Bring Your Own Device Policy

Version: 2.0

Date: 23/09/2024

thesovereigntrust.uk

The Sovereign Trust is a Multi Academy Trust registered in England No. 09666511. Registered Office: Manor Academy Sale, Manor Avenue, Sale M33 5JX

Document Control

Title	Bring Your Own Device Policy
Supersedes	1.1
Owner	CEO
Circulation/Distribution	All
Review Period	Annually

The Sovereign Trust is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with Trust's policy review schedule.

A current version of this document is available to all interested parties [The Sovereign Trust Website]

Signature: P. Eckley *Date:23/09/2024*

Version History

Next Review Date	23/09/2025			
Version	Date	Amendments	Author	Status
1.0	17/10/2022	Initial issue	CEO	Approved
1.1	28/11/2023	No changes	CEO	Approved
2.0	23/09/2025	Included some additional security procedures and a password policy.	CEO	Approved

The Sovereign Trust ("Trust") has implemented this policy to protect the Trust and all parties when using ICT and media devices. Staff are able to use devices at work and outside of work for work-related activities provided the terms of this policy are met. The Trust reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the Trust's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. This policy is not designed to offer protection for the device itself. The safety of the user's own device is the responsibility of the user.

Mobile devices within the context of this policy include any mobile phone, tablet, laptop, MP3/iPod, or other device capable of connecting with the Internet or mobile networks or taking images or sound recordings.

This guidance is in addition to the Trust's Acceptable Use Policy.

Ensuring the Safe and Appropriate Use of Mobile Devices

The Trust allows staff to bring in mobile phones for their own personal use. However, they must be kept out of toilets, changing rooms or play areas, and if in classrooms or other teaching spaces, they are not to be accessed in the presence of students.

If staff fail to follow this guidance, disciplinary action will be taken. If staff need to make an emergency call, they must do so in a staff room or office. Staff must ensure that the device does not contain inappropriate or illegal content.

There may be particular occasions when staff might want to keep their phones with them for urgent and personal reasons. If this arises, staff will discuss the need with the Executive Headteacher/Head of Schools, and an agreement will be reached that does not compromise the Trust's safeguarding for an agreed period of time.

All staff must be responsible for their mobile phones and electronic devices. They must keep their telephone numbers, login details, passwords, passcodes, PIN details, and personal email addresses private and secure.

All concerns relating to communications, contact, and usage must be raised with the Headteacher immediately.

Acceptable Use

The Trust embraces the use of new and mobile technologies and acknowledges that they are valuable resources with an educational purpose in the classroom.

However, staff who access the Trust's systems and networks are likely to use personal data, and they must abide by the terms of the Data Protection Act 2018 when doing so (including ensuring adequate security of that personal information).

All employees must agree to the following terms and conditions in order to be able to connect their devices to the company network:

- All staff who wish to use their own devices to access the Trust’s network must sign and return the statement at the conclusion of this policy.
- When in Trust, staff should connect their device via the Trust’s wireless network for security.
- When out of Trust, staff should access work systems on their mobile device using Splashtop or Chrome.
- All internet access via the network is logged, and as set out in the Acceptable Use Policy, employees are blocked from accessing certain websites whilst connected to the Trust network.
- The use of a camera, microphone, and/or video capabilities is prohibited while in Trust unless the CEO has approved it. If approved, pictures, videos, or sound recordings can only be used for Trust purposes and cannot be posted or uploaded to any website or system outside the Trust network.
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission.
- WhatsApp must not be used on personal devices for Trust-related communication. Members of staff are able to use WhatsApp on their own devices for personal communication. However, staff should not communicate internally with other staff members for Trust business using their personal WhatsApp accounts or sharing Trust-related information, which could include categories of personal data.

Non-acceptable Use

- Any apps or software downloaded onto the user’s device while using the Trust’s own network are done at the user’s risk and not with the Trust's approval.
- Devices may not be used at any time to:
  - Store or transmit illicit materials;
  - Store or transmit proprietary information belonging to the Trust;
  - Harass others;
  - Act in any way against the Trust’s Acceptable Use Policy and other safeguarding and data-related policies.
- The Trust does not provide technical support on the user’s own devices.
- Storing Trust data on personal devices is not allowed. This includes forwarding Trust emails to your personal email address.

Devices and Support

- Smartphones, including iPhones and Android phones, are allowed provided their operating system is no more than two versions older than the current release version and they are still receiving security updates from the manufacturer.
- Tablets, including iPad and Android, are allowed provided their operating system is no more than two versions older than the current release version and they are still receiving security updates from the manufacturer.
- Before they can access the network, devices must be presented to IT for proper job provisioning and configuration of standard apps such as browsers, office productivity software, and security tools.
- To prevent unauthorised access, devices must be password/pin/fingerprint protected using their features, and a strong password is required to access the Trust network.

Security Requirements

- When using personal data, it is the user's responsibility to ensure data security on their device. This includes preventing data theft and loss (for example, through password protection and cloud backup), keeping information confidential (for example, by ensuring access to emails or sensitive information is password protected), and maintaining that information.
- The Trust does not accept responsibility for any loss or damage to the user's device when used on the Trust's premises. It is up to the user to ensure they have protection (such as insurance) for their own device.
- Staff are prevented from installing email apps which allow direct access to the Trust's emails without use of a login/password.
- If information is particularly sensitive, then users should ensure that the data is either appropriately secured or deleted from the device (including any local copies that may have been stored on the device).
- In the event of any loss or theft of personal data/device, this must be reported immediately as a data breach in accordance with the School's Data Breach policy.
- The Trust may require access to a device when investigating policy breaches (for example, to investigate cyberbullying).
- Staff are not permitted to share access details to the Trust's network or Wi-Fi password with anyone else.
- Protect the device with a PIN or strong password (or use facial or fingerprint recognition if available) and always keep that PIN or password secure. If the confidentiality of a PIN number or password is compromised, you must change it immediately.
- Ensure that access to the device is denied if an incorrect PIN or password is input too many times and that the device automatically locks if it is inactive for a period of time.
- Maintain the device's original operating and security system and settings and keep it current with security patches and updates.
- Do Not use private email, text messaging, messaging apps or any other instant messaging or chat programs or services installed on the device to discuss work-related matters or for any other business

purposes – you must always use the Trust's official correspondence channels for work-related business and you must

Disclaimer

- The Trust will not monitor the content of the user's own device but will monitor any traffic over the Trust system to prevent threats to the Trust's network.
- The Trust reserves the right to disconnect devices or disable services without notification.
- Employees are expected to use their devices ethically at all times and adhere to the Trust's policy, as outlined above.
- The employee is personally liable for all costs associated with their device.
- The Trust reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

I confirm that I have read, understood and will comply with the terms of the Bring Your Own Device Policy when using my mobile device to access the Trust network.

Signed: ……………………………………………………………………………………

Date: ………………………………………………………………………………………..

Print Name: ……………………………………………………………………………….