Thinking Schools Academy Trust

"Transforming Life Chances"

ICT Systems Administration Policy

This policy was adopted on	May 2018
The policy is to be reviewed on	September 2022

1. INTRODUCTION

1.1 The widespread use and ownership of IT devices, systems and services requires that Trust/Academies take steps to ensure that persons with responsibility to administer and control those systems do so in a manner that is controlled, secure and respectful.

1.2 This policy ensures that potential issues involving the use of administrator, root and any, or all, accounts that provide administration of devices, systems or services be clearly identified and addressed, ensuring these accounts can continue to be utilised, balancing security with accessibility.

2. Definitions

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

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 *"Least Privilege"* means providing a user account only those privileges which are essential to that user's work.

2.6 *"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 The creation and operation of ICT Facilities require personnel to configure, manage, administer, and monitor computer and other electronic communications, hardware and software. System Administrators who configure these systems and services and monitor the performance of these systems are responsible for:

- Setting up accounts and groups for individuals to access information and services;
- Helping resolve problems with usernames and passwords;
- Researching and resolving problems relating to the correct operation of the ICT Facilities;
- Configuring systems and services to the needs of the organisation;
- Monitoring the performance of systems and services;
- Taking corrective action to improve performance;
- Implementing corrections and upgrades to provide new features and enhancements; and
- Identifying internal and external risks to the security, confidentiality, and integrity of information.

3.2 All ICT Facilities owned and/or leased by the Academy are the property of the Academy. The Academy will designate selected staff and agents as System Administrators and provide system authentication rights applicable to his or her terms and conditions of employment. The Academy retains the right, at any time, without notice, to withdraw with immediate effect any authentication rights set forth within this paragraph as deemed necessary by the Academy, Governing Body or other recognised legal authority.

3.3 System Administrators with the position of second line (2nd) engineer or higher may be granted access to Enterprise, Domain and Root authentication rights, as necessary, to undertake the installation and administration of system wide changes. Systems Administrators within positions below second line (2nd) engineer will not usually be granted Enterprise, Domain and Root authentication rights without prior authorisation from the relevant Head of IT, Data Protection Officer, Headteacher/Principal or Director.

3.4 System Administrators are not permitted to use Enterprise, Domain and Root authentication rights, or any other permissive access permissions or role for everyday use, and must follow the principles of Least Privilege at all times. Administration permission, access rights and accounts must only be used to perform a specific task or function for which the permission or access was granted.

3.5 All staff within the IT support teams and/or agents on behalf of the Academy will be delegated authentication rights and permissions for the specific ICT Facilities, as deemed necessary by the Academy in order to perform the responsibilities of his or her post as defined within the terms and conditions of employment, on the basis of Least Privilege.

4. Account Access and Monitoring

4.1 As set forth in the ICT Acceptable Use and ICT Monitoring policies, The Academy may monitor the usage of any or all IT Facilitates and has access to reports on any internet sites that have been visited. This is irrespective of whether it is for Academy or personal use. System Administrators must ensure that all monitoring and account access requests follows the procedures defined within the ICT Acceptable Use and ICT Monitoring policies.

4.2 Personnel authorised to monitor IT systems and services 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.

4.3 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.

4.4 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 & Operations 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.

7. SYSTEM ADMINISTRATOR AUTHORISARION FORM

I have read and understand the above information about appropriate use of System Administrator permissions and/or accounts and I understand that this form will be kept on file at the Academy. I will be solely responsible for ensuring that permissions and accounts provided to me will be used appropriately and correctly as outlined in this document.

APPROVAL		
Staff Member I have read the Terms & Conditions governing the use of System Administration permissions or Accounts	Name	
	Signature	
	Date	
Head of IT & Operations	Name	
	Signature	
	Date	