Thinking Schools Academy Trust

"Transforming Life Chances"

ICT Monitoring Policy

This policy was adopted on	December 2022
The policy is to be reviewed on	May 2026

1. INTRODUCTION

1.1 This Policy provides the guidelines for the monitoring of Information Communications Technology (ICT) equipment and facilities within The Thinking Schools Academy Trust. As whilst ICT is seen as beneficial to all members of the Academy in supporting learning, teaching, research, administration and approved business activities of the Academy, these systems need to be maintained and used appropriately.

1.2 The Academy has a duty of care to all users of its systems and services, including but limited to, staff, students, trainees, volunteers, temporary guests, to provide a safe environment for them to operate within. The Academy's ICT Facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users at the Academy. This could also lead to a breach of the data protection rights of individuals, resulting in harm to that individual and the Academy.

1.3 The Academy has a moral and statutory responsibility to safeguard and promote the welfare of students and takes seriously its responsibility under section 175 of the Education Act 2002 to safeguard and promote the welfare of children; and to work together with other agencies to ensure adequate arrangements within the Academy to identify, assess, and support those children who are suffering harm.

1.4 The Academy has a statutory duty with regard to the use of the ICT facilities for writing, publishing or circulation any material that could be seen by any one or more of the persons under the Terrorism Act 2006, and a duty to alert and report any such material that may have been created or made available.

1.5 The Academy has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism under the PREVENT element of the Counter-Terrorism and Security Act (2015) and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material.

Note: The UK government has defined extremism as: 'vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs.

1.6 When monitoring the ICT facilities, an important to be aware of the distinction made between:

- Intercepting information in transit - email messages being sent, for example, or watching the web pages visited - here the relevant law is found in the Regulation of Investigatory Powers Act 200 0 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR)
- Examination of material stored on a computer - the law applicable may depend on variables such as who owns the computer, what material is being examined, and how the material is examined. However, the Human Rights Act 1998 and the General Data Protection Regulation provide an over - arching framework to protect the individual's right to privacy

1.7 Under the Regulation of Investigatory Powers Act 2000, unlawful interception of communications on the Academy computer network may lead to criminal proceedings against an individual operating without the Academy's authority; unlawful interception may also lead to civil action against the institution where the institution authorised the interception. The RIPA and LBPR do, however, allow for legitimate interceptions of communications by organisations on their private computer and telecommunications networks, through 'lawful authority'.

1.8 The purpose of this policy is to outline the types of monitoring that may be performed, and to inform users of the extent that network activities; interactions, services, systems and communications methods may be monitored, what personnel may be authorised to perform monitoring functions and the ethics, procedures and safeguards authorised personnel must employ prior to, during and after performing monitoring functions.

2. Definitions

1.1. 2.1 *"Academy"* means Thinking Schools Academy Trust. This Policy applies to all Academies of The Thinking Schools Academy Trust and all Nurseries and Pre Schools of Little Thinkers Nursery & Pre School, a subsidiary of The Thinking Schools Academy Trust. When 'Academy' is used within this policy it applies to Nursery and Pre School settings. When 'Headteacher/Principal' is used with this policy it applies to Nursery Managers. When 'The Thinking Schools Academy Trust' is used within this policy is applies to Little Thinkers Nursery and Pre School.

2.2 *"ICT Facilities"* means all IT devices, facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, personal organisers, music players, software, websites, web applications or services and any device, system or service which may become available in the future which is provided as part of the ICT service.

2.3 *"Users"* means directors, committee members, Regional Governing Bodies, Academy Advisory Boards, staff, students, trainees, volunteers, temporary guests, and all other persons authorised by the Academy to use the ICT Facilities.

2.4 *"Personal use"* means any use or activity not directly related to the users' employment, study or purpose.

2.4 *"Authorised Personnel"* means employee(s) authorised by the Academy to perform systems administration and/or monitoring of the ICT Facilities.

2.5 *"Operational Monitoring"* means the monitoring of ICT Facilities in relation to the maintenance, operation or provision of the equipment, system or service.

2.6 *"Policy Monitoring"* means the monitoring of specific person(s) use of the ICT Facilities to ensure compliance with the policies, procedures, and regulations of the Academy, and relevant legislation.

2.7 *"Materials"* means files and data created using the ICT facilities including but not limited to documents, photographs, audio, video, printed output, web pages, social networking sites, bulletin boards and newsgroups forums and blogs.

3. Policy Statement

3.1 To protect our Users and ICT Facilities, the Academy reserves the right to monitor the use of the ICT Facilities, and access any information stored, or connected to, our ICT Facilities, but will do so in ways that are consistent with relevant legislation and guidance provided by the office of the UK Information Commissioner.

3.2 The Academy requires that all Users making use of the Academy's ICT Facilities are aware that monitoring an activity logging takes place, and that monitoring or content inspection of an individual's activity may occur. Through LBPR, the Academy is permitted to intercept and record information which can be associated with an individual's communications via the ICT Facilities services (whether, made for purposes associated with the Academy's business or activities or otherwise). This may only be done where

Academy's has made reasonable efforts to inform potential users that such interceptions may be made. As such, the Academy, may intercept and record information:

- Comply with our regulatory and statutory obligations;
- Preventing and detecting crime;
- Assess compliance with the Academy's policies including, but not limited to, Acceptable Use, Data Protection, System Administration, and Information Security policies, and the security policies the Academy is required to adhere to through interconnections with third-parties;
- Provision and management of the systems and services;
- Capacity planning for Network expansion and Service upgrades;
- Fault investigations Incident handling;
- Prevent and detect unauthorised access, use or other threats to the ICT Facilities;
- Safety and security of our Users, resources and facilities;
- Evaluate staff training; and
- Monitor system performance.

3.3 When authorised, personnel may monitor and analyse all ICT Facilities including but not limited to, network services, systems, all types of data and materials

(including file systems), applications, cloud services and data communications facilities and any or all other equipment or devices connected to a system or service owned or operated by or on behalf of the Academy under an agreement or contract. Monitoring will include active attacks by Authorised Personnel to test or verify the security of the ICT facilities.

3.4 The Academy may monitor its systems to ensure that they are performing properly, herein known as Operational Monitoring. Based on standard practice, the Academy will normally only aggregate anonymous data that does not identify individuals or the contents of their communications. Information Systems, for example, records the number of email messages passing through its servers each day, and the time it takes to deliver messages, to help with capacity planning. This type of monitoring does not fall within the RIPA, as it does not involve interception, and by virtue of not identifying individuals, it does not trigger laws relating to personal privacy.

3.5 Through Operational Monitoring the Academy may intercept certain communications where the interception is by Authorised Personnel for purposes connected with the provision or operation of a service, which is permitted through a general exemption in the RIPA. This may allow the Authorised Personnel to identify individuals or the source and or destination of the data, but only for the purpose of providing the system or service.

3.6 All other activities falling under the exemptions within the LBPR will constitute monitoring for policy or (legal) compliance, herein known as 'Policy Monitoring'. Each individual act of monitoring for this purpose must be specifically authorised and documented using the form in Appendix 1.

3.7 Persons that are permitted to undertake Operations Monitoring and/or Policy Monitoring are required by RIPA LBPR to be properly authorised by the Academy. Authorised Personnel will be identified through their job description and as required by written authorisation (see section 4.1).

3.8 Access to stored data, information or other materials must be authorised through the procedures listed in the Academy's ICT Acceptable Use policy and is beyond the scope of this policy.

Authorisation of Monitoring

4.1 The Academy grants the Head of IT & Capital Strategy, the authority to authorise personnel from the Information Technology Systems department (herein known as "Authorised Personnel") to perform Operational and/or Policy Monitoring, that conform to this Policy and all relevant UK laws and regulations.

4.2 Policy Monitoring may only be carried out by Authorised Personnel with additional written authorisation using the form in Appendix 1. The monitoring request must be authorised by Academy representatives as defined in the decision tree in Appendix 2. The written authorisation covers an individual act of monitoring and only for the purposes and scope indicated on the authorisation form.

4.2 Only Authorised Personnel are permitted to monitor and analyse the ICT Facilities within scope authorised. All other monitoring or analysis is expressly prohibited and any User in breach of this policy will be subject to the disciplinary procedures, in addition to potential prosecution under the Regulation of Investigatory Powers Act 2000.

4.3 Authorised Personnel may undertake Operation monitoring through their role within the Information Technology Systems department, as required. Authorised Personnel carrying out monitoring for operational reasons are required to ensure that any monitoring is limited to the original purpose. If, at any stage, monitoring or access to stored material is required to investigate matters of policy (or legal) compliance the appropriate authorisation must be obtained.

4.4 Authorised Personnel must execute their duties in accordance with the Academy's Data Protection and System Administration Policies, in particular authorised personnel must:

- Respect the privacy of others;
- Not use or disclose information realised in the process of administering or monitoring the ICT facilities for purposes other than those for which the process was approved;
- Safeguard information collected in the administration or monitoring process; and
- Destroy information collected in the administration or monitoring process when it is no longer required.

4.5 Authorised Personnel shall not access, read, listen to or otherwise view the contents of any data, files or records of any other person or system, unless required to access the contents in order to perform the responsibilities as set forth within Academy policies and the responsibilities of their terms and conditions of employment.

4.6 If, in the course of performing their responsibilities, Authorised Personnel encounters evidence that an individual is not using the ICT Facilities in a lawful and ethical manner as outlined in the Academy policies, and/or is breaching the confidentiality of ICT Facilities, any potential misuse identified must be reported to the Head of IT & Capital Strategy or Data Protection Officer, for advice on the preservation of evidence should be sought before proceeding. Any misuse may result in disciplinary or legal action.

5. Monitoring & Review

5.1 This policy will be reviewed every 4 years and may be subject to change.

Appendix 1 – Policy Monitoring Request Form

Monitoring Request Form		
Reason Please include why the monitoring is in the interests of the Academy, for example if any internal disciplinary offence or suspected or alleged civil or criminal act which may have been committed		
Scope (e.g. systems/persons)		
Names and Usernames List all Authorised Personnel and their usernames that will perform the monitoring	Name	
	Username	
	Name	
	Username	
	Name	
	Username	
Period Access is to be granted for (in days)		
Access is for investigation	Yes ☐ No ☐	
Access Special Category Data	Yes ☐ No ☐	
Requested By	Name	

	Signature	
	Position	
	Date	

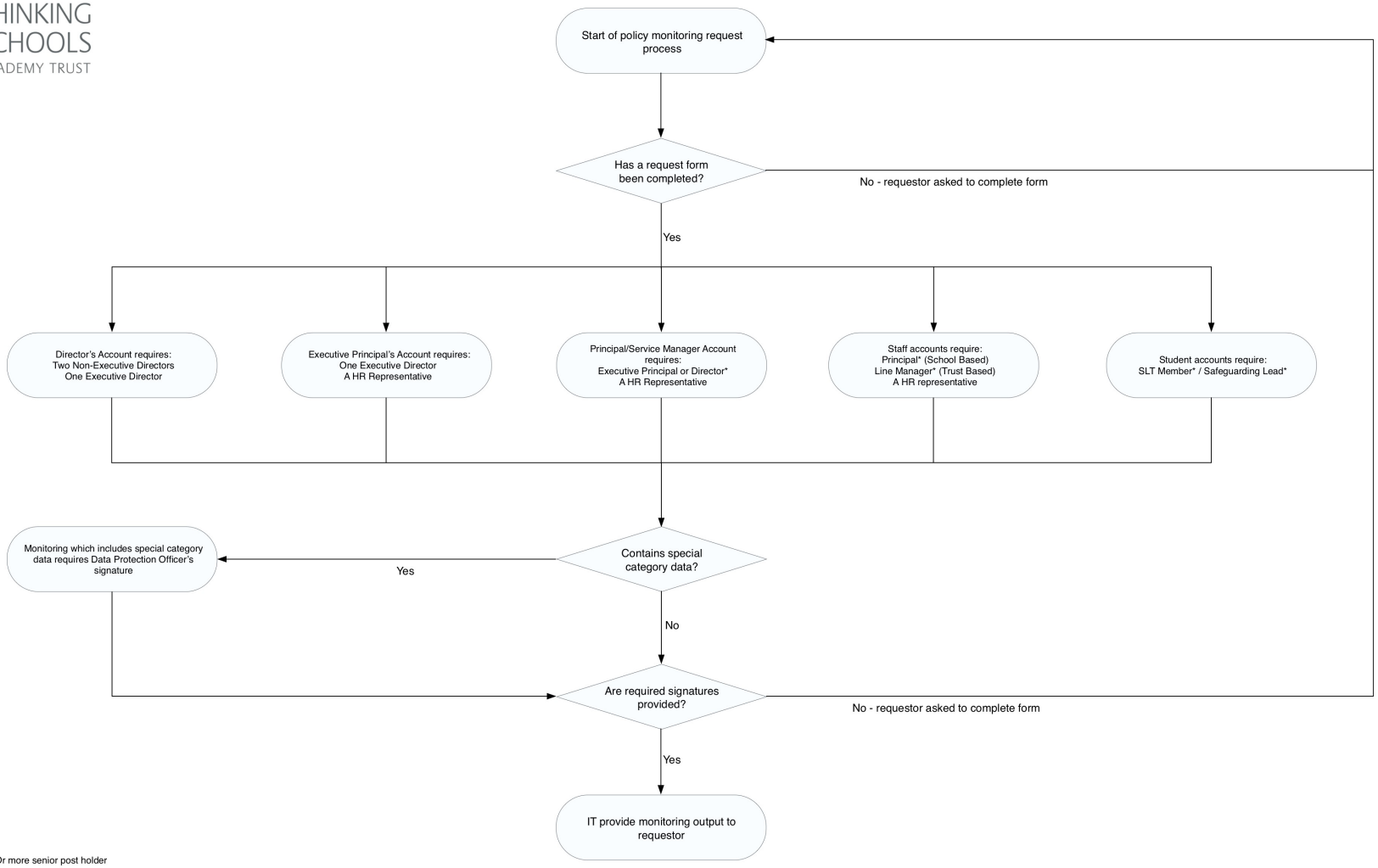
Please turn over

Monitoring Request Form (continued)		
Authorisation 1	Name	
	Signature	
	Position	
	Date	
Authorisation 2	Name	
	Signature	
	Position	
	Date	
Authorisation 3 (if required)	Name	
	Signature	
	Position	
	Date	
Data Protection Officer (If access request includes the need to access Special Category Personal Data the Data Protection Officer (or nominated delegate in absence) **MUST** authorise the request)	Name	
	Signature	
	Position	Data Protection Officer
	Date	

Appendix 1 – Policy Monitoring Authorisation Decision Tree

THINKING SCHOOLS ACADEMY TRUST

Policy Monitoring Request Decision Tree



* Or more senior post holder