**Considerations**

This policy is for schools / trusts implementing a ‘Bring Your Own Device’ (BYOD) approach. It is important that you will have considered security issues to maximise the advantages of BYOD, while also minimising the risks. Imposition of restrictions and controls that may be perceived by users as too stringent, may deter use of the BYOD facility and hence the school / trust getting the benefits of a BYOD approach.

In conjunction with your IT provider (contracted out or in-house) it is important that the school’s / trust’s leadership has considered the following risks before setting-up a BYOD facility.

* Easier user-initiated deliberate data loss (e.g. copying data from work app to personal)
* Higher potential for accidental data loss (e.g. device backups containing work data, users sharing their device with family, users disposing of device with work data held on the device)
* Higher potential for accidental disclosure (e.g. inadvertent sharing of data, users sharing their device with family)
* Malicious exfiltration of data (e.g. malicious application leaking data that users have allowed it to access)
* Malicious exploitation of devices as a result of weak security configuration (e.g. no data at rest encryption leading to data extraction)
* Higher likelihood of unsupported or out-of-date devices, leading to exploitation of known security vulnerabilities
* Malicious exploitation of devices remains undetected due to lack of monitoring, potentially leading to further spread of malware
* Additional exposure of devices to threats they are being used in a broader personal context, such as user sharing devices or passwords with others

Your BYOD facility should include either all or some of the following good practices:

* Only present the minimum set of services and data required to BYOD users.
* Use a separate WiFi network for onsite use of BYOD
* Employ strong user authentication approaches if this possible.
* Authenticate the device if this is possible.
* Employ risk-based authentication and access control if this is possible.
* Monitor the service and data being accessed as effectively as possible.
* Consider the use of Mobile Device Management (MDM) to remotely wipe segregated (work) data from the device in the event of device loss/theft.
* Assess, understand, and manage the risks.
* Select an approach that is compatible with most supported devices that staff already own.
* Have processes and procedures in place.

**Instructions**

**Please read the draft policy before making changes.**

* Where you see square brackets ‘[ ]’ the approach of your school / trust with regard to this point needs to be considered before making any changes.
	+ In some cases, where your school / trust has decided to not impose certain restrictions and controls this text should be deleted. You may have to speak with the IT department, if in-house, or your contractor, to identify the most appropriate course of action this.
	+ Most of the points presented for consideration are regarded as highly desirable/best practice.
	+ If you are unsure of the applicability these points to your school contact One West for advice but importantly One West will not be able to make that decision for you. Once, all points have been considered and changes made, delete the square brackets.
* Where you see highlighted text replace with the appropriate details.
* Finally, delete this text box and save the file to your set of data protection related documents. *Note the importance of recording the version of this document on cover page and registering it in your school’s document control system*.

**Contents**

[1. Introduction 2](#_Toc209791803)

[2. Purpose 2](#_Toc209791804)

[3. Scope 3](#_Toc209791805)

[4. Conditions of Use 3](#_Toc209791806)

[5. Responsibilities 4](#_Toc209791807)

[5.1. School / Trust 4](#_Toc209791813)

[5.2. Student / Staff 4](#_Toc209791814)

[5.3. Staff 5](#_Toc209791815)

[6. Data loss 5](#_Toc209791816)

[7. Security 5](#_Toc209791817)

[8. Monitoring 6](#_Toc209791818)

[9. Risk 6](#_Toc209791819)

[10. Associated Policy and Guidance 6](#_Toc209791820)

[11. Policy Review 6](#_Toc209791821)

[12. Approval 6](#_Toc209791822)

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |

# Introduction

Bring Your Own Device (BYOD) is the practice of allowing [students and /or 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.

# 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. [IT Department etc may put a consent page on the ‘front page’ of the BYOD Facility re compliance with this policy]

# Scope

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

All users must also comply with all other mandatory policies which are listed below: [Insert as appropriate, changing name to account for name of policy in your school / trust. You may want to hypertext link to those documents that can be accessed by all.]:

1. Data Protection
2. Information Security
3. Records Management
4. Data Breach
5. Acceptable Usage Policy
6. Staff behaviour policy / code of conduct including guidelines on social media and taking images of students.

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

# Conditions of Use

The following conditions apply to the use of this facility.

1. Staff / students may only connect to the school’s / trust’s systems for the purpose of authorised work or their studies.
2. 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.
3. 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.
4. No data from the school / trust 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. [The school should link this with extant policy relating to use of external storage devices although we would strongly discourage this].
5. Staff/ students 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.
6. Screenshots of systems must not be taken.
7. Staff must inform IT (name of individual/organisation that will be responsible for managing the BYOD facility. It may be worth adding contact details – telephone number, email address) if they leave employment with the organisation.
8. The device must have latest update applied and should not be running on any unsupported operating system.

# Responsibilities

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

1.
2.
3.
4.
5.

## School / Trust

Personal devices are brought into the school entirely at the risk of the owner. The school / trust 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 / trust 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 / trust 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 / trust 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.

## Student / Staff

In addition to the school’s /Trust’s standard acceptable use policies, when using the BYOD facility: students / staff should only access systems which they require and normally use. students / 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:

1. Store or transmit illicit / illegal materials including (but not limited to) pornography, fraud and terrorism
2. Store or transmit proprietary information belonging to a company/legal entity
3. Harass, bully or intimidate others
4. Engage in outside business activities

## Staff

These responsibilities relate to staff only:

1. Confidential data should only be accessed for a specific work-related requirement.
2. Printing hard copies of material containing personal data is strongly discouraged as it will create security and destruction issues.
3. Hard copies may only be disposed of (insert details e.g. at school in confidential waste / via school shredders).
4. 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.
5. Staff should not save the personal numbers of students to their devices and should use trip phones where appropriate.

# Data loss

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

1. Their password has been breached
2. Their device is lost or stolen
3. 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.
4. In the event of a loss of personal data, the school’s Data Breach Policy [it may be helpful to insert hypertext link to this policy] must also be followed (staff only).

# Security

Passwords or PINs must be set on personal devices in accordance with the password policy [detail where these are found for your organisation e.g. information security policy].

1. Passwords must not be saved, either in a web browser on the device or written down and left in accessible places.
2. Users must log out of programmes/applications when they are no longer using them.
3. The latest updates/patches must be applied to the device.
4. 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 pupil or 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.

# Monitoring

The school’s / trust’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 / students 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.]

# Risk

Operation of a BYOD is identified in the school’s / trust’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.

# Associated Policy and Guidance

1. Data Protection Policy
2. Information Security Policy
3. Acceptable Use Policy
4. Data Breach Policy
5. Records Management Policy

# Policy Review

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

# Approval

This policy was approved by the Governing Body/ Board of Trustees on DATE

Signed: NAME & ROLE