.

12. Avoiding phishing attacks

The Senior ICT Technician will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with only the access rights necessary to perform their roles.

Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account. Multi-factor authentication will be used in accordance with the requirements set out in the 'User privileges and passwords' section of this policy.

Staff will use the following warning signs when considering whether a communication may be unusual:

- Is it from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is it addressed to a 'valued customer,' 'friend' or 'colleague'?
- Does it contain a veiled threat that asks the staff member to act urgently?
- Is it from a senior member of the school asking for a payment?
- Is it from a supplier advising of a change in bank account details for payment?
- Does it sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free
- Is it from a generic email address, such as Gmail or Hotmail?

The Senior ICT Technician will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' section of this policy. ICT support will ensure that the filtering system is neither too strict nor too lenient, to allow the correct emails to be sent to the relevant folders.

SLT Digital Leads will coordinate training for staff and pupils on phishing attacks as part of TCAT's wider cyber-security training and awareness activities. Staff and pupils will be encouraged to report any suspicious emails they suspect as phishing to the Senior ICT Technician and/or other relevant contacts within TCAT and their school.

The Senior ICT Technician will also conduct phishing simulations throughout the year and record the statistics relating to those who reported the phishing and those who clicked the links. These statistics will be reported to the CEO and CFO.

13. Social media and website data

To prevent anyone having access to unnecessary personal information, the CFO acting for the DPO will ensure TCAT and our schools social media accounts and websites are reviewed on a regular basis, making sure that only necessary information is shared. The CEO and CFO acting for the DPO will ensure TCAT's Social Media Policy includes expectations for sharing of information and determines what is and is not appropriate to share.

Executive Headteachers, Headteachers and Heads of School will ensure parents, pupils, staff and other members of the school community are aware of acceptable use of social media and the information they share about TCAT, the school and themselves.

14. User training and awareness

TCAT and our schools will recognise that well-informed users are a critical line of defence against cyber security threats. As many cyber incidents exploit common behaviours and everyday use of technology, TCAT will prioritise raising awareness and delivering effective cyber security training to pupils, staff and relevant stakeholders.

TCAT will implement a comprehensive training and awareness programme to:

- Reduce the risk of cyber incidents and attacks
- Safeguard pupils and staff, particularly where personal data is involved

- Foster a culture in which pupils and staff feel confident identifying and reporting risks
- Promote a clear understanding of acceptable use of digital technology and reinforce expected behaviours
- Ensure that cyber incidents, risks and breaches are identified and reported promptly to minimise impact

TCAT will acknowledge that a lack of awareness and understanding of cyber risks may lead to safeguarding concerns, data breaches, and disruptive or costly cyber incidents. To mitigate these risks, TCAT will establish strong foundations through appropriate policy and structured training provision.

Acceptable Use

TCAT schools will develop, implement and regularly review acceptable use agreements that clearly defines appropriate and inappropriate use of digital systems and data.

Each school will ensure that:

- All users with access to their school network or data, including guests and supply teachers using the school's network or Wi-Fi, are made aware of and agree to the relevant acceptable use agreement
- Acceptable use agreements are reviewed regularly to reflect emerging risks and organisational needs specific to the school
- Pupil agreements or contracts incorporate relevant elements of the acceptable use agreement and are issued at the start of each academic year

Training and Pupil Awareness Provision

TCAT and our schools will deliver regular and up-to-date cyber security training and age-appropriate pupil awareness activities. Training will be provided at least annually, and more frequently where specific risks are identified.

Where provided by an individual school, the school will ensure that training is coordinated by their SLT Digital Lead in collaboration with the Senior ICT Technician, the CFO acting for the DPO and the DSL, and will be provided to all pupils and staff, at least one Local Governor, and any additional users with system access.

Training will be age-appropriate and tailored to the school's risk profile. It will include, but not be limited to:

- Recognising and responding to phishing and other social engineering attacks
- Maintaining strong password security
- Understanding online safety risks
- Avoiding unsafe or inappropriate websites that may contain malware
- Ensuring the physical security of devices
- Understanding the risks associated with removable media such as USB devices
- Using MFA
- Recognising and reporting cyber incidents and data breaches
- Understanding data protection responsibilities, with enhanced training for higher-risk roles

TCAT will ensure that all staff users complete National Cyber Security Centre (NCSC) training annually and will retain evidence of completion.

15. Cyber-security incidents

All cyber-security incidents will be managed in line with the school's Cyber Response and Recovery Plan and the Cyber Crash File.

TCAT schools will ensure that all cyber incidents, attacks, suspected compromises and near misses are reported promptly, recorded appropriately and managed effectively.

TCAT will recognise that educational institutions, including schools, continue to be targeted by cybercriminals, and will implement appropriate measures to mitigate associated risks.

All staff and pupils will be responsible for reporting any suspected cyber risk, incident or attack immediately to the Senior ICT Technician, the CEO and the CFO. This will include, but is not limited to, phishing attempts, suspicious emails, malware alerts, unauthorised access, unusual system behaviour, or lost or stolen devices.

Any individual that discovers a cyber-security incident will report this immediately to the Senior ICT Technician and the CFO. The DPO will be informed where personal data concerns may be involved and the DSL when safeguarding concerns may be involved.

On identification of a cyber incident, the school or where the incident is across the Trust, TCAT will activate their Cyber Response and Recovery Plan and Cyber Crash File and take immediate steps to contain the risk and protect systems and data.

When an incident is raised, the Senior ICT Technician or CFO will ensure that the following information is recorded:

- Name of the individual who has raised the incident
- Description and date of the incident
- Description of any perceived impact upon and level of risk to individuals including the type of data involved in the incident
- Description and identification codes of any devices involved e.g. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident
- Whether the incident needs to be reported to the relevant authorities, e.g. the ICO or police

The SLT Digital Lead will coordinate their school's response to, and investigation of the incident, with assistance from the Senior ICT Technician and the school cyber recovery team and will ensure that appropriate time and resources are allocated. The CFO will advise on and support the investigation where personal or sensitive personal data is involved.

If the incident is assessed as low severity, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access
- Where a pupil or member of staff is responsible for a breach, the Executive Headteacher, Headteacher or Head of School will consider whether disciplinary action is appropriate in accordance with the school Behaviour Policy or TCAT's Disciplinary Policy and Procedure
- TCAT will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes
- TCAT and our schools will organise updated staff training following a breach
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups

If the incident is assessed as high severity, the incident will be managed in accordance with the following procedures further to the above procedures (where applicable):

- SLT Digital Leads will work with the internal and external breach response team including the Senior ICT Technician, the Executive Headteacher, Headteacher or Head of School, the CEO and CFO and other relevant staff to immediately investigate the breach, its source, the method of attack and which systems and data have been affected
- Compromised or suspected compromised systems will be isolated from the network and taken offline
- A record will be kept of any personal data breaches along with whether the ICO and individuals were notified along with the reasons for this
- Retrieving any lost, stolen or otherwise unaccounted for data
- Restricting access to systems entirely or to a small group
- Backing up all existing data and storing it in a safe location
- Reviewing basic security, including:
    - Changing passwords and login details on electronic equipment
    - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation
- TCAT will cooperate in a timely manner with the relevant regulators and law enforcement bodies to investigate the breach
- Communications with staff, pupils, parents and any other interested parties will be carried out only in accordance with the strategy agreed with breach response team
- Immediate steps will be taken to remediate the breach by securing and restoring affected systems and ensuring the necessary security measures are taken
- All lost personal data should be recovered as soon as possible from backups
- The relevant internal stakeholders will be informed and updated of the breach

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach.

TCAT will be required to report any personal data breaches to the ICO where there is a likelihood of risk to individuals' rights and freedoms. Where the CFO in consultation with the DPO determines that such a risk is unlikely, the breach will not be reported; however, TCAT will document the breach in full and justify the decision not to report.

The CFO acting for the DPO will notify the ICO within 72 hours of becoming aware of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours. The information required can be provided in phases, as long as this is done without undue further delay.

In line with the UK GDPR, the following will be provided to the ICO when reporting a personal data breach:

- A description of the nature of the breach, including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, to deal with the breach
- A description of the measures taken to mitigate any possible adverse effects, where appropriate

TCAT will report a personal data breach via the ICO website. TCAT will also make use of the ICO's self-assessment tool to determine whether reporting a breach is a necessary next step.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the CFO acting for the DPO will notify those concerned directly of the breach without undue delay.

Where appropriate, TCAT will report cyber incidents or attacks to relevant external bodies.

This will include:

- Report Fraud, where the school has experienced a cyber-attack, cyber-crime, fraud or ransomware incident
- The DfE sector cyber team, where an incident or attack causes significant disruption, affects multiple schools, or results in significant financial loss
- TCAT's cyber insurance provider or risk protection arrangement (RPA), where applicable

TCAT will ensure that external reporting is conducted promptly and in line with national guidance and any legal or contractual obligations.

SLT Digital Leads will review records of previous cyber incidents and attacks to identify common themes, vulnerabilities and areas for improvement. Relevant findings will be used to inform TCAT and our schools cyber-security risk assessment and future security measures.

TCAT and our schools will ensure that all staff and pupils understand how to report cyber incidents and feel confident and supported in doing so. Clear reporting routes will be communicated through training and awareness activities.

The Senior ICT Technician will assess affected systems to ensure they are functioning normally and are safe to use before the incident is deemed resolved.

16. Assessment of risks

TCAT and our schools will ensure that staff, and where appropriate pupils, understand the risks associated with their hardware, software and data to properly mitigate and defend against any potential cyber incidents or attacks.

Cyber risks will be assessed to:

- Understand how to keep pupils, staff and the wider school community safe
- Understand how prepared TCAT and our schools are in response to a cyber incident or attack
- Highlight weaknesses and put processes in place to help reduce risk
- Secure systems to make sure they are more resilient to cyber incidents and attacks
- Assist in the preparation of a cyber response plan that can be implemented quickly in the event of a serious incident to minimise any impact

SLT Digital Leads will be responsible for coordinating activity in relation to conducting a Cyber-security Risk Assessment and the Cyber Crash File for their school.

SLT Digital Leads will work with:

- The Senior ICT Technician to review the outcomes of discussions with key staff and action them within the risk assessment
- ICT leads in the broader organisation to find out if anything needs to be actioned or approved by them
- The CFO and DPO, who will provide advice on any risks around data processes to ensure personal and sensitive personal data is secure

- The Trust Estate Manager to identify any physical security risks that could create problems for core systems and data, e.g. a door that will not lock on a server room
- Their executive Headteacher, Headteacher or Head of School, who will make decisions on action suggested by the SLT Digital Lead and the Senior ICT Technician
- The CFO, who will help budget and plan for any changes needed, update the risk register, and buy in any additional services needed
- Their Local Governing Body for oversight and strategic risk management

In working with additional external providers, TCAT will discuss with the provider how it meets the requirements of the DfE's Cyber Security Core Standard, including how it will mitigate the risk of a cyber incident or attack on its own network affecting TCAT's networks. TCAT may also consider whether the provider is certified with Cyber Essentials or Cyber Essentials Plus.

The CFO and the Senior ICT Technician will regularly review digital technology assets and any related cyber security risk, and check that all digital technology is licensed, supported and updated.

The Senior ICT Technician will work with the CFO to:

- Complete a record of processing activities for all new and current systems storing or processing personal and sensitive data
- Assess staff access and permissions to systems and data and check password policies
- Check that email systems are set up to be secure and reduce the risk of third parties being able to send imitation emails

The Senior ICT Technician will work with the CFO to collect information from other relevant staff members to:

- Understand what the greatest cyber risks are and establish the likelihood of these happening, and the potential impact
- Capture how many cyber incidents or attacks have already occurred and what they are in order to understand common themes and where to improve
- Identify any pupil or staff behaviour that may pose a risk and could expose TCAT or a TCAT school to a cyber incident or attack

The Senior ICT Technician will work with the CFO to:

- Create a simple reporting structure for cyber risks to be captured, escalated and actioned, ensuring that cyber risks are recorded in the TCAT's risk register and incorporated into a regularly tested business continuity plan
- Maintain documentation and the business continuity plan at one or more locations
- Flag any risks or issues identified to governors as part of the risk management process
- Put a cyber response plan in place

TCAT will ensure that appropriate insurance is in place to minimise costs in the event of a cyber incident or attack.

Risk assessments will be completed as soon as possible and repeated annually or in the event of significant technology or process changes, or an incident or attack.

Risk assessments will be revisited every term by relevant staff members to highlight vulnerabilities and actions that may be needed to minimise them.

Where a cyber-security incident or attack involves, or may involve, personal data, the CFO acting for the DPO will consider the following questions to assess the risks to individuals and determine the appropriate next steps. All relevant questions will be clearly and fully answered in the report, which should record:

- What type of, and how much, data is involved?
- How sensitive is the data? Sensitive data is defined in the UK GDPR; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details)
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
- Have individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could the data be used to commit identity fraud?
- Could harm come to individuals? This could include risks to the following:

    - Physical safety
    - Emotional wellbeing
    - Reputation
    - Finances
    - Identity
    - Private affairs becoming public
- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence and/or damage to TCAT or the school's reputation, or risk to TCAT's operations?
- Who could help or advise TCAT on the breach? Could the LA, external partners, authorities, or others provide effective support?
- Does the breach need to be reported to the ICO? If so, has it been successfully reported without undue delay?

In the event that the CFO acting for the DPO, or other persons involved in assessing the risks to the school, are not confident in the assessment of risk, they will seek advice from the ICO.

17. Consideration of further notification

The CFO acting for the DPO will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in data security.

The CFO will assess whether notification could help the individual(s) affected, and whether the individual(s) could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password. In line with the 'Cyber-security incidents' section of this policy, where a personal data breach is likely to result in a risk to individuals' rights and freedoms, the ICO will be informed without undue delay and, where feasible, within 72 hours of the school becoming aware of the breach.

The CFO acting for the DPO will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved
- Details of what has already been done to respond to the risks posed by the breach
- Specific and clear advice on the steps they can take to protect themselves, and what TCAT is willing to do to help them

- A way in which they can contact TCAT for further information or to ask questions about what has occurred

The CFO acting for the DPO will consider, as necessary, the need to notify any third parties, such as the police, insurers, professional bodies, funders, trade unions, website and/or system owners, banks and/or credit card companies, who can assist in helping or mitigating the impact on individuals.

Monitoring and review

Lifespan of Policy: 3 Years

At any point this policy is updated or fully reviewed, it will be updated on the main TCAT website and will automatically update on all TCAT school websites simultaneously.

Where an annual check or other check results in minor changes, the Version History will be reviewed and updated with a change in the number following the decimal point, for example, v1.1 ⇨ v1.2. Where the policy is reviewed in full, then the number before the decimal point will change and reset, for example v1.4 ⇨ v2.0.

Any changes made by the CEO in collaboration with the Board Appointed Trustee will be passed to the Trust Board for ratification and subsequently be notified to Clerks to Local Governing Bodies and Headteachers/Heads of School.

The next scheduled full review date for this policy is 5th November 2029.

Date approved by the Board Appointed Trustee: 6th November 2026.

To be ratified and recorded in the minutes at the first Trust Board Meeting after 6th November 2026.

Trust Glossary

AA	Admissions Authority	**H&S**	Health and Safety
AAI	Adrenaline Auto-Injector (Epi Pen)	**HoS**	Head of School
ACM	Asbestos Containing Materials	**HSE**	Health and Safety Executive
AHT	Assistant Headteacher	**ICO**	Information Commissioners Office
AIR	Attendance Intervention Reviews	**IDSR**	Inspection Data Summary Report
APDR	Assess Plan Do Review Cycle	**IHP**	Individual Healthcare Plan
APIs	Application Programming Interfaces	**IRMS**	Information and Records Management Society
ASC	Autistic Spectrum Condition	**IWF**	Internet Watch Foundation
ASP	Analyse School Performance	**KCSIE**	Keeping Children Safe in Education
ATH	Academy Trust Handbook	**KS1/2/3/4**	Key Stage 1/2/3/4
BAME	Black, Asian and Minority Ethnic Backgrounds	**LAC**	Looked After Child
BAT	Board Appointed Trustee	**LADO**	Local Authority Designated Officer
BCP	Business Continuity Plan	**LGB**	Local Governing Body
BFR	Budget Forecast Return	**LLC**	Low-Level Concerns
CEO	Chief Executive Officer	**LSA**	Learning Support Assistants
CFO	Chief Financial Officer	**MASH**	Multi-Agency Safeguarding Hub
CIF	Condition Improvement Fund	**MAT**	Multi-Academy Trust

CIN	Child in Need	**MFA**	Multi-Factor Authentication
CLA	Children Looked After	**MFL**	Modern Foreign Language
CMIE	Child Missing in Education	**NCSC**	National Cyber Security Centre
COO	Chief Operating Officer	**NoV**	Note of Visit
COSHH	Control of Substances Hazardous to Health	**NPQ**	National Professional Qualifications
CP	Child Protection	**PA**	Persistent Absence
CPD	Continuing Professional Development	**PAN**	Published Admission Number
CPOMS	Child Protection Online Management System	**PECR**	Privacy and Electronic Communications Regulations
CSCS	Children's Social Care Services	**PEP**	Personal Education Plan
CSE	Child Sexual Exploitation	**PEEP**	Personal Emergency Evacuation Plan
CTIRU	Counter-Terrorism Internet Referral Unit	**PEx**	Permanent Exclusion
CWD	Children with Disabilities	**PP**	Pupil Premium
CYPMHS	Children and Young People's Mental Health Services	**PPG**	Pupil Premium Grant
DBS	Disclosure and Barring Service	**PSHE**	Personal, Social and Health Education
DDSL	Deputy Designated Safeguarding Lead	**PSED**	Public Sector Equality Duty
DfE	Department for Education	**PTFA**	Parent, Teacher and Friends Association
DHT	Deputy Headteacher	**QA**	Quality Assurance

DSE	Display Screen Equipment	**RIDDOR**	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
DSL	Designated Safeguarding Lead	**RHE**	Relationships and Health Education
DPO	Data Protection Officer	**RPA**	Risk Protection Arrangement
EAL	English as an Additional Language	**RSHE**	Relationships, Sex and Health Education
ECT	Early Career Teacher	**SA**	Severely Absent
EDIB	Equality, Diversity, Inclusion and Belonging	**SALT**	Speech and Language Therapist
EHA	Early Help Assessment	**SARC**	Sexual Assault Referral Centre
EHCNA	Education, Health and Care Needs Assessment	**SBM**	School Business Manager
EHCP	Education, Health and Care Plan	**SCC**	Standard Contractual Clause
EHE	Elective Home Education	**SCITT**	School-Centred Initial Teacher Training
ELSA	Emotional Literacy Support Assistant	**SCR**	Single Central Record
ESFA	Education and Skills Funding Agency	**SDP**	School Development Plan
EVC	Educational Visit Coordinator	**SDQ**	Strengths and Difficulties Questionnaire
EWOSSO	Education Welfare and Safeguarding Support Officer	**SEF**	Self-Evaluation Form
EYFS	Early Years Foundation Stage	**SEMH**	Social, Emotional, and Mental Health
FBV	Fundamental British Values	**SENCO**	Special Educational Needs Coordinator
FFT	Fischer Family Trust	**SEND**	Special Educational Needs and Disabilities

FGM	Female Genital Mutilation	**SIP**	School Improvement Partner
FGMPO	FGM Protection Order	**SLA**	Service Level Agreement
FOI	Freedom of Information	**SLCN**	Speech, Language and Communication Needs
FSM	Free School Meals	**SLT**	Senior Leadership Team
FTS	Find a Tender Service	**SPOC**	Single Point of Contact
GAG	General Annual Grant	**STEM**	Science, Technology, Engineering and Maths
GDPR	General Data Protection Regulation	**TA**	Teaching Assistant
GIAS	Get Information about Schools	**TAC**	Team Around the Child
HASH	Herefordshire Association of Secondary Heads	**TCAT**	Three Counties Academy Trust
HBA	Honour Based Abuse	**TUPE**	Transfer of Undertakings (Protection of Employment)
HR	Human Resources	**VSH**	Virtual School Headteacher