Thurlstone Primary School
BYOD (Bring Your Own Device) Policy

Introduction

Thurlstone Primary School recognises the benefits that can be achieved by allowing staff to use their own devices when working, whether that is at home, on site or while travelling. This includes laptops, smart phones, tablets and any other connected device which connects to school systems. The practice is commonly known as 'bring your own device' or BYOD. The school is committed to supporting staff in this practice and ensuring as few technical restrictions as responsibility possible are imposed on accessing school provided services on BYDB, whilst maintaining data security and GDPR compliance.

The use of such devices to create and process academy information and data create issues that need to be addressed, particularly in the area of information security.

The school must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

This policy covers users own device use as detailed below, for which permission must be sought prior to use/access, using appendix 1.

- Any device which connects to the school Wi-Fi to access either the network or the Internet.
- Any device which is connected physically to a network point or switch within the school, to access either the network or the Internet.
- Any device which is able to receive mail from the user's school mailbox, other than webmail.
- Any device which shares files with the school network through the use of a VPN or cloud-based storage applications (e.g. Dropbox, Google Drive), whether the account used was provided by the school or not.

Information Security Policies

All relevant policies still apply to staff using BYOD. Staff should note, in particular, the school's Acceptable Use Policy.

The Responsibilities of Staff Members

Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of the school information (as well as their own information).
- Invoke the relevant security features.
- Maintain the device themselves ensuring it is regularly patched and upgraded.
- Ensure that the device is not used for any purpose that would be at odds with aims and ethos of the school and its policies.

STAFF SHOULD NOT USE JAILBROKEN DEVICES

Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data.
- Keep information confidential where appropriate
- Maintain the integrity of data and information, including that on site.
- Take responsibility for any software they download onto their device.
- Ensure that work done on a BYOD is transferred or copied onto the academies computer systems.

The school understands that some users will require different levels of settings for their devices depending on what the resource is used for and what it is.

IT IS RECOMMENDED THAT WHEN USING A PERSONAL DEVICE, STAFF USE TWO FACTOR AUTHENTICATION (TWO LEVELS OF SECURITY TO ACCESS INFORMATION. EG. 1 SECURITY LEVEL - ACCESS PHONE, 2 SECURITY LEVEL - ACCESS SCHOOL DATA

Mobile phones, smart phones, smart watches and "tablet" devices

- Configure your device to enable you to remote-wipe it should it become lost (E.g. "Find my iPhone" app for Apple devices).
- If your device is second hand, restore to factory settings before using it for the first time.
- Only download applications ('apps') or other software from reputable sources. In relation to Android devices, staff should ensure that no apps that contain malicious software are downloaded.

IF YOU SELL YOUR DEVICE OR GIFT IT TO SOMEONE ELSE, IT SHOULD BE PUT BACK TO FACTORY SETTINGS

All type of devices

- Set and use a passcode (e.g. pin number or password) to access your device. Whenever possible, use a strong passcode. Do not share the passcode with anyone else. We recommend the use of biometric or facial recognition authorisation over passcodes where available.
- Set your device to lock automatically when the device is inactive for more than a few minutes.
- Take appropriate physical security measures. Do not leave your device unattended.
- Keep your software up to date and ensure that your device still is able to updates its security settings.
- Make arrangements to back up your documents.
- Keep master copies of work documents on any school servers.
- If other members of your household use your device, ensure they cannot access school information, for example, with an additional account passcode. (Our preference is for you to not share the device with others.)
- Regularly review the information on your device. Delete copies from your device when no longer needed.
- When you stop using your device (for example because you have replaced it) and when you leave the school's employment, securely delete all academy information on your device.
- Ensure that no school information is left on any personal device indefinitely and only kept while needed.
- Encrypt the device (to prevent access even if someone extracts the storage chips or disks and houses them in another device).
- Report any data breaches in accordance with GDPR policies.
- If you install a CCTV monitoring app on your personal device, you must refer to the CCTV policy regarding the protocols of using this app.
- Any staff using their personal device to update the school's Twitter and/or Facebook account, must have the authorisation of the headteacher.
- Configure your device to maximise its security. For example, each new technology brings new enhanced security features. Take time to study and discover how to use these and decide which of them are relevant to you. Seek help from the IT support team if necessary.
- Use anti-virus software and keep it up to date if required for your device.
- If staff are using their personal device to communicate with colleagues via message apps e.g. WhatsApp, then they must ensure they adhere to the school's social media or code of conduct policy.

Using wireless networks outside the academy

- Control your device's connections by disabling automatic connections to open, unsecured Wi-Fi networks and make risk conscious decisions before connecting.

Monitoring and Access

The school will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or the wireless networks or both.
- Prevent access to a particular system.
- Take all necessary and appropriate steps to retrieve information owned by the school.

Data Protection, GDPR and BYOD

The school must process 'personal data' i.e. data about identifiable living individuals in accordance with GDPR. Sensitive personal data is information that relates to race/ethnic origin, religious beliefs, health details or any information, which can identify an individual. This category of information should be handled with a higher degree of protection at all times.

The school recognizes that there are inherit risks in using BYOD to hold and process personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data and permission to use a device for this purpose must be sought.

A breach of GDPR can lead to the school being fined up to €20 million. Any member of staff found to have deliberately breached the directive may be subject to disciplinary measures, having access to school systems withdrawn, or even criminal prosecution. Staff who report non-compliance of the BYOD procedures, will be protected under the schools whistleblowing policy.

Covid 19

Due to Covid 19, methods of engaging with pupils and parents have had to change. During lockdown periods, members of staff have been asked to phone pupils to check on their welfare and mental wellbeing. In most instances, this should be on a school device.

However, there are occasions when staff may be asked to use their personal phones to make calls. Here is a list of protocols in relation to using personal devices.

- Staff should use the feature on their phone, to ensure that they do not reveal their personal number.
- The school should communicate with parents prior to the phone call that the school is using a new method of communication.
- When phoning pupils, the speakerphone on the device should be enabled, so parents can listen to the conversation.
- When making calls offsite, this should be done in a private room with no other individuals present.
- The school should issue a template, so staff can record each call made on their device and any notes that need to be circulated to the DSL and headteacher.
- If the school has specific telephone systems that allows phone calls to be made through the central school phone system. It is important that schools speak to their phone supplier about this.
- If the school provides staff with a school owned Ipad, it could look at enabling the function where calls can be made over the staff's home wifi.

It is important that staff are reimbursed for calls made via their personal phone. The headteacher should work with the SBM on methods of payment.

Finally, if staff do not feel comfortable using their own personal device, every opportunity should be made for them to make calls on a school device.

Responsibility and Damage

While school IT staff will always endeavour to assist colleagues wherever possible, the school cannot take responsibility for supporting devices it does not provide.

Staff, who use their personal devices for school purposes do so at their own risk. Staff are expected to act responsibly with regards to their own device, keeping it up to date via regular anti-virus and operating system updates and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Thurlstone Primary School is in no way responsible for:

- Personal devices that are broken whilst at school or during school-sponsored activities.
- Personal devices that are lost or stolen at school or during school-sponsored activities in terms of replacement, but the school would need to be informed immediately about any data held on the device.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
- Staff should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal device in the event of loss/damage to the device.
- Staff downloading malicious software that could compromise their personal device.

Thurlstone Primary School

BYOD (Bring Your Own Device) Policy - Appendix 1

BYOD Request Form

Date: _____

Staff Member Name: _____

☐ Job Title: _____

☐ Please now provide details of the device you wish to use.

Manufacturer: _____

☐ Device (e.g. iPad, Smart Phone, Laptop): _____

Model e.g. Iphone 9 etc: _____

Please tick the appropriate boxes for this device.

I wish to connect this device to the academy network either by wire or Wi-Fi to only access the Internet.

I wish to use this device to use an application or program to access my school email account.

I wish to use this device for work purposes in line with my job, which will involve storing and processing information, some of which will be personal information about adults or children.

Please now read the statements below.

I have read and understand the BYOD policy.
I understand the settings needed to use my device and these settings are in place.
I understand that the device is used at my own risk.
I understand that any issues regarding a data protection breech on a BYOD must be reported to SMT immediately, no matter how small.

Approved by Headteacher: _____