

Aberdare Community School Ysgol Gymunedol Aberdâr



Mobile Device Acceptable Use Policy

Date Adopted	21 st September 2022
Signature of Headteacher	<i>Chwella Morgan</i>
Signature of Chair of Governors	<i>John Brindley</i>
Date to be reviewed	September 2023

MOBILE DEVICE ACCEPTABLE USE POLICY

Review

This policy has been approved by the Technical Management Team and any amendments to it require the team's approval.

- Last approval: N/A
- Last review: N/A
- Next review: TBA

Overview

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business uses for connecting mobile devices to the School's network and data.

In order to protect the integrity of the confidential client and business data that resides within the School's infrastructure, including internal and external cloud services, this policy encompasses any mobile hardware device that is used to access corporate resources, whether the device is owned by the user or by the organization.

This device list includes but is not limited to:

- Smartphones
- Other mobile/cellular phones
- Tablets
- E-readers
- Portable media devices
- All classes of personal computers
- Wearable computing devices
- Any other mobile device capable of storing corporate data and connecting to a network

In order to maintain security and manageability, only devices fitting the following criteria are allowed to access corporate resources:

- Smartphones, tablets, and other devices running Android version 2.3 (Gingerbread) and higher.
- Smartphones and tablets running iOS 6.0 and higher.
- Smartphones running the BlackBerry OS.
- Smartphones and tablets running Windows Mobile OS 7 and higher.

Applicability

This policy applies to all Aberdare Community School employees, including full and part-time staff, students, contractors, guests and other agents who use a mobile device to access, store, back up, or relocate any organization or client-specific data. Consequently, employment at ACS does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

The policy addresses a range of threats to enterprise data, or related to its use, such as:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive corporate data is deliberately stolen and sold by an employee or unsanctioned third party.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced to or via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose Medaille College to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of the IT Manager. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the enterprise network.

Acceptable Use

The ACSCS has the overall responsibility for the confidentiality, integrity, and availability of corporate data as well as for the execution and maintenance of information technology and information systems.

All ACS employees are responsible to act in accordance with company policies and procedures.

Affected Technology

Connectivity of all ACS owned mobile devices will be centrally managed by ACSCS and will use authentication and strong encryption measures. Although ACSCS will not directly manage personal devices purchased by employees, end users are expected to adhere to the same security protocols when connected to non-corporate equipment.

Policy & Appropriate Use

It is the responsibility of any ACS user who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct School business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

Access Control

1. ACSCS reserves the right to refuse, without notice, the ability to connect mobile devices to schools networks and systems. ACSCS will engage in such action if such equipment is being used in a way that puts the schools, data and users at risk.
2. Prior to initial use on the corporate network or related infrastructure, all mobile devices must be approved by IT Manager. ACSCS will maintain a list of approved mobile devices and related software applications and utilities, and it will be maintained in the School's Approved Technology List.

3. End users who wish to connect such devices to the network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT Manager. This includes access via VPN, enrolment in the Schools mobile device management solution or another method approved by ACSCS. Enterprise data is not to be accessed on any hardware that fails to meet Schools established data access methods.
4. All personal mobile devices attempting to connect to the corporate network through the Internet will be inspected using technology centrally managed by ACSCS. Devices that are not approved by the IT Manager, are not in compliance with the schools security policies, or represent any threat to the corporate network or data will not be allowed to connect. Devices may only access the corporate network and data through the Internet using a Virtual Private Network (VPN) connection. Smart mobile devices such as smartphones, tablets, and laptops will access the corporate network and data using mobile management software installed on the device by ACSCS.

Mobile Device Management (MDM)

1. ACS uses Cisco Meraki mobile device management solution to secure mobile devices and enforce policies remotely. Before connecting a mobile device to the schools resources, the device must be set to be managed by MDM.
2. Cisco Meraki client agent must be installed on any mobile device connecting to Schools resources. Even personal devices owned by employees must have the client application installed. The application can be installed by contacting the IT Manager.
3. The mobile device management solution enables the ACSCS to take the following actions on mobile devices: remote device wipe, location tracking, application visibility, and hardware feature management. ACS also allows securing and provisioning mobile devices properly to minimize corporate risk.
4. Any attempt to contravene or bypass the mobile device management implementation will result in immediate disconnection from all corporate resources. For School-owned devices this will result in device locking or erasure.

Security

1. Users using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password. Users agree never to disclose their passwords to anyone.

2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.
3. Any non-corporate computers used to synchronize or back up data on mobile devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by IT Manager.
4. Any mobile device that is being used to store Schools data must adhere to the authentication requirements of ACSCS. In addition, all hardware security configurations must be pre-approved by the IT Manager before any enterprise data-carrying device can be connected to the corporate network.
5. ACS will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt.

In the event of a lost or stolen mobile device, it is incumbent on the user to report the incident to the IT Manager immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than the school. If the device is recovered, it can be submitted to ACS for re-provisioning.

Hardware & Support

1. ACS reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.
2. Users will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, jail breaking, rooting) without the express approval of ACSCS.
3. ACS will support the connection of mobile devices to corporate resources. On personally owned devices, ACSCS will not support hardware issues or non-approved applications.

Organizational Protocol

1. ACS can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to school's networks may be monitored to record dates, times, duration of access, etc. in order to

identify unusual usage patterns or other suspicious activity. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with schools' policies.

2. The end user agrees to immediately report to ACS any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

Policy Non-Compliance

Failure to comply with the Schools Mobile Device Acceptable Use Policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment/education.



Mobile Device Acceptance Form

Device Name:
Device Model:
Device Serial:
Issued To:
Department:

1. I acknowledge receipt of an Aberdare Community School mobile device and receipt of the usage policy document for mobile devices (this document).
2. I agree to read the complete usage policy document before using the mobile device and to abide by the directives and guidelines contained within it. In the event that I do not agree with the policy document, having read it, I agree to return the mobile device immediately, unused.
3. I agree to ensure that my line manager is aware of their responsibilities relating to this mobile device.
4. I agree to ensure to inform the IT Manager in the event of loss of this mobile device.

Personal Usage: I will / I will not be using this mobile device for personal usage.

Signed: _____

Printed: _____

Date: _____