PolyMAT

Bring Your Own Device Policy

Reviewed: November 2023

Approved: December 2023

Revision due: December 2024

Bring Your Own Device Policy

The Trust has implemented this policy to protect all parties when using ICT and media devices. Staff (and selected students) are able to bring and use personal devices in or out of Trust premises 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 includes any mobile phone (staff only), tablet, laptop or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

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

Acceptable Use

The Trust embrace the use of new and mobile technologies and acknowledge they can be a valuable resource in the classroom having educational purpose.

However, by accessing the Trust's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing so (including ensuring adequate security of that personal information).

All employees (and selected students) must agree to the following terms and conditions in order to be able to connect their devices to the Trust's networks:

- Authorised users who wish to use their own devices to access the Trust's networks must sign and return the statement at the conclusion of this policy.
- When in a PolyMAT School, they should connect their device via that School's wireless network for security.
- When out of School, they should access work systems on their mobile device using secure connections.
- When connecting to the Trust's networks from outside the workplace, users will be required to use 2-factor authentication to reduce the likelihood of unauthorised access.
- All internet access via the network is logged and as set out in the Acceptable Use policy, users are blocked from accessing certain websites whilst connected to the Trust's networks.
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.
- WhatsApp (or similar platforms) should not be used on personal devices for School 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 School business using their personal WhatsApp accounts, sharing school related information which could include categories of personal data.

Non-acceptable Use

- Any apps or software which are downloaded onto the user's device whilst using the Trust's networks is done at the users risk and not with the approval of the Trust.
- 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.
- Technical support is not provided by the Trust on the user's own devices.

Devices and Support

- Desktops, laptops or tablets are allowed provided they are running the same or higher version of Windows as used within the Trust, or the latest version of MacOS.
- Only the latest versions of Android and IOS are supported for BYOD access. Earlier versions of Android and IOS, and other devices are not supported for BYOD, because they do not meet the required security standards. Users must ensure updates are installed as soon as they are available.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps such as browsers, office productivity software and security tools, before they can access the network.
- In order to prevent unauthorised access, devices must be password/pin/biometric protected using the features of the device and a strong password is required to access the Trust's networks.
- Devices which have been tampered with or unlocked to enable non-standard functionality not intended by manufacturer - known as "rooted" (Android) or "jailbroken" (IOS) devices - will not be enabled for BYOD use. Any device that becomes rooted or jail broken will have access denied or removed.

Security

- When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example, through password protection and cloud back up), 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 their own protection on their own device (such as insurance).
- If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device).
- In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the Trust's Data Breach policy.
- The Trust may require access to a device when investigating policy breaches (for example, to investigate cyber bullying).
- Staff are not permitted to share access details to the Trust's networks or Wi-Fi passwords with anyone else.

Disclaimer

- The Trust will not monitor the content of the user's own device but will monitor any traffic over the Trust's systems to prevent threats to the Trust's networks.
- The Trust reserves the right to disconnect devices or disable services without notification.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the Trust's policy as outlined above.
- The employee is personally liable for all costs associated with his or her 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 School network.

Signed: ……

Date: ……

Print Name: ……