Thinking Schools Academy Trust
"Transforming Life Chances"

Student BYOD Policy

This policy was adopted on	November 2025
The policy is to be reviewed on	November 2027

1. Introduction

1.1 This Policy provides the guidelines of acceptable use of personal devices by students within The Thinking Schools Academy Trust. Technology has formed an integral part of modern life and continues to change how people communicate and access information. The Thinking Schools Academy Trust recognises the impact technology can have to support teaching and learning, especially independent learning through digital resources and research.

1.2 The Student Bring Your Own Device (BYOD) Use Policy aims to promote safe and appropriate practice through establishing clear guidelines for the use of personal devices to enhance learning.

1.3 This policy applies to all students who wish to use a personal device within the Academy for education purposes. All students who intend to access the BYOD service must ensure that they have read this Policy and obtained prior approval from the Academy before attempting to connect to the BYOD service.

1.4 The Student BYOD Policy should be read in conjunction with the Trust's ICT Acceptable Use, ICT Monitoring and Mobile Device Policies.

2. Definitions

2.1 The *"Trust"* means Thinking Schools Academy Trust and all its Academies.

2.2 The *"Academy"* means a school within the Thinking Schools Academy Trust.

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

2.4 *"Personal Device"* means a Client Device not directly owned by the Trust.

2.5 *"BYOD"* means bring your own device, which specifically refers to the use of a personal device within the Academy for educational purposes.

2.6 *"BYOD Service"* means the wireless network provided to personal devices in order to access the Internet within the Academy.

2.7 *"ICT Facilities"* means all devices, facilities, systems and services including, but not limited to, network infrastructure, ICT Devices, 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.

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

2.9 *"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.

2.10 "*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.

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

3. Policy Statement

3.1 The Academy's BYOD service should only be used to support learning and must not be used for any personal use or other activities unless expressly authorised by the Academy.

3.2 Access to the Academy's BYOD service is at the discretion of the Academy and is not an automatic right.

3.3 Prior to attempting to connect to the Academy's BYOD service, students must sign and return a copy of the Learner Acceptable Use Policy Agreement, which can be found in the appendix of the Trust's ICT Acceptable Use Policy.

3.4 Up to a maximum of one personal device per student may be connected to the Academy's BYOD service at any one time.

3.5 Students connecting a personal device to the BYOD service must authenticate using their own username and strong password. Under no circumstances should students share their credentials to assist other personal devices accessing the BYOD service.

3.6 The BYOD service provides access to the Internet only and any cloud hosted services used by the Academy. No internal services, such as printing or accessing documents saved to the Academy's internal servers are supported and students must not attempt to connect to any internal ICT Facilities or systems and services that are not accessible on the Internet.

3.7 Each personal device accessing the BYOD service will be issued with an IP address. Students are not permitted to edit, adjust, disguise, or share the IP address that their device has been allocated.

3.8 The use of a personal device within the Academy must not be used in such a way that it causes distraction to staff, students or disrupt lessons.

3.9 The use of cellular data (e.g. GPRS, EDGE, 3G, 4G, etc) to access the Internet within the Academy is strictly prohibited. All personal devices accessing the Internet within the Academy must only do so through the BYOD service.

3.10 The use of cameras or microphones on personal devices within the Academy is prohibited unless approved by a member of staff. In circumstances where approval for

such functions to be used on Academy premises is obtained they must be used in accordance with the Trust's Mobile Device Policy.

3.11 Users accessing the Academy's BYOD service should be aware that the Academy cannot guarantee security, and users should therefore engage in safe computing practices by adhering to the Trust's ICT Policies at all times.

3.12 Personal devices must only be used within the Academy when permitted by staff. The use of personal devices in classrooms is at the teacher's discretion.

3.13 Students must not make any attempts to circumvent the Academy's BYOD service or other security measures enforced to protect the Trust's ICT Facilities.

3.14 Whilst within the Academy all personal devices must be set to operate in silent mode.

3.15 Personal devices should be fully charged before being brought into the Academy and connected to the BYOD service.

3.16 It is at the discretion of the Academy to provide charging facilities for personal devices, where charging facilities are provided these must only be used once the equipment has been PAT tested. Personal devices must only be charged in the location(s) identified by the Academy and without cables trailing across the floor to prevent trip hazards.

3.17 Where charging facilities are provided, the Academy will arrange for equipment to be PAT tested by a certified third-party.

3.18 The Academy is unable to provide licenses to personal devices for operating systems or software applications.

3.19 All personal devices that access the BYOD service must be capable of supporting regular software updates, security updates and anti-virus updates and personal devices must be configured to perform such updates.

3.20 Under the Trust's ICT Monitoring Policy, the Academy reserves the right to check the security posture of personal devices prior to these being connected to the BYOD service. This can be achieved through both manual inspection and automated processes.

4. Unacceptable Use

4.1 The Academy reserves the right to disconnect a personal device from the BYOD service if the user does not comply with the Trust or Academy policies, including but not limited to this policy, the ICT Acceptable Use Policy and the Academy Behaviour Policy.

5. Equal Opportunities

5.1 To prevent students without access to their own device the Academy will provide devices to support curriculum activities, when access to technology is required. Where possible the Academy will also provide access to devices to support independent learning outside of the lessons.

6. Monitoring

6.1 The Trust may monitor the usage of personal devices whilst used within the Academy and has access to reports on any Internet sites that have been visited. Such monitoring will be performed in compliance with this policy and the Trust's ICT Monitoring policy.

6.2 The Trust will not monitor content or applications installed on personal devices, but students may be asked to delete inappropriate content or applications installed on their device if staff become aware that this is being accessed or shared within the Academy. Failure to remove such content will result in access to the BYOD service being revoked.

7 ICT Support

7.1 The Trust cannot provide support for personal devices, but will endeavour to provide guidance for connecting to the BYOD service where possible.

7.2 The Trust accepts no liability for any loss of data stored on personal devices whilst using the BYOD service, and in such instances the Trust is unable to assist with any data recovery. Additionally, the Trust accepts no responsibility for any device malfunctions as a result of changes made to personal devices to connect to the BYOD service.

7.3 Users are responsible for the maintenance of personal devices. The Trust is not responsible for the maintenance of any personal devices, including but not limited to the charging of devices, installation of software or operating system updates, or hardware faults.

7.4 Any costs incurred while using a personal device are not chargeable against the Trust.

8. Accidental Damage, Loss, Theft and Insurance

8.1 The Trust accepts no responsibility or liability for any damage, loss or theft of any personal devices, whilst onsite or during other activities organised by the Academy.

8.2 It is recommended that personal devices have insurance to provide cover for accidental damage, loss and theft. It is not the responsibility of the Trust to provide insurance for personal devices.

8.3 Whereby a personal device is damaged or stolen within the Academy, the Academy will provide support to investigate the incident. If a device is damaged or stolen while on the Academy premises, it should be reported to a member of staff immediately.

9. Monitoring & Review

9.1 This policy will be reviewed every 2 years and may be subject to change.