St Matthew's CE Primary School

Data Protection:
Bring Your Own Device Policy

ST MATTHEW'S
CE PRIMARY SCHOOL

Created by:	P Langridge	**Date:** February 2023
Approved by:	FGB	**Date:** February 2023
Last reviewed on:	N/A	
Next review due by:	February 2026	

The School has implemented this policy to protect the School 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 School 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 School'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, tablet, laptop, MP3/iPod 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 School's Acceptable Use Policy.

Acceptable Use

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

However by accessing the School'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 (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 school's network (accessing the school's server to exchange data and share resources e.g. printers):

- When in School staff should connect their device via the School's wireless network for security.
- When out of School, staff should access work systems on their mobile device using cloud-based services, secure connections or direct remote connection.
- 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 School network.
- The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by the Headteacher. If approved, any pictures, videos or sound recordings can only be used for School purposes, must be transferred onto school devices/network as soon as possible, delete off the user's device and cannot be posted or uploaded to any website or system outside of the School network from the user's device.
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.
- WhatsApp must not be used on personal devices for sharing School related information which includes categories of personal data.

Non-Acceptable Use

- Any apps or software that are downloaded onto the user's device whilst using the School's own network is done at the users risk and not with the approval of the School.
- Devices may not be used at any time to:
    - Store or transmit illicit materials;
    - Store or transmit proprietary information belonging to the school;
    - Harass others;
    - Act in any way against the School's acceptable use policy and other safeguarding and data related policies.
- Technical support is not provided by the School on the user's own devices
- Distribute images of school children.

Devices and Support

- Smartphones including iPhones and Android phones are allowed as long as these are as up to date as possible (and still supported with official updates) to avoid any known security issues.
- Tablets including iPad and Android are allowed as long as these are as up to date as possible (and still supported with official updates) to avoid any known security issues.
- Where users request the use of school apps or software on their own devices, these must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools.
- In order to prevent unauthorised access, devices must be password/pin/fingerprint protected using the strongest features of the device and a password is required to access the School network.

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 School does not accept responsibility for any loss or damage to the user's device when used on the School's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).
- If possible, staff should install an email app which only allows direct access to School emails with the 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 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 School's data breach policy.
- The School 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 School's network or Wi-Fi password with anyone else.

- The School will not monitor the content of the user's own device but will monitor any traffic over the School system to prevent threats to the School's network.

Disclaimer

- The School 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 School's policy as outlined above.
- The employee is personally liable for all costs associated with their device.
- The School 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, understand and will comply with the terms of this Bring Your Own Device Policy when using my mobile device to access the School network or using my device to access school information or systems.

Signed: ……

Date: …….

Print Name: ……