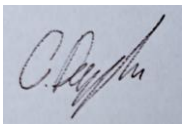
A Caring community ● Courageously learning ● Inspired to live life to the full

Jesus said, ***'I have come that you may have life and have it to the full.'*** John 10:10

Bring Your Own Device (BYOD) Policy (Modal Policy)

Signed (chair): 	Name: Chris Douglas	Date:
Signed (Head): 	Name: Anna Martin	Date:
Ratified by: Governing Body on		Next Review:

Contents

Version	Date	Summary of changes	Author
V1.0	Nov 2021	Initial version	One West
V1.1	Oct 2023	Latest OS/updates applied. Devices/OS not to be used which are out of support Use of separate BYOD WiFi	One West
V1.2	Aug 2025	Refresh	One West

1. Introduction

Bring Your Own Device (BYOD) is the practice of allowing staff to utilise personally owned devices (such as smartphones, tablets or laptops) to securely access some or all of the school's systems, applications and services. BYOD is optional and offered to provide flexibility. Accessing the school's systems, applications and services may not be available to everyone.

2. Purpose

The purpose of this policy is to provide guidance which must be followed when using your own device at work. All users of the BYOD facility are required to read this policy in full and confirm they understand and will comply with it.

3. Scope

This policy applies to all employees of school including contract, agency and temporary staff, volunteers, work placement students and employees of partner organisations working for school.

All users must also comply with all other mandatory policies which are listed below:

a) Data Protection
b) Information Security
c) Records Management
d) Data Breach
e) Acceptable Usage Policy
f) Staff behaviour policy / code of conduct including guidelines on social media and taking images of students.

Should the school discover that these policies are not being complied with at any point, the school reserves the right to withdraw this facility – either disconnect devices or disable services, and without notification.

4. Conditions of Use

The following conditions apply to the use of this facility.

a) Staff / students may only connect to the school's systems for the purpose of authorised work or their studies.
b) Ideally use of a device that has access to the school's systems, applications and services via the BYOD facility should be limited to its owner and should not be shared. If it is necessary to share a device, the first user must ensure that they are logged out of their school account before handing over the device to a colleague/friend. Likewise, when disposing of a device, all work systems, applications, and services must be logged out of and any cached passwords cleared.
c) Account logon, passwords and pin numbers for gaining access to the school's systems, applications and services that have been issued to individuals must remain confidential and never shared with others.

d) No data from the school system may be downloaded and saved to a device. Similarly, data and information may not be downloaded to any storage device, such as a USB memory stick, that is attached to the BYOD device that has been granted access.
e) Staff should be conscious of where they are using their device. They should ensure data and systems displayed on the screen of the device are not visible to others.
f) Screenshots of systems must not be taken.
g) The office team must inform the IT support if staff leave employment with the organisation to have all accounts disabled.
h) The device must have latest update applied and should not be running on any unsupported operating system.

5. Responsibilities

When using the BYOD facility, the school and individuals are responsible for:

5.1. School / Trust

Personal devices are brought into the school entirely at the risk of the owner. The school does not accept any liability for loss or damage of personal devices and data that are using the BYOD system. It is recommended that the owner (at their own expense) purchases an insurance policy to cover loss / theft / damage etc.

The school accepts no responsibility for the day-to-day maintenance or upkeep of a user's personal device, nor for any malfunction of a device due to changes made to the device while on the school's network or whilst resolving any connectivity issues.

The school recommends that all devices are made easily identifiable and have a protective case as the devices are moved around the school.

Students / Staff are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD.

Any charges relating to connecting a BYOD device to the school's systems, applications and services, such as using the data element of a mobile phone contract, are the responsibility of the device owner. It is recommended that Staff / Students using mobile data or Wi-Fi hotspots should periodically monitor the flow of data to ensure that they have sufficient allowance. The school accepts no responsibility for the data required to provide those applications and services.

While the school will take every precaution to prevent a student's / employee's own data from being lost when the school needs to 'remote wipe' a device, it is the staff student's /employee's responsibility to take precautions to protect their data and information, such as backing up emails, contacts, etc.

Only those devices with an operating system (OS) configured to the latest release will be given access to the school's systems, applications, and services. Device owners / users will be responsible for maintaining their device to the latest configuration. The school may periodically ask device users to update the OS on their device in response to a notice from the device manufacturer.

5.2. Staff

In addition to the school's standard acceptable use policies, when using the BYOD facility: staff should only access systems which they require and normally use. Staff should never try to access systems for which they are not authorised. The school's systems may not be used at any time to:

a) Store or transmit illicit / illegal materials including (but not limited to) pornography, fraud and terrorism
b) Store or transmit proprietary information belonging to a company/legal entity
c) Harass, bully or intimidate others
d) Engage in outside business activities
e) Confidential data should only be accessed for a specific work-related requirement.
f) Printing hard copies of material containing personal data is strongly discouraged as it will create security and destruction issues.
g) Hard copies may only be disposed of via school shredders.
h) Staff must not use their own devices to take images or footage of students. Only school equipment may be used, and images must be deleted as soon as they are no longer required, saved securely on the school system and deleted in accordance with the retention policy.
i) Staff should not save the personal numbers of students to their devices and should use trip phones where appropriate.

6. Data loss

In the case of data loss staff must immediately inform the IT department if:

a) Their password has been breached
b) Their device is lost or stolen
c) Organisational systems are not working normally in those cases the IT department may choose to wipe data from the device in order to minimise risk of an impact on either the school's systems, applications and services.
d) In the event of a loss of personal data, the school's Data Breach Policy must also be followed (staff only).

7. Security

Passwords or PINs must be set on personal devices.

a) Passwords must not be saved, either in a web browser on the device or written down and left in accessible places.
b) Users must log out of programmes/applications when they are no longer using them.
c) The latest updates/patches must be applied to the device.
d) Devices/operating systems (OS) must not be used if out of support (see Section 8 below).

The device may be remotely wiped if:

- The device is lost
- When a member of staff leaves the school

- IT detects an incident, such as a data breach or a cyber incident, that presents a threat to the school's systems, applications and services.

8. Monitoring

The school's IT department will monitor use of the school's systems, applications and services accessed via BYOD devices. Monitoring is limited to device usage, and they cannot access personal application data. In some instances, device location may be collected but this data will only be used if the device is lost or stolen.

The IT Department will scan the make and model of devices in use and the version of the operating system (OS) installed. Where an OS is out of date, the user will be expected to upgrade the OS to the latest version within 5 days. Failure to update the OS may result in withdrawal of access to the BYOD facility. Crucially, an out-of-date OS may contain vulnerabilities that could put at risk the school's systems, applications and services.

Spot checks on BYOD devices may be initiated at any time and staff will be expected to allow access to authorised personnel to check settings related to BYOD usage. Spot checks will always be conducted in the presence of the staff member and devices will never be taken away from their owner.

9. Risk

Operation of a BYOD is identified in the school's risk register. The IT Department will periodically update the SLT/Board of Governors/Board of Trustees where risks associated with operating a BYOD increase for whatever reason. This may be due to emerging threats and vulnerabilities.

10. Associated Policy and Guidance

a) Data Protection Policy
b) Information Security Policy
c) Acceptable Use Policy
d) Data Breach Policy
e) Records Management Policy

11. Policy Review

This policy should be reviewed on annually or more frequently if issues arise.