APPROVED BY: Trust Board

LAST REVIEWED: November 2023 by A&R Committee

Date: December 2023

NEXT REVIEW DATE DUE BY: December 2024

CYBER AND INFORMATION SECURITY POLICY

Purpose

This policy defines how St Thomas Catholic Academies Trust (STCAT) manages access to and protection of information assets and our approach to cybersecurity threats. It includes the following principles and controls:

- How STCAT manages access to information assets.
- How STCAT protects its information assets from malware.
- How STCAT manages firewalling technology and mechanisms for IT systems used by its staff.
- How STCAT ensures it has information security practices necessary to ensure adequate controls and appropriate processes are applied to safeguard the school's information assets.
- How STCAT manages the secure and responsible disposal of IT assets.
- How STCAT manages authentication mechanisms for information technology systems used by its staff and subcontractors.
- How STCAT prepares to defend against the threat of ransomware attacks on the school's computer systems.
- How STCAT ensures consistent secure configuration across all hardware and software applications.

The Policy is available to, and is mandatory to be read by all employees, agency and service providers, including guest users with access to St Thomas Catholic Academies Trust's information technology systems, including any central and school systems, on premise or cloud based.

Responsibilities

All users, inclusive of employees, subcontractors and suppliers with direct access to St Thomas Catholic Academies Trust's information technology systems are expected to comply with this policy.

St Thomas Catholic Academies Trust's IT Support Team is responsible for providing support to St Thomas Catholic Academies Trust in complying with this policy.

The Board of Directors are ultimately responsible for organisational compliance to this policy, and are responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated. They delegate day to day responsibility for organisational compliance to the Chief Operations Officer, who provides guidance to the Board in their role.

All users, inclusive of suppliers with direct access to St Thomas Catholic Academies Trust's information technology systems will take all reasonable care to prevent their access to the system being hijacked by an unauthorised person. This includes ensuring that computers are locked or logged off when left unattended and conforming with the Password Management Section of this Policy.

Information Security

Definitions

Availability	Readiness to access information resources when needed.
Confidentiality	Access controls to information assets to ensure that only authorised users with the right access privileges have access to the appropriate resources.
Information Asset	Any valuable resources or components in the interest of the school's strategic requirements.
Integrity	Information preservation to prevent any unauthorised modifications ensuring correctness and completeness.

Information Security Principles

To assure that systems are secure, three key information security principles must be guaranteed, namely confidentiality, integrity and availability. A violation of any of these principles compromises the security of a computer system and such may lead to severe unintended consequences. These principles aim to:

- make provision for the availability of information where there is a legitimate reason to do.
- ensure the integrity of information is always maintained.
- guide technical and non-technical controls and measures that ensure information is protected from unauthorised access using authentication and authorisation methods.

Information Governance

St Thomas Catholic Academies Trust's Chief Operations Officer is responsible for the oversight in the production, maintenance and distribution of cybersecurity policies. This policy will undergo regular reviews and all significant changes are approved by the board to ensure internal consistency.

School Administration/Board responsibilities

- Ensuring that any changes made to this policy and any related policies are effectively communicated to all users.
- Ensuring staff understand and adhere to this policy and any related sub-policies.
- Reporting all instances of non-compliance.

Other users

Any person who uses, has access to or interacts with the school's information systems in any way possible should be responsible for:

- Conforming to the acceptable use of the school's information assets.
- Adhering to this information security policy and all related sub-polices.
- Reporting all suspected cyber security incidents through the approved procedure as stipulated in the school's cyber security incident management plan.

Incident Management and Response

St Thomas Catholic Academies Trust's cyber security incident management and response plan provides guidance on what the school regards to be a cybersecurity incident, including methods of reporting. All suspected information security breaches need to be reported and investigated. All significant security recommendations must be incorporated into the risk action plan. In the case of a significant disruption to the school's information systems, the business continuity plan should be invoked to ensure a systematic, swift and effective recovery process in the best interest of the school.

Acceptable System Use

The use of the school's information assets and systems by authorised users must be in a lawful and safe manner. St Thomas Catholic Academies Trust's information assets shall only be used for supporting learning activities, administration tasks and any other task that is directly or indirectly related to the school's interest. Any use of the school's information resources for personal gain or any other business requires the approval of St Thomas Catholic Academies Trust's the Chief Operations Officer.

Information Classification

St Thomas Catholic Academies Trust understands that not all information is equal, and thus the need for a sensitivity classification. This is important so as to adequately protect information based on value.

System Change Management

Changes to St Thomas Catholic Academies Trust's functional requirements that may call for modifications to existing information systems might affect the information security controls and processes and thus risk management controls may need to be implemented accordingly. Appropriate security provisions need to be considered before any significant changes are made to the school's network.

Breach of Policy

Any form of violation towards this policy may call for disciplinary measures under St Thomas Catholic Academies Trust's disciplinary procedure.

Access Control

St Thomas Catholic Academies Trust follows the following principles when designing, configuring, administering, and using information systems.

'Least Privilege'
When determining who requires access to information and what they can do with it, St Thomas Catholic Academies Trust will only grant the privileges required to effectively carry out their job role.

‘Need to Know’
When determining who requires access to sensitive information, St Thomas Catholic Academies Trust will consider who needs access to the data; not who might at some point need access to the data, granting individuals access to highly sensitive documents, rather than groups.

‘Access by Job Function or Department’
St Thomas Catholic Academies Trust provides access to non-sensitive data by job function or department. This is to simplify the privileges structure and to limit the impact in the event of compromise.

‘Unique Digital Identities’
Where possible, St Thomas Catholic Academies Trust always issue unique digital identities to employees and service providers with access to its information technology systems. On most occasions, this is a unique username and password.

‘Regular Review of Access’
St Thomas Catholic Academies Trust will conduct an ‘Accounts and Privileges Review’ every 12 months.

Configuration and Administration

Accounts used to administrate St Thomas Catholic Academies Trust’s information technology systems are, where possible, only used for administration purposes. Administrative accounts on operating systems and productivity services will not be used for daily operations.

Provisioning, Decommissioning, Promotion and Deletion

User accounts are provisioned, decommissioned, promoted and demoted by means of submitting a request to the Trust’s ICT Support Team

Special Privileges

St Thomas Catholic Academies Trust maintains a register of all users with special privileges to information systems. Special Privileges are digital identities with a level of access higher than any standard account. This register is known as the Special Privilege Register and is reviewed during the ‘Accounts and Privileges Review’ every 6 months. Maintaining the Special Privilege Register allows St Thomas Catholic Academies Trust to provide additional controls to higher risk digital identities.

Anti-Malware

Software Approval

St Thomas Catholic Academies Trust prohibits any form of software that hasn’t been approved and formally documented on its Approved Software Register.

Anti-Malware Software

All information technology assets of St Thomas Catholic Academies Trust must have the organisation's designated anti-malware software installed where the software is compatible. Other anti-malware software may be approved by the Chief Operations Officer if required, for example schools joining and requiring a transitional coverage from their existing system.

Designated Anti-Malware Software

St Thomas Catholic Academies Trust has chosen Sophos Central as its designated anti-malware software solution.

Anti-Malware Software Configuration

St Thomas Catholic Academies Trust's anti-malware software will be configured to perform:

- On-access scanning of files and web pages
- On-access scanning of removable media
- Scheduled full system scans on a daily basis
- Daily definition database updates

Home-based Staff and Bring-Your-Own-Device

St Thomas Catholic Academies Trust requires all personal devices used by staff to access its information assets to have at least the operating system's default anti-malware software to be enabled and preferably its designated anti-malware software installed.

Anti-Malware Review

St Thomas Catholic Academies Trust's ICT Support Team is responsible for monitoring the installation and updating status of the anti-malware provision across the organisation.

Firewall

Default Credentials

St Thomas Catholic Academies Trust always changes default credentials on network boundary firewalls. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.

Strong Passwords

St Thomas Catholic Academies Trust follows the principles outlined in the Password Management Section of this Policy when changing network boundary firewall passwords.

Network Boundary Firewalls

St Thomas Catholic Academies Trust requires that Network Boundary Firewalls have the following capabilities supported and enabled:

- HTTP and HTTPS proxy
- Gateway antivirus
- Multi-WAN with failover functionality (if multiple WANs are installed)
- Intrusion Prevention System
- Advanced Persistent Threat protection

Personal Firewalls (School Computers)

St Thomas Catholic Academies Trust requires that the Operating System or approved third party host-based firewall is enabled on all network connected endpoints that have such ability.

Personal Firewalls (Home-based and Bring-your-own-device Computers)

St Thomas Catholic Academies Trust requires that at least the built-in Windows or Mac OS host-based firewall is enabled on all network connected endpoints that have such ability.

Blocked Services

St Thomas Catholic Academies Trust does not allow services that are identified by the NCSC, GCHQ or the Cyber Essentials scheme as vulnerable to be allowed to connect through firewalls. Services that are identified as vulnerable are as follows:

- SMB
- TELNET
- NetBIOS
- TFTP
- RPC
- rLogin
- RSH
- rExec
- HTTP

Internet Access

Access to the internet from St Thomas Catholic Academies Trust Local Area Networks is granted only to devices that require access as an operational necessity. Restriction of access is implemented by a ‘Blanket Deny’.

Maintaining the Register

St Thomas Catholic Academies Trust maintains a register of all approved firewall rules permitted on Boundary Firewalls using the built-in access control list on the device, adding clear justification in the description of each rule. Rules are approved only by the Chief Operations Officer.

ICT Asset Disposal

Asset Identification

This policy seeks to address the disposal of all of St Thomas Catholic Academies Trust's information assets that have the capability to record or store data, including:

- PCs
- Laptops
- Servers
- Mobile Phones/Tablets
- Firewalls/Routers/Switches
- Printers/Scanners/Fax Machines
- USB Flash Drives/External Hard Drives

Data Backup and Media Sanitisation

St Thomas Catholic Academies Trust's IT assets should not be disposed of before ensuring that the required data backups and backup tests are done. All media with the capability to record or store data must be properly sanitised according to the sensitivity of the data.

Disposal Criteria

St Thomas Catholic Academies Trust's ICT Support Team should be notified if any IT equipment needs to be decommissioned. A decision should be made to either reuse/recycle or dispose. Before any equipment is disposed of, a risk-based approach should be taken based on the type of asset and the sensitivity of the data potentially stored.

- **Restricted** - Assets used for the processing and storage of restricted and/or personal data should be identified as high risk because data loss could potentially have significantly detrimental effects. Such assets should be properly sanitised using approved technology or physically destroyed.
- **Confidential** - Assets used for the processing and storage of confidential data should identified as high risk as data loss could also potentially have significantly detrimental effects. Such assets should be properly sanitised using approved technology or physically destroyed.
- **Internal** - Assets used for the processing and storage of internal data should be identified as medium risk. Such assets should be sanitised using approved technology.
- **Public** - Assets used for the processing and storage of public data should be identified as low risk. Such assets should be sanitised and could potentially be reused somewhere else.

Third Party Service Providers

Where incapacitated, an approved licensed third-party service provider is contracted to undertake the IT disposal process on behalf of St Thomas Catholic Academies Trust. This will continue to be monitored to ensure that St Thomas Catholic Academies Trust's IT disposal standards are met.

Environmental Responsibility

St Thomas Catholic Academies Trust is fully aware of the hazardous impact of incorrectly discarding electronic equipment. Reasonable care should be taken to thoroughly separate and isolate toxic chemicals and components from all electronic equipment before shipment to a landfill.

Password Management

Default Credentials

St Thomas Catholic Academies Trust always changes default credentials. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.

Strong Passwords

St Thomas Catholic Academies Trust follows the following principles when creating a new password.

- Are never obvious (easy for an attacker to guess)
- Are never commonly used passwords
- Have never been disclosed in a breach (validated using the HaveIBeenPwned service (haveibeenpwned.com)
- Are never re-used when a password expires
- Are never re-used across different accounts

Password Disclosure

St Thomas Catholic Academies Trust employees and contracted staff will never:

- Write down their passwords or encryption keys
- Disclose their password to others

St Thomas Catholic Academies Trust's ICT Support Team will never ask employees or contracted staff for their password.

Multi-Factor Authentication

All employees and contracted staff at St Thomas Catholic Academies Trust will ensure that multi-factor authentication is enabled for all devices and services that support this technology.

Training

All employees and contracted staff at St Thomas Catholic Academies Trust are encouraged to remain conversant with password advice from the UK's National Cyber Security Centre.

Patch Management

Workstations

St Thomas Catholic Academies Trust ensures that all its workstations are running an operating system that is actively supported by the vendor according to its development life cycle. Workstations running retired or legacy operating systems are removed from service. Automatic updates are enabled for all workstations' operating system, updating at least as often as the default frequency defined by the vendor.

Patching Schedule

St Thomas Catholic Academies Trust implements a Risk Based Approach to patching:

For devices where automatic patching is available we will enable those features and aim to update those devices within 14 days of release and aim to install patches not related to security within 90 days.

For devices where manual patching is required we aim to update them on the following schedule:

Server Devices: Within 30 days of release
Network Appliances (Switches and active equipment): Within 30 days of release
Client Endpoint Devices: Within 45 days of release

We aim to install patches not related to security within 90 days.

Problematic Patches

St Thomas Catholic Academies Trust's ICT Support Team will take all reasonable measures to ensure that updates known to be problematic are prevented from being installed until resolved by the vendor.

Software Licensing

St Thomas Catholic Academies Trust does not operate unlicensed software and takes all reasonable measures to ensure that it meets all End User Licence Agreement terms.

Legacy Software

St Thomas Catholic Academies Trust takes all reasonable measures to ensure that the software it uses is supported by its vendor. There may be occasions where no alternative software is available; in this case the software must be approved by the Chief Operations Officer and marked as unsupported in the St Thomas Catholic Academies Trust information asset register.

Monitoring and Internal Audit

St Thomas Catholic Academies Trust aims to conduct annual vulnerability scans to ensure compliance with this policy.

Ransomware

Definition

The National Cyber Security Centre's (NCSC) definition reads: *"Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted."*

Preparation

St Thomas Catholic Academies Trust recognises and acknowledges the threat of ransomware attacks and the severity of the impact on the Trust's computer systems and operations and aims to prepare accordingly. To prepare for and defend against ransomware attacks, the Trust deploys strategies and controls which may include the following:

- **Data classification** - Not all data is equal and thus data should be classified and stored according to the sensitivity level. The school should be aware of the systems that process and store critical/sensitive data and such must be documented.
- **Effective backup strategies** - Backup systems are the first port of call in the case of a ransomware attack. Ransomware attacks aim to sabotage recovery operations thus, the school aims to implement effective backup strategies and data recovery operations by:
    - conducting regular backups of data, and most importantly, of critical/sensitive data
    - having offline backups preferably offsite
    - having multiple copies of the same file using different backup systems
    - scanning backup systems for malware where possible, especially before recovery
    - regularly testing data recovery operations
- **Staff awareness training** - The school conducts regular staff awareness training to educate staff in areas which include but not limited to best security practices, common attack vectors, phishing email attacks, password handling, reporting channels.
- **Patch management** - St Thomas Catholic Academies Trust follows the patching schedule described in this Policy to reduce an attacker's probability of gaining access through a discovered security vulnerability.
- **Cyber insurance** - Cyber insurance will assist the Trust with recovery costs in the case the Trust suffers a breach.
- **Regular incident management plan rehearsal** - A timely and well-coordinated response to a ransomware attack might lessen the impact. St Thomas Catholic Academies Trust aims to review and test the incident management plan to ensure that it's up-to-date and that all the pre-defined roles and responsibilities are clearly defined. This will be rehearsed at least annually.

Monitoring and Detection Controls

Network monitoring strategies and suspicious behaviour detection controls are implemented across the Trust's computer systems and networks. This approach aims to implement technology best practices as well as non-technical approaches which may include:

- Ensuring anti-malware software applications are installed and enabled on all endpoints, virus signature databases are always up-to-date and files are set to be scanned on-access.

- Automated suspicious/unusual behaviour event notifications including the deploying a monitored 'honeypot' folder at the top of critical data directories that serves as an early-warning.
- Deploying robust email filtering systems to block, quarantine or flag suspicious emails.
- Reporting of suspicious emails or events by school staff.

Eradication and Recovery Process

In the case the Trust is breached, the main aim is to contain the malware to prevent it from spreading to
other systems. St Thomas Catholic Academies Trust follows the NCSC guidelines to help limit the impact:

- Quick disconnection and isolation of infected computers, laptops or tablets from all network connections. If multiple devices are infected, network equipment including routers, switches and wireless access points may also need to be turned off.
- User credentials for user accounts associated with the infected device will be reset
- The latest patches will be applied to non-infected devices
- Infected devices are wiped and rebuilt
- All backup systems must be thoroughly scanned for malware before data recovery operations are commenced.
- Verify that endpoint anti-malware software applications are installed, up-to-date and enabled on all systems.
- Continuous monitoring of network traffic and anti-malware scans to verify if traces of the malware still exist.

Post Incident

Lessons learnt are discussed, documented and changes are made to the incident management plan and other internal processes where necessary.

Ransomware Payments

In the event that the Trust's backup systems fail and data is unrecoverable, the only option might be to pay and that so being, St Thomas Catholic Academies Trust follows the National Crime Agency (NCA) and the ESFA's guidance regarding ransomware payments.

After Board approval, St Thomas Catholic Academies Trust will contact the ESFA to obtain permission to pay any cyber ransom demands. St Thomas Catholic Academies Trust is fully aware that by making such payments:

- our computer systems may be more likely to be targeted in the future
- there is no guarantee that the Trust's data will be returned

Secure Configuration

Configuration Principles

St Thomas Catholic Academies Trust’s IT assets are regularly reviewed to keep them aligned to the school’s dynamic functional requirements and any unnecessary or unused services are removed. All default credentials are changed to meet the standard detailed in this policy. St Thomas Catholic Academies Trust adheres to the ‘least privilege’ principle which ensures that users are granted the least possible privileges adequate enough to carry out work responsibilities. These principles aim to:

- Prevent unauthorised users from collecting, copying and modifying data.
- Prohibit the use of removable media (and other external peripheral devices) where possible, and to scan for malware where use is allowed.
- Prevent the execution of malicious code.

Unapproved Hardware and Software

St Thomas Catholic Academies Trust maintains an asset register which contains a list of approved software applications and hardware. All new software and hardware installations and modifications are approved and continuously monitored by St Thomas Catholic Academies Trust’s ICT Support Team and standard users are not permitted to perform any new installations.

Access to Systems

St Thomas Catholic Academies Trust ensures least privilege access to standard users which prevents them from installing additional software or creating additional user accounts. Access to systems strictly requires a strong password as detailed in the password policy. All user accounts are reviewed as stipulated in the school’s access control policy and unnecessary accounts are removed or disabled by St Thomas Catholic Academies Trust’s ICT Support Team.

Application Allow-listing and Execution Management

St Thomas Catholic Academies Trust implements application allow-listing for mobile and tablet devices, which explicitly permits only authorised software from the operating system vendor's 'app store' to be installed and executed on school devices where possible. Where allow-listing is not possible, the installation of new scripts and applications is prevented by restricting user privileges.

Auto-run/Auto-play

Automatic execution of code is prohibited. On Windows systems, auto-run is disabled using technical controls.

Implementation of This Policy

It is absolutely essential that this policy is implemented as completely as possible across all schools and systems as our weakest school or network will be an entry point into the whole trust infrastructure and systems. It is however important to note that implementing this policy globally will take time to achieve, and there are many cost implications to school budgets where hardware or systems cannot support the technical requirements of this policy. There are also requirements for harmonisation of systems for schools which join our Trust.

In order to manage the above implications with sensitivity to schools budgets and operational capacity, we will approve a transitional period to allow changes to be implemented in support of this policy. This will be agreed by the board of directors following a review of individual school circumstances conducted by the ICT Support Team and detailing the risks to Directors.

An action plan will be produced for those schools to ensure that high risk items are identified and remedied as soon as possible with all policy requirements being implemented within an agreed timeframe.

Author	Clark Campbell
Version	1.1