INFORMATION SECURITY POLICY

INTRODUCTION

Thomas's Academy frequently depends on its information systems. The availability, integrity, security and confidentiality of this information is vital to maintain service levels, legal compliance and the image and perception of Thomas's. Threats to the security of information/data are becoming more widespread, ambitious and increasingly more sophisticated. Consequently, Thomas's has a continual commitment to protect the School's and stakeholder information.

This purpose of this policy is to inform staff and explain the procedures Thomas's adopts to protect against security issues that might have an adverse impact on our organisation.

Security issues can include:

- Confidentiality (the wrong people obtaining information),
- Integrity (information being altered without permission, whether deliberate or accidental)
- Availability (information not being available when it is required and needed).

To this end, the application of Information Security across Thomas's is founded upon the following guiding principles:

- Information is a critical asset. All storage and transmission of information processed or controlled by Thomas's must only be carried out for the lawful purposes for which it is held.
- Information will be classified and protected in a manner commensurate with its sensitivity, value, and criticality.
- Information will be protected from loss of confidentiality, integrity and availability.
- Thomas's information should only be provided on a need to know basis and disclosed only to those people who have a legitimate need for that information.
- Information security requirements will be identified by assessment of risks to determine the balance of investment in information security against the risk to Thomas's and its stakeholders.
- A process of continual review and improvement will be implemented.
- Users, resources or processes that store, transmit or process information will have no more privileges than necessary to be able to fulfil their function.
- All relevant regulatory and legislative Information Security requirements will be met.
- All incidents and losses, regarding Information Security, actual or suspected, must be reported to the Data Protection Officer – Clare James, Deputy Head at cjames@academy.thomas-s.co.uk or 02077362318

- All systems must be reviewed, prior to implementation, and undergo a rigorous security assessment as part of that process.
- All Thomas's leaders are responsible for the implementation of Information Security Policies within their areas.
- Disregard for these policies may be regarded as misconduct to which the Thomas's Disciplinary Policy applies and a serious breach of any aspect may be treated as gross misconduct and may lead to dismissal.
- All staff are responsible for upholding this policy, under the guidance and with the assistance of the Data Protection Officer and the P & C team.
- Thomas's will provide appropriate security awareness training to all staff and provide specific security training where required, thereby developing and supporting a security and risk aware culture throughout Thomas's.

SCOPE

This policy applies to all members of staff; "Staff" includes all employees, counsellors, peripatetic staff, volunteers, gap students, work experience and any other individuals working for the Thomas's on a contractual basis, including temporary workers employed under special contracts and employees of organisations contracted to Thomas's.

It covers the use of all devices being used for purposes connected with the work of Thomas's. This includes users that work on Thomas's owned fixed or mobile devices, those who use Thomas's facilitated remote access technologies to connect from home or other non-Thomas's devices, or those users that have approval to use personal devices for work purposes using appropriate Thomas's approved and provided technologies.

Contents

1. Password and Authentication
2. Anti-Malware
3. Access Control
4. Clear Desk & Clear Screen
5. Mobile Working
6. Removable Media Devices
7. Encryption
8. Protective Monitoring of Thomas's Information Systems
9. Security Incident Management
10. Patch Management
11. Backup and Retention
12. Starters and Leavers Data Access

1. Passwords and Authentication

A password is arguably the most critical IT Security control for any computer system. Thomas's has clear standards for the creation, protection, use and management of passwords across and within the organisation. They must always be used in conjunction with a Unique Username.

Passwords are required to be long and complex because of the tools cyber criminals use, the premise is to make the password complex enough so by the time it could be recovered by automated attacks it would have been changed.

Passwords assist in protecting against unauthorised access to Thomas's data, confidential or otherwise.

Authenticating yourself to a computer system requires a process where you prove ownership of the account by demonstrating knowledge or possession of a shared secret; generally this can be achieved in several ways using one or more of the following methods:

- Something you know (Password, secret word, phrase etc.)
- Something you are (Biometric – fingerprint, retina etc.)
- Something you have (e.g. Google Authenticator, Number Generator Token)

Any user of any organisation accessing a Thomas's managed system or Thomas's managed data must be issued a unique account to identify them.

For email access, delegation is the only permitted method of accessing another employee's email account (for Heads with PA's).

The user must select a password that meets or exceeds the minimum requirement for the specific system. In general password length must be a minimum of 8 characters. Some systems are configured with specific password requirements that may be more complex than only 8 characters. The most secure method of authentication must be used where it is available i.e. a 2-Factor method where there is a choice instead of Basic Authentication using just a username and password.

All passwords are to be treated as 'sensitive' information.

Thomas's staff must not:

- Share system passwords with anyone, including peers, assistants or superiors, even if requested
- Discuss or talk about a password in front of others
- Hint at the format of a password (e.g., "my family name")
- Reveal a password on any questionnaires
- Share a password with family members
- Reveal a system password to co-workers providing holiday or absence cover
- Write passwords down
- Store unencrypted passwords in a file on ANY computer system

Thomas's staff should immediately change a password if they suspect that it has been compromised, following which they must immediately report the incident to the Director of IT.

2. Anti-Malware

All devices within the Thomas's computing infrastructure must meet the following requirements in order to protect the confidentiality, integrity and availability of Thomas's software and information assets from the effects of malware.

- Unless undertaken by or following instruction from IT support staff, Thomas's staff must not disable anti-malware software running on, or prevent updates being applied to, devices within the Thomas's computing infrastructure.
- The intentional introduction of viruses to Thomas's computing infrastructure is strictly prohibited.
- Only software that has been authorised by the Thomas's IT Department can be installed upon Thomas's systems.
- Each Thomas's member of staff is responsible for immediately reporting any abnormal behaviour of Thomas's computing systems to the IT Support.
- All members of staff are responsible for ensuring that appropriate and effective anti-virus detection software is installed and running, where technically possible, on all personal devices that are used to access Thomas's information.

3. Access Control

Access to specific resources is only to be granted to authorised personnel who have a legitimate need to use those resources.

- Users of Thomas's information will have no more privileges than necessary to be able to fulfil their role.
- All requests for access to Thomas's computer systems must be made in writing to the Director of IT.
- Thomas's reserves the right to revoke access to any or all of its computer systems at any time.
- Regarding inappropriate access:
    - Users of Thomas's systems must immediately report to the IT Department if they have an inappropriate access level to a Thomas's system.
    - If they have observed that another user has an inappropriate access level to a Thomas's system, then they are required to raise this with IT Support to raise this potential security incident.
- Accounts are to be created so that the identity of all users can be established and activity audited at any time during their computer usage.
- Users must not circumvent the permissions granted to their accounts in order to gain unauthorised access to information resources.
- Users must not allow anyone else to use their account, or use their computers while logged in with their account.

4. Clear Desk and Clear Screen

Thomas's has both a Clear Desk and Clear Screen Policy to reduce the risk of unauthorised access, loss of and damage to information during and outside normal working hours or when work areas and computers are unattended. The Schools require protection against unauthorised access to information. In addition, all information must be protected according to legal and contractual requirements.

This policy applies to all staff members and any other person utilising any form of Thomas's information technology, or having responsibility for school data stored in an alternate format, such as paper. It covers any papers, removable storage media and any computing devices that contain or display sensitive, personal or confidential information, regardless of location.

Thomas's requirements are as follows:

- It should be assumed at all times that individuals, other than Thomas's employees, may have access to office areas. Consequently, no sensitive information should be left on a desk surface overnight or when the desk is unoccupied.
- Removable media and easily portable devices, such as laptop computers or iPads, that have not been physically secured, should not be left unattended after hours, overnight or during school holidays.
- Where practically possible, sensitive papers, computer media and portable computing equipment should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use.
- At the end of each working day all personal and sensitive information should be stored in locked furniture.
- Where lockable storage is not available, office/room doors must be locked if left unattended.
- All information should be cleared from printers and photocopiers immediately after processing and, when no longer required, destroyed in a secure manner using approved methods.
- Reception areas, and other areas of high levels of foot traffic, should be kept as clear as possible at all times; in particular Thomas's information classified as confidential or personal should not be held on a reception desk within reach or sight of visitors.
- Any visit, appointment or message books should be stored in a locked area when not in use.
- When vacating meeting rooms or shared areas the area should be checked to ensure that no information, regardless of format, has been left behind. All whiteboards should be cleaned of information, and used flipchart pages removed and disposed of securely.
- Computer screens should be 'locked' or the user logged out before leaving any workstation unattended, even for a brief period.

5. Mobile Working

Thomas's aims to continue to take advantage of the many benefits offered by mobile computing technology. However the school recognises there are additional risks which must be effectively managed to protect Thomas's, its staff, pupils and parents, and the services and data on which they rely, against known and emerging threats.

Any user of a mobile computing device used to store or process Thomas's data should comply with this policy and follow the instructions whilst using, transporting and acting as custodian of any Thomas's procured mobile device or any other mobile device approved by the IT Department for use within Thomas's. It describes what information can be stored and processed on mobile devices and how data must be protected physically and/or electronically.

Definitions

- Mobile devices continue to evolve and thus this is not an exhaustive definition/list however, it includes all battery powered and mains adapted computing and storage devices such as:
    - Laptop
    - Tablet
    - Mobile Phone
- Sensitive Electronic Data (SED) is either personal identifiable data or confidential business data, the unauthorised disclosure of which could cause Thomas's and its employees to be in breach of the law and/or cause embarrassment to the Thomas's, staff, pupils and parents.

Duties and Responsibilities

- The IT Department will:
    - ensure that Thomas's issued mobile devices are encrypted as a matter of course unless an exceptional case for not doing so has been approved
    - provide advice on implementation of this policy as requested
    - ensure that user access rights are correctly implemented
- The Director of IT is responsible for ensuring that:
    - all staff allocated mobile devices have a genuine need for mobile computing
    - staff sign to confirm they have received the Thomas's owned device loaned to them
    - suspected breaches of this policy are logged
    - all Thomas's mobile devices are returned by owners leaving Thomas's or no longer requiring them
- Thomas's staff must:
    - abide by this and the ICT (Acceptable Use) Policy
    - report any suspected breaches of this policy to the IT Department
    - understand that failure to comply with this policy may result in disciplinary action
    - report the loss or theft of a mobile device to the Director of IT at the earliest possible opportunity
    - return all devices to the IT department when leaving Thomas's or no longer requiring the use of a Thomas's procured device

Physical Security

Owners shall accept full responsibility for the security of the device, taking necessary precautions to avoid loss, theft or damage. In particular:

- taking all reasonable care to prevent the theft or loss of the device. Mobile devices should not be left unattended in a public place or in vehicles. When transporting devices they should be safely stowed out of sight
- taking extra vigilance if using a mobile device during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of Thomas's data by a third party "overlooking"

- not leaving the device unattended for any reason whilst working on it unless the session is "locked" and it is in a safe working place
- ensuring that other 'non' authorised users are not given access to the device or the data it contains

Passwords & PIN Codes

Passwords are an integral part of the Access Control mechanisms which are enforced by the Operating System. Passwords and/or PINs should not be written down.

Approved Use

Thomas's mobile devices are supplied with pre-installed software that has been procured by the IT Department and approved by the Thomas's. Owners must not attempt to install any software including their own privately procured and licensed software onto any Thomas's mobile device. Under no circumstance is Thomas's software to be upgraded, deleted or copied by users/owners. Owners are not permitted to attach additional unauthorised hardware, with the exception of printers, or in any way change the original hardware configuration of the device, without prior approval from the IT Department.

Storage of Data

Data should not normally stored on the local drives as such storage is not backed up by Thomas's. Data should be saved or transferred to network drives or Thomas's provided Cloud storage.

Protection of Sensitive Electronic Data

All Thomas's issued laptops are encrypted. Any tablet or mobile phone issued by Thomas's shall be managed by the approved Mobile Device Management (MDM) solution and may not be removed from the MDM. The security features of the MDM ensures that if the device is lost or stolen a remote wipe can be sent to clear data off the device.

Remote Access

All Thomas's laptops issued to staff will be fully configured to enable the user to connect back to the Thomas's network, by Fortigate VPN client. Connecting through the Fortigate VPN client creates a secure tunnel back to the network and the user will have access to the Thomas's network resources and systems. The same Fortigate VPN access is also available on special request in writing for other personal devices and Thomas's iPads. All mobile devices with Fortigate VPN access will be logged in the VPN access log.

Back Up

In order to make sure that data can be recovered if accidentally deleted or corrupted it is essential to ensure that it is routinely 'backed-up'. The safest method to backup information is by routinely saving work to a dedicated Thomas's network share or cloud storage. During occasions where this is not possible and data has been created in a "local profile" the user must connect the device to the Thomas's network and download locally stored data to the designated Thomas's network storage area when it is possible. It is advised that information transfers to Thomas's storage areas should not exceed 14 days.

Audit and Monitoring Controls

Thomas's systems are capable of logging events that have a relevance to potential breaches of security.

Investigations/Disciplinary Proceedings

- The Director of IT is authorised to investigate all suspicious, inappropriate or illegal activity involving Thomas's IT equipment and data however it may come to their attention. No other members of staff are authorised to conduct such activities involving IT equipment or data unless directed by the Director of IT
- In the event of a requirement to investigate user activity or disciplinary proceedings being conducted by the Personnel Department, the Director of IT will gather and make available all appropriate information from various sources to assist the investigator(s)
- In the event that a line manager requests the Director of IT to provide reports about user activity then these will only be completed where authorisation from the Governors endorses this request
- Where action has been taken by the Director of IT to remove access to a user account or data then access to that computer account or data may only be granted if appropriate confirmation in writing is forthcoming to the Director of IT. (Email is considered written confirmation)

Training Requirements

Training for Thomas's procured mobile devices is covered when the devices are first given to an employee. This covers basic elements of Information Security and draws attention to relevant policies that all users are expected to read and comply with. If members of staff require further training they should request this from the IT department. IT Support staff are conversant with the appropriate standards and guidelines referenced by this policy.

Monitoring Compliance

The IT Department routinely audit and monitor relevant aspects of this policy. Compliance to this policy is mandatory and loss of a device is a major risk to the Thomas's, any loss would be reportable to the Information Commissioner's Office.

6. Removable Media

All Thomas's systems are accessible remotely by VPN or secure Cloud storage and the School has mandated that there is no need for anyone to use a USB Memory Device or External Hard Drive to store or transfer data. If there is a need for anyone to use such a device a request must be made to the Director of IT in writing. Only secure and encrypted Thomas's issued devices may then be used in rare circumstances.

7. Encryption

In order to mitigate the risk of disclosure or tampering with Thomas's data through interception, loss or theft of data or equipment, Thomas's shall deploy appropriate cryptographic security controls in conjunction with procedures that manage the associated encryption keys. The policy covers the application of encryption to Thomas's mobile devices, external storage devices and remote access.

Where valid reasons exist, exceptions to this policy can be signed off by the Director of IT.

Thomas's data shall normally be created and stored within a Thomas's managed secured system. However, when Thomas's data is transmitted outside such a secure system, it shall be encrypted in transit. Encryption in transit may include encrypting a file sent via email, encrypting a laptop, tablet, mobile phone or external storage device used to transfer or store data or the use of encrypted transmission protocols such as SSL. All data externally shared electronically or by synchronising with 3rd parties will be done by encryption technologies such as SSL

8. Protective Monitoring of Thomas's Information Systems

The use of Thomas's data communications infrastructure, services, systems and applications may be monitored by authorised personnel as permitted by UK legislation, which allows the monitoring of systems and network traffic without consent for legitimate purposes such as:

- Recording evidence of activity
- Policing regulatory compliance
- Detecting crime or unauthorised use
- Safeguarding the integrity of Thomas's information and information systems

Authorised Thomas's personnel may monitor and analyse network services, systems, data (including file systems), applications and data communications facilities pertaining to Thomas's business activities.

Thomas's staff are prohibited from engaging in monitoring activities or monitoring outside of their areas of responsibility without written authorisation from any of the following:

- Governors
- Director of IT
- Personnel Manager

9. Security Incident Management

Thomas's aims to respond to security Incidents effectively and in a timely manner. Staff members should understand their roles and responsibilities when dealing with and notifying the IT department of an Information security incident.

- It is the responsibility of each member of staff to report any suspicion or details about Information/Cyber Security Incidents to the Thomas's Privacy and Compliance team as soon as possible to help us deal with the incident swiftly by directing to the correct resource.
- Thomas's staff must never attempt to interfere with, prevent, obstruct, or dissuade an employee, in their efforts to report an information security problem or violation, or retaliate against an individual for reporting or investigating.
- Any details relating to an information security incident can only be communicated to the press or other media by the Governors.
- Unless compelled by local or UK law, or authorised by the Governors, staff must not report information security incidents to individuals or organisations external to Thomas's.

- All staff must be aware of and have access to the current documented Personal Data Breach Procedure that clearly specifies how Information Security Incidents will be handled; all security incidents are dealt with by the Privacy and Compliance team, as per the procedure.
- Users of Thomas's information systems must immediately report to IT Support, any unusual and suspicious activity such as unusual requests for information coming from any internal or external party, and abnormal system behaviour.
- Thomas's staff must immediately report to the Privacy and Compliance team any damage to or loss of Thomas's computer hardware (including mobile devices), software, or information (electronic or paper) that has been entrusted to their care.
- All information security incidents must be handled with the involvement and cooperation of the Privacy and Compliance team.
- Any member of staff who reports a security problem, vulnerability, or an unethical condition within Thomas's will be protected in line with Thomas's Whistleblowing Policy.
- All investigations, where an individual is identified as a possible cause, must be kept strictly confidential to preserve the reputation of the suspected party as charges may be formalised and/or disciplinary action taken.

10. Patch Management

Software is critical to the delivery of services to users. Thomas's carries out regular security updates and patches to operating systems, firmware, productivity applications, and utilities in order to maintain a secure operational environment.

Regular application of vendor-issued critical security updates and patches are necessary to protect data and systems from malicious attacks and erroneous function. All electronic devices connected to the network including servers, workstations, mobile devices, wireless access points and firewalls routinely require patching for functional and secure operations.

- GENERAL
  All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the network shall be regularly maintained by applying critical security patches within 30 days after release by the vendor. Other patches not designated as critical by the vendor shall be applied during Thomas's school holidays.
- PATCHING EXCEPTIONS
  Patches on production systems may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing. Deviations from normal patch schedules shall require authorisation from the Director of IT.
- AUDIT CONTROLS AND MANAGEMENT
  Documented evidence of practice are in place for this operational policy and listed below.
  - Documented change management meetings and conversations between key stakeholder
  - System updates and patch logs for all major system and utility categories
  - Logs include system, date patched, patch status, exception, and reason for exception

11. Backup

The purpose of backup is as follows

- To safeguard the information assets of Thomas's.
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media used in the process.

This policy applies to all servers in the Thomas's Domain.

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.

Backup retention periods are in contrast to retention periods defined by legal or business requirements.

System backups are not meant for the following purposes

- Archiving data for future reference.
- Maintaining a versioned history of data.

Scope

This policy, and supporting procedures, encompasses all system resources and supporting assets that are owned, operated, maintained, and controlled by Thomas's and all other system resources, both internally and externally, that interact with these systems.

Roles and Responsibilities

- The Director of IT will ensure facilities are available.
- The Director of IT will ensure sufficient backup locations are available and shall take overall responsibility for adherence to this policy.
- The Director of IT will ensure backup operators are available, check the backup log for completion, be responsible for the safekeeping and availability of all backup locations and logs, and meet with departments with regard to actual/test restores.
- Backup operators will ensure backup logs are completed, report any backup failures to the Director of IT, and investigate any reported exceptions.

System Backup

- All servers and data stored on dedicated network shares and NAS appliances will be regularly backed up as follows:
    - Incremental backups daily (Monday to Thursday) and data located on-site.
    - Full backups weekly (Friday) and data located on-site.
    - Full backups every four weeks (Friday) and data located off-site.

Backup Locations

- Backups will be written to a dedicated backup NAS on each site.
- Backup locations are in a secure area that is accessible only to IT staff.
- Daily backups will be maintained for one week.
- Weekly backups will be maintained for a period of three weeks.
- Backups off-site will be maintained for a period of eight weeks.

Disposal of Backup Locations

- Prior to retirement and disposal, IT will ensure that:
    - The media no longer contains active backup images
    - The media's current or former contents cannot be read or recovered by an unauthorised party.
    - With all backup media, IT will ensure the physical destruction by an approved IT disposal company.

Verification

- On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:
    - To check for and correct errors
    - To monitor the duration of the backup job
    - To optimise backup performance where possible
- IT will identify problems and take corrective action to reduce any risks associated with failed backups.
- Random test restores will be done once a month in order to verify that backups have been successful
- IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

Data Recovery

- In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days.
- In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.
- A full disaster recovery of one Thomas's school site will be performed each Summer holiday for verification. The full disaster recovery will be logged and any problems addressed.

Restoration Requests

- In the event of accidental deletion or corruption of information, requests for restoration of information will be made to itsupport@thomas-s.co.uk.

12. Starters and Leavers Data Access for members of staff

With access now available through a wide array of systems, it is vital to have a correct procedure for managing the flow of employees' access from the moment they join to when they leave.

Procedure for staff starting at Thomas's:

- The Personnel department notifies the IT department when a new member of staff is employed with their start date
- This information is captured in a staff changes sheet/log
- The IT department creates all new staff accounts with the correct access one day before the new employee starts or one day before they come for their induction training
- The office manager and IT support technician on-site are all informed of the new staff member and their login details when the accounts are created

Procedure for staff leaving Thomas's:

- The Personnel department notifies the IT department when a staff member gives notice
- This information is captured in the staff changes sheet/log
- At the end of the day of termination of employment all accounts are removed or disabled and the old member of staff will have no further access to any systems
- Any keys and/or IT equipment issued to the staff member should also be returned to the IT department on or before their last day of employment
- It is the responsibility of the IT department to ensure all equipment is handed back

See also: CCTV Policy, Data Protection Policy, ICT (Acceptable Use) Policy, Online Safety Policy, Personal Devices and Photography Policy, Pupil and Parent Privacy Notice, Record Management Policy, Safeguarding and Child Protection Policy

Staff Handbook: Staff Privacy Notice

This policy will be reviewed annually		
Created: May 2018	By:	Michael Swart, Director of IT
Next Review: May 2019	By:	Michael Swart, Director of IT