Thinking Schools Academy Trust
“Transforming Life Chances”

Information Security Policy

This policy was adopted on	July 2023
The policy is to be reviewed on	July 2027

1. INTRODUCTION

1.1 Information is one of the Trusts most important assets. Failure to ensure adequate security and protection of information held by the Academy or Trust may lead to legal action against the Academy and/or the individual responsible for the breach. Such legal action could include an investigation by the Information Commissioner's Office ("ICO") who can impose significant financial penalties and/or a claim for damages for breach of the General Data Protection Regulation and the Data Protection Act 2018 (together the "Data Protection Legislation").

1.2 In addition to the possibility of legal action being taken against the Academy or Trust, if the information held by the Academy or Trust is not kept safe, confidence in the Academy and the Trust by pupils, parents, guardians, volunteers, the Board of Governors, members of staff and the public at large could be irreparably damaged.

1.3 Keeping information secure yet available to those that need it often presents a difficult challenge. This policy strives to achieve a sensible balance of securing the information held by the Academy while making it accessible to those who need the information. The Academy will always however favour security over accessibility where there is any doubt as to the security of information.

2. Definitions

2.1 "*The Trust*" means Thinking Schools Academy Trust.

2.2 "*Data Protection Legislation"* means the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2.3 *"Data"* means Personal Data and Special Category Personal Data as defined by the *Data Protection Legislation*, and confidential and sensitive information held by the Trust.

2.4 "*Personal Data*" any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.5 *"Special Category Personal Data*" means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

2.6 "*Processing*" means any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

2.7 *"Data Controller"* is the organisation which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing

 practices and policies in line with Data Protection Legislation. The Data Controller referred to in this policy is The Thinking Schools Academy Trust

2.8 *"Data Protection Officer"* is The person within the organisation who is responsible for overseeing data protection strategy and implementation to ensure compliance with data protection legislation. Within The Thinking Schools Academy Trust that role is held by the Deputy CEO.

2.9 "*Data Subject*" means all living individuals about whom the Academy holds Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in respect of their Data and the information that the Academy holds about them.

2.10 *"Data Processor*" means any person who or organisation which processes Data on behalf of the Data Controller including members of staff, volunteers, contractors, and suppliers and any third party whose work involves accessing or otherwise using Data held by the Academy. Data Processors have a duty to protect the information they process for and on behalf of the Academy by following this and other Academy information governance policies at all times.

2.11 "*Subject Access Request*" ("SAR") means a request by an individual to the Academy pursuant to Article 15 of the GDPR.

2.12 *"Information Asset"* means Data held by the Academy in any form. This Data may be held electronically by software in computer systems and transferred across a network, on paper, in files or transferred by post, courier or in person.

2.13 "*Information Governance Policy*" means the Data Protection, Freedom of Information, Information Security, Retention, Disposal and Records Management and Subject Access Request policies and any other policies which may from time to time be in place at the Academy.

2.14 "*ICO*" means the Information Commissioner's Office.

2.15 "*Information Security*" means the protection of information and information systems against unauthorised access to or modification of information, whether in electronic or manual storage, Processing, transit and against the denial of service to authorised users.

2.16 "*Information Security Breach*" means a breach which may be caused by a technical failure, unauthorised access to either the Academy's network or a Client Device used for Academy business by a third party, loss of the Academy's information and/or inappropriate actions of an individual or individuals which result in the compromise of information belonging to or held by the Academy.

2.17 "*Information Security Vulnerability*" means an identified weakness of a system(s) or process that puts the security and availability of information at risk.

2.18 "*Member of Staff*" means individuals working at the Academy whether on a full time, part time, temporary, fixed term, casual or volunteer basis.

2.19 *"Client Device*" means laptops, tablets, telephones, smartphones, desktop computers or other electronic equipment that could be used for the carrying out of Academy business or the Processing or storing of information.

2.20 *"Personal Device*" means a Client Device not directly owned by the Academy.

2.21 *"Username"* means a unique sequence of characters used to identify a person, system or service, allowing access to a computer system, computer network, client device, or online account.

2.22 "*Strong Password*" means a phrase of sufficient random characters to prevent guessing or brute-force attacks. A Strong Password must be a minimum of 9 characters, does not use single common number sequences/dictionary words or easily accessible personal information (i.e. any portion of your name, date of birth, telephone numbers or NI numbers). Strong Passwords of less 24 characters must include a combination of three of the following: lowercase and uppercase letters, numbers and symbols.

2.23 "*Secure Authentication Device*" means a device or component integrated into a Client Device that allows the encrypted storage and retrieval of Strong Passwords using biometric information.

2.24 "*Two-Factor Authentication (also known as Multi-Factor Authentication, MFA or 2FA)"* means a method of confirming a claimed identity using a combination of at least two of the following categories: knowledge (something they know, e.g. a password), possession (something they have, e.g. a token), and inherence (something they are, e.g. a fingerprint).

2.25 "*Authorised User"* means a person, or administrative service, that is authorised by the Trust to authenticate to a system, that may contain Data and potentially to receive authorization to access resources provided by or connected to that system;

2.26 "*Removable Media*" includes USB sticks, external hard drives, CD's or other media which can be connected to the Academy network or a Client Device and used for storing information.

2.27 "*External*" means any and all buildings, systems or services not directly owned by the Trust, including all accounts not ending in tsatrust.org.uk or tsatstuduent.org.uk

2.28 "*Social Media"* means websites and applications that enable users to create and share content or to participate in social networking including Facebook, LinkedIn, Twitter, Google+, and all other social networking sites, internet postings and blogs. It applies to use of Social Media for Academy purposes as well as personal use that may affect the Academy in any way.

2.29 "*Cloud service*" means Cloud computing/Service is the delivery of computing resources using a network of remote servers hosted on the Internet to store, manage, and process data, rather than local servers or a personal computer.

3.30 *"Non-trusted location"* means a computer network that is not provided or managed by the Trust. For example, a home network or personal cellular connection.

3. Summary

3.1 Much of the information held by the Trust is confidential and sensitive in nature. Therefore, it is necessary for all information systems to have appropriate protection against adverse events (accidental or malicious) which may put at risk the activities of the Academy or protection of the information held.

3.2 The Academy has a responsibility to maintain:

i. **Confidentiality** – access to Data must be confined to those with specific authority to view the Data in question;

ii. **Integrity** – information should be complete and accurate. All systems, assets and applicable networks must operate correctly and according to any designated specification;

iii. **Availability** – information must be available and delivered to the right person at the time when it is needed and in accordance with the relevant statutory provisions.

3.3 The Academy must minimise the risk of data security breaches and any person connected to or acting on behalf of the Academy must meet the minimum requirements as set by the Academy/Trust for connecting to any network operated by or on behalf of the Academy. This can be found in Appendix 2.

3.4 It is important that members of staff, governors or anyone else acting on behalf or with the authority of the Academy:

i. Are aware of how and under what circumstances they are permitted to access Personal Data held by or on behalf of the Academy;
ii. Is aware of who they are allowed to share Personal Data and other information with and how it can and should be shared;
iii. Reports any Information Security incidents/breaches including phishing emails[1] to the Data Protection Officer in respect of information in respect of or held by the Academy. Staff & Governors must follow the Data Breach flowchart in Appendix 4 when reporting a Data Breach;
iv. A Data Breach report must be filled out and past to the DPO after initial reporting of a breach. The report can be found in Appendix 5
v. Ensures Data is stored and handled securely and in accordance with this and the other information governance and IT Policies;
vi. Does not ignore, turn off or otherwise bypass any Information Security controls put in place by the Academy;
vii. Does not send, distribute or otherwise divulge Data unless permitted to do so. The sending or distribution of any Data should only be done in accordance with the

applicable statutory provisions, this policy and any other applicable policy of the Academy;

viii. Data must only be sent by secure methods and, all Data sent externally shall be encrypted.

4. Policy Statement

4.1 It is essential that the Academy's information systems and data networks are adequately protected from events which may compromise the information held or the carrying on of Academy business and to this end the Academy is committed to developing and maintaining an information systems structure which has an appropriate level of security.

4.2 The Academy will maintain the security and confidentiality of Data held by it, its information security systems and relevant applications and networks for which it is directly responsible by:

i. Ensuring appropriate technical and organisational measures are in place to prevent unauthorised access, damage or interference to and/or with information, IT assets and network services;
ii. Ensuring that it is aware of, and complies with, the relevant legislation as described in this and the other information governance and IT Policies;
iii. Describing the principles of Information Security to Members of Staff, pupils, governors and volunteers and explaining how they will be implemented by the Academy;
iv. Creating and maintaining a level of awareness of the need for information security to be an integral part of the conducting of Academy business and ensuring that everyone understands their individual and collective responsibilities in this respect;
v. Protecting Data and other information held by and/or on behalf of the Academy.

4.3 To ensure a consistent approach to Information Security, the controls set out at sections 7 and 8 of this policy will apply.

5. Use of Client and Personal Devices

5.1 Client Devices used for, or in connection with, Academy business and in particular for the collection or storing of Personal Data and/or Special Category Personal Data must be kept secure with Strong Passwords (see Definitions). If available with the device, an approved Secure Authentication Device to aid entering the of the password;

5.2 Client Devices used for, or in connection with, Academy business must not be left unattended in plain sight at any time, including whilst at home or travelling, and must be protected against loss, damage, misuse or unauthorised access. When not in use, Personal Devices must stored in a secure, lockable location and should never be stored in vehicles, even if locked.

5.3 Client Devices used for, or in connection with, Academy business must not be used to access, view or process Personal Data or Special Category Personal Data in a manner that allows Persons other than the Authorised User to view the Data.

5.4 Personal Devices, including but not limited to, laptops, tablets, telephones, smartphones, desktop computers or other electronic equipment, must not be used to store or transmit Data. Where a Member of Staff believes there is a legitimate need to Page **7** of **22** process Special Category Personal Data using a Client Device, the Member of Staff should contact

their Line Manager with a business case for the provision of a Client Device, who shall evaluate the business case for such request.

5.5 Client Devices used for, or in connection with, Academy business must be updated with the manufacturer's software and other updates regularly when updates become available, and where supported have antivirus software installed and regularly updated.

5.6 Client Devices used to store Personal Data or Special Category Personal Data must be encrypted.

5.7 Client Devices issued to a Member of Staff for or in connection with, Academy business by the Academy must only be used by Academy Members of Staff. At no time shall any other User, including but not limited to, family members, friends, employee from another organisation, be permitted to use the device.

5.8 If a Client Device used for, or in connection with Academy business it lost or stolen, the loss/theft should be reported to Data Protection Officer and IT Support Team as soon as possible and in any event within 24 hours of the loss/theft occurring. Where possible the Client Device should be remotely accessed and the information erased.

6. Removable Media

6.1 Removable Media storing Data must only be used as a last resort, when all other options have been considered, including the need to store or process the data. All Data must secure network service is not available.

6.2 Only Removable Media provided by the Academy or Trust that has been encrypted should be used for the storing of Data.

6.3 Removable Media should not be used for the storing of Personal Data, Special Category or Sensitive Data unless the device is capable of and has been encrypted.

6.4 Removable Media must be stored securely.

6.5 If Removable Media used for, or in connection with Academy business is lost or stolen, the loss/theft should be reported to Data Protection Officer and IT Support Team immediately. Where possible the Personal Device should be remotely accessed and the information erased.

7. Securing Information

7.1 Physical Access Controls

i. A nominated member of the Academy will be responsible for ensuring the Information Security of all Information Assets held by or on behalf of the Academy. The nominated person will also have and maintain an Information Asset register which should record all Information Assets held by the Academy;

ii. A copy of the Information Asset register will be filed with the Data Protection Officer at the Trust each year; Page **8** of **22**

iii. The Academy will ensure that only authorised individuals are allowed access to restricted areas containing Personal Data or Special Category Personal Data or information systems where there is an identifiable need to access that area;

iv. Access to Personal Data and/or restricted physical locations will be monitored by the Academies nominated person to ensure authorised access to relevant information and to prevent unauthorised access to Personal Data or Special Category Personal Data;

v. Where an unidentified person or any other person without authorisation to be in a restricted area is found, the individual is to be challenged as to their identity and the purpose for which they are in the restricted area. If the unauthorised individual has no legitimate reason to be in the restricted area, this information is to be logged as an Information Security Breach and the Data Protection Officer should be consulted as to whether the matter requires reporting to the ICO;

vi. External doors and windows must be locked at the end of each day;

vii. Equipment that serves multiple users must be capable of identifying and verifying the identity of each authorised user;

viii. Devices or equipment capable of displaying output upon multi-user displays or presentation equipment, including but not limited to, Projectors, Interactive Whiteboards, televisions, video walls, remote computer sessions and desktops, or any other form of presentation equipment, must not be used to access, view or process Data in a manner that allows Persons other than the Authorised User to view the Data.

ix. Members of staff of the Academy with access to and use of Data must maintain a clear desk and clear screen policy to reduce the risk of unauthorised access to Information Assets such as papers, media and information processing facilities;

x. Academy wireless systems should be secured to industry standard Enterprise security level/appropriate standards suitable for educational use;

xi. Data recorded on paper must be kept locked away in a safe, cabinet or other form of secure furniture when not in use;

xii. Personal Data and Special Category Personal Data, confidential and sensitive information about the Academy whether stored electronically or on paper must be kept locked away in a secure room or in a safe, cabinet or other form of secure furniture when not in use;

xiii. Documents containing Data must not be left unsecured, unattended at mail points or on printers, photocopiers, scanners or fax machines and must be removed immediately when received.

7.2 Password and Access Control

i. Access to Data stored electronically must be controlled through the use of a Strong Password;

ii. Access to Authorised User accounts must be controlled, as a minimum, through the use of a password, which must not be less than 6 ASCII characters Page **9** of

22 in length. Wherein, a system or service, provides alternative authentication methods, including but not limited to, facial or biometric recognition, the alternative authentication method must be in additional to a password;

iii. Members of Staff must ensure that they have a Strong Password for all Authorised User accounts and the same password not re-used across different types of system;

iv. Members of Staff must also ensure that they use Two-Factor Authentication for all Authorised User accounts for cloud services and web applications, whereby the vendor provides support for additional authentication;

v. Effective from the 1st September 2023 all staff and governors will be required to complete Two-Factor Authentication when attempting to sign-into the Trust's Microsoft365 tenancy from a non-trusted location;

vi. Following the latest industry guidance, Authorised User accounts that are configured to require Two-Factor Authentication and a Strong Password will not be forced to change the password upon reaching an expiration date. Forced password changes will be enforced for any user accounts that are either known to have been compromised or have been flagged as "high risk" due to the account activity;

vii. All Authorised Users, aged 11 or over after the 1st September each year, should ensure they have a Strong Password for all accounts;

viii. Authorised Users are responsible for keeping their assigned password(s) secure and must ensure their password(s) is neither disclosed to, nor used by, anyone else under any circumstances;

ix. Use of another person's username or password will constitute an Information Security Breach and must be reported in accordance with the procedures set out in this policy or any other relevant policy from time to time in force;

x. Authorised Users are responsible for ensuring that all Academy and/or Client Devices used to access Data or other confidential information, are logged off, switched off or otherwise controlled by a Strong Password when unattended or not in use, at all times;

xi. Authorised Users with access to the Academy network or a Client Device which is used for, or in connection with Academy business is responsible for any actions carried out under their username and password.

7.3 Cloud Computing

i. Only cloud computing networks or services, including Social Media commissioned by the Academy, or expressly authorised by the Data Protection Officer, may be used to store and send information concerning or relating to Academy business. The use of personal cloud storage solutions (Skydrive, Onedrive Personal, iCloud, G-Drive etc.) for the transfer of Academy information is expressly forbidden.

ii. Personal Data, Special Category Personal, confidential and sensitive information, whether on the Academy network or a Client Device must not be stored on a cloud computing network or service not commissioned by the Academy, or expressly authorised by the Data Protection Officer.

iii. If Data or other information concerning or relating to Academy business is to be stored in or on a cloud network, the Academy will take all reasonable steps to find out in which country the Data or other information is being stored, and to ensure that appropriate measures are in place in relation to any Data transferred outside of the EEA.

iv. If the Academy receives notification that Data in respect of Academy business has been corrupted, lost or otherwise compromised while stored on a cloud Page **10**

of **22** network, the Academy should ascertain whether any or all of the information stored in the cloud can be recovered and if this is possible restore that information;

v. Any corruption, loss or compromise of information held on a cloud network should be recorded in the risk register and if appropriate reported via the mandatory reporting procedure set out at section 9 of this Policy.

7.4 Leaving the Academy/Contract Termination

i. Upon leaving the Academy, Members of Staff must return/transfer, in a useable format, all equipment and information, including Data to the Academy, on or before the agree leaving date (e.g. last day of employment) to their Line Manager, or other Academy representative if their Line Manager is not available. This includes, but is not limited to:

- All information, including data, used or stored as part of the role, both physical and electronic;
- All information, including files, documents and emails, including any Data, stored within individual Cloud Service accounts;
- Client Devices loaned by the Academy, including PIN numbers, usernames or passwords required to reuse or reset the devices;
- Any Removable Devices provided by the Academy;
- Access control, PIN, tokens and ID Cards;
- Keys and PIN numbers used to access physical locations.

ii. The Off-Boarding Checklist (see Appendix 3) must be completed and returned to Human Resources by the leaving date;

iii. After leaving Members of Staff may not attempt to access or use any Academy information, including any Data.

8. Storing and Transportation of Non-Electronic Data

8.1 Data can be vulnerable to loss, unauthorised access, misuse or corruption when being physically transported either personally by Member of Staff of the Academy or when sending Data via the postal service or couriers;

8.2 Special controls should be adopted where necessary to protect Data from unauthorised disclosure or modification and may include:

i. Ensuring the packaging is sufficient to protect the contents from any physical damage likely to arise in transit;

ii. Delivering by hand records containing Personal Data, where appropriate;

iii. Sending Data via secure post such as Royal Mail recorded or signed for delivery or special delivery or as otherwise agreed with the Data Subject;

iv. Records containing Special Category Personal Data shall not be delivered by hand unless absolutely necessary. In which case the following should occur:

a. Documents transported in vehicles should be hidden away or placed in boot where possible, and the vehicle locked.

b. Documents should never be left unattended even in a locked vehicle.

8.3 Consideration should be given to the necessity of transporting or moving Data or other records as this increases the risk of Data loss.

9. Transportation/Transmission of Electronic Data

9.1 Personal Data, Special Category Personal, confidential and sensitive information sent or transmitted externally using an electronic systems or services must be secured using a process that ensures the Data is encrypted and Users must carefully check the recipient's contact details before sending.

9.2 Data must only be sent or transmitted externally when authorised by job description, Trust policy, applicable legislation, or when specially authorised by the Data Protection Officer. The sending of Personal Data and Special Category Personal Data to personal cloud systems or services email accounts is expressly forbidden. Members of staff working remotely are required to access Data through the Trust's authorised systems and services.

9.3 Data must not be sent using any systems or services, including but not limited to, cloud platforms and social media providers or any other type system not owned by the Academy, including text messaging.

9.4 Personal Data and Special Category Personal Data must be sent to named Users only. Multi-User posting, sending or transmission, including, but not limited to, email lists, distribution groups, security groups, chat/team-based groups, forums, rooms, and channels is prohibited.

10. Information Security Incident Reporting and Management

10.1 The Academy will have and maintain a register where all Information Security incidents are logged. The form in Appendix 4, can be used as the basis for the Information Security incidents to the Data Protection Officer. = This log as a minimum should include:

i. The nature of the breach;
ii. The number of Information Assets compromised;
iii. How the Information Asset(s) has/have been compromised;
iv. Whether any Special Category Personal Data was compromised;
v. Whether the incident needs to be reported in accordance with the mandatory reporting section of this policy at paragraph 10.3 below.

10.2 Where there has been any breach the Data Protection Officer must be informed immediately, so they can decide if an Information Security Breach has occurred and in order that consideration can be given to reporting the breach to the appropriate authorities;

10.3 If there has been an Information Security Breach but it does not involve the compromise of more than [xx] records, it should be recorded in the Information Security Incident Log;

10.4 Examples of an Information Security Breach include but are not limited to:

i. Password(s) written down or stored, in an accessible, plain text or otherwise visible, manner to persons other than the Authorised User;
ii. Using another person's password;
iii. Divulging of a password;
iv. Making use of Personal Data for personal gain;
v. Accessing Data for personal knowledge;
vi. Attempting to gain access under false pretences;

vii. Unauthorised release of Data;
viii. Knowingly entering inaccurate Data;
ix. Deleting Data prior to the retention period or any other period set out in the Retention, Disposal and Records Management policy expiring;
x. Loss or misuse of Data;
xi. Malicious damage to equipment or Data;
xii. Changing permissions that allows access to, or sharing information (including Data) with, persons not authorised to access the information.
xiii. Unauthorised removal of Data, Academy equipment or equipment used for or in connection with Academy business from Academy premises or another site authorised for the storage of such information or equipment.
xiv. Loss or theft of a Client Device used for or in connection with Academy and/or Trust purposes or any other device belonging to the Academy or Trust.

11. Business Continuity and Disaster Recovery Plans

11.1 Each Academy will develop a managed process to counteract the interruption of Academy business caused by major IT service failure. The Academy will ensure that business continuity and disaster recovery plans are produced for all IT systems and networks which store and/or Process Data.

11.2 The Academy will have procedures in place to maintain essential services in the event of an IT system failure.

12. Monitoring and Review

12.1 This policy will be reviewed every 4 years or earlier if required and may be subject to change.

APPENDIX 1

Personal Devices Statement

The Thinking Schools Academy Trust recognises that its employees will use personal devices to access work information and emails. This must be achieved with appropriate protection of the data that is held within the documents. Therefore, all Employees using personal devices to access Trust documents and emails must adhere to the below requirements.

Personal devices include but not limited to mobile phones, tablets, laptops and PCs.

Personal Devices used for, or in connection with, Academy business must be encrypted and should be kept secure at all times and be protected against loss, damage, misuse or unauthorised access. When not in use, Personal Devices must stored in a secure location, and should never be stored in vehicles, even if locked.

Personal Devices are expressly prohibited from being used to store or externally transmit Special Category Personal Data at any time.

The use of Personal Devices for, or in connection with, other Academy business should be kept to a minimum to reduce the risk of unauthorised access to, or disclosure of, information held by the Academy, and must be updated with the manufacturer's software and other updates regularly when updates become available, and where supported have antivirus software installed and regularly updated.

Subject to the requirement of a Strong Password (see below) for access, if the Employee is the only person with access to the personal device that is being used for Academy work, then documents, apps (including email) and web-based programmes may be left open on the device, whilst the device is locked or logged out.

If a personal device is not solely used by the Employee, then if supported, the device must be configured with separate user accounts for each user, so that the Employee has their own device logon account and others cannot access any documents, apps (including email) and web-based programmes they have open. If the device does not support separate user accounts, or the device is accessible to other people (such as family members, other employees), any documents, apps and web-based programmes must be closed when not in use, and require a password to access the data when re-opened.

Passwords

All Trust data, in particular Personal Data and/or Special Category Personal Data must be kept secure with Strong Password at all times.

When not in use the user account or personal device must require a Strong Password to 'login', 'unlock' or access any information or Data using the device.

The definition of a Strong Password is available in the Trust's Information Security Policy, available from www.tsatrust.org.uk

Lost or Stolen Personal Devices

If a personal device is lost or stolen and has access to Trust information on it, the following actions must be taken.

1. Contact the /Data Protection Officer immediately, who will assess the risk of loss of data.
2. Immediately remotely access the device or application (i.e. Office365) and change the password or
3. Contact the Academy 's IT support team immediately. They will be able to remotely reset passwords for services provided by the Academy.

APPENDIX 2

Minimum security standards for networked client devices

The Thinking Schools Academy Trust Information Security Policy requires all network capable devices that connect to any Trust/Academy network(s), comply with the following minimum security requirements.

The requirements help to protect both the individual client device and other client devices connected to the Trust/Academy network(s).

In the event that a client device cannot demonstrate that it meets the minimum requirements, the device must not be connected to the network, unless written authorisation is provided by the Data Protection Officer..

Software Patch Updates
Client devices must only use operating systems and software applications that are supported by the manufacturer. The client device must be able to demonstrate that all currently available security patches have been installed, and that there is a recurring schedule to notify the user of future updates.

Anti-virus/malware Software
Client devices must be configured to use and run, anti-virus/malware software that utilises real-time scanning and/or scans the entire device at least once a day. The anti-virus/malware software must also be configured to receive software and virus/malware definition updates regularly.

Authentication
Client devices must not provide unauthenticated user access. User authentication must be provided by means of strong passphrases or other secure authentication mechanisms.

Unnecessary Software or Services
Devices must not run any software applications or services for any purposes, other than the agreed intended use.

No Unattended User Sessions
Users must not leave the device unattended when logged in or with an active session open. The user must manually suspend or close the active session when they are not using the device. Due to the nature of teaching and learning, Academy devices/operating systems should be configured to automatically lock after 20 minutes of inactivity, to allow reasonable instruction time.

Firewall Software
Client devices should be configured to use an active client-based firewall. The firewall software should be configured to only allow incoming traffic for the intended use.

Privileged User Accounts
Client devices should support the separation of user account privileges, to reduce the risk of malware spreading across the network. All users should be aware that a standard account should be used for non-administration tasks at all times.

APPENDIX 3

Off-Boarding Checklist

Prior to your final leaving date at the Academy, you must review the following checklist to ensure that all applicable Academy property has been collected. **Both you, the Member of Staff, and your Line Manager must sign this document to verify that all property and information has been returned**

When a Member of Staff leaves the Academy, their user accounts are closed, and the accounts that belong to that person may not be accessible to others, this checklist is designed to help ensure that all information and equipment is available for use after the Member of Staff leaves the Academy. Failure to complete the actions within the checklist, may result in any final payments being withheld until completed.

Human Resources

- ☐ Letter of resignation sent to HR
- ☐ Confirm balance of remaining holiday days with HR (if applicable)
- ☐ Reconcile outstanding expense reimbursements
- ☐ Leaving date provided to Finance, ICT and Facilities for the removal of access rights

Return Equipment

- ☐ Client Devices (i.e. mobile phones, tablets, laptops, computers, other devices)
- ☐ Removable Media
- ☐ ID Card(s)
- ☐ Keys (i.e., classrooms, offices, cars)
- ☐ Access cards, fobs or tokens
- ☐ Academy property (i.e., books, tools, uniforms, etc…)
- ☐ Other

Return/Transfer Information

- ☐ Provide an update on outstanding work and projects to a Line Manager/colleague
- ☐ Transfer internal files, documents to a Line Manager/colleague
- ☐ Transfer internal work-related email messages to a Line Manager/colleague
- ☐ Transfer ownership of Cloud Service documents to a Line Manager/colleague. This will ensure that documents will remain accessible once your Academy account is closed
- ☐ Add an additional owner(s) to any Cloud Service Calendars and/or calendar resources that you own. This will ensure that these resources continue to be accessible once your Academy account is closed
- ☐ Make sure to transfer any important meetings in your Cloud Service Calendar to another owner

- ☐ Add an additional owner(s) to any Cloud Service Groups and Cloud Service Sites that you own. This will ensure that Cloud Service groups, lists and Sites continue to be accessible once your Academy account is closed

Return/Transfer Information (continued)

- ☐ Forward voicemail and telephone password to a Line Manager/colleague
- ☐ Remove any non-work related files or email messages
- ☐ Remove any personal Cloud Service profiles or pages
- ☐ Other

_____

Other

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

I, _____ (print name) have returned all property and information to the Academy and have removed all Academy information from my possession.

_____ _____

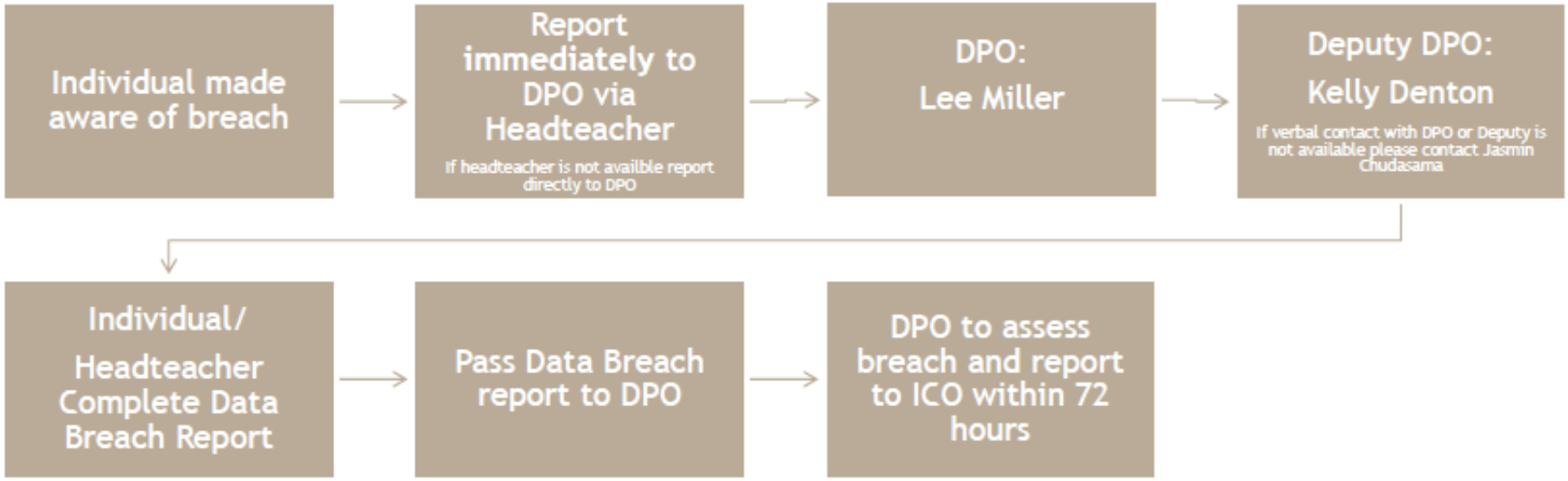
Member of Staff signature **Line Manager signature**

_____ _____

Date Date

APPENDIX 4

Data Breach Flowchart



Reporting Data Breaches

Initial reporting of a Data Breach must be made verbally, **do not report a data breach via email.**

APPENDIX 5

Data Breach Report

Organisation Details

Name of Organisation	**The Thinking schools academy Trust**
Data controller's registration number (if applicable).	ZA147649
DPO	**Mr Lee Miller**
Contact Details	

2. Details of the data protection breach

Set out the details of the breach and ensure that all mandatory (*) fields are completed.

(a) * Please describe the incident in as much detail as possible. (b) * When did the incident happen? (c) * How did the incident happen? (d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this. (e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Details of the Personal Data placed at risk

Set out the details of the personal data placed at risk as a result of the breach and ensure that all mandatory (*) fields are completed.

(a) * What personal data has been placed at risk? Please specify if any financial or special category (sensitive) personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the School / Trust about the incident?

4. Containment and recovery

Set out the details of any steps the School and Trust has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) As the data controller, does the [Trust/Academy/School] provide its staff with training on the requirements of Data Protection Legislation? If so, please provide any extracts relevant to this incident here.0

(b)

(c) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

(d) As the data controller, does the [Trust/Academy/School] provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

(b) YES / NO

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.
(b)Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.
(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.
(d) Has there been any media coverage of the incident? If so, please provide details of this.

This form was completed on behalf of [Trust/Academy/School] by:

Name:……

Role:……..

Date and Time:……..