Aldar Education

Aldar Education Bring Your Own Device (BYOD) Policy Manual

Instrument Information	
Name	Aldar Education Bring Your Own Device (BYOD) Policy Manual
Reference	ALDED-EDT-DSR-PL-00001

Instrument Version Control		
Version	**Date**	**Change Summary**
Version 1	September 02, 2025	Initial Version

Contents

A. INTRODUCTION

1. TITLE

1.1. This Instrument is entitled the Aldar Education Bring Your Own Device (BYOD) Policy Manual ("the Policy").

2. PURPOSE

2.1. The purpose of this Policy is to:

2.1.1. Define controls in place for accessing Company information through mobile devices not owned by the Company, including the services that may be accessed, how the services will be accessed and where the services must be accessed from.

2.1.2. Promote digital literacy and responsibility,

2.1.3. Enhance access to educational resources,

2.1.4. Ensure data security and privacy, and

2.1.5. Establish clear expectations for appropriate use.

2.2. Users must agree to the terms and conditions set forth in this Policy to be able to connect their personally owned devices to the Company's intranet / internet applications (including email).

3. GOVERNING INSTRUMENT

3.1. This Policy Manual must be read in conjunction with the following sections of ISO 27001:2022:

3.1.1. A.5.14 Information transfer,

3.1.2. A.6.7 Remote Working, and

3.1.3. A.8.1 User endpoint devices.

4. SCOPE

4.1. Except to the extent that a contrary intention is expressed, this Policy binds and applies to all Employees across the Aldar Education (AE) HQ and its Operated Schools, the students and other personnel who wish to use their personally owned devices on school premises or access school resources remotely (hereafter referred to as User). For Managed Schools, this Policy will be referred to areas where the responsibility is given to Aldar Education as per the respective legal agreement.

4.2. Nothing in this Policy has the effect of invalidating past acts validly performed under previous Instruments.

4.3. This Policy addresses the following areas:

4.3.1. Device Registration and Usage,

4.3.2. Securing the BYOD,

4.3.3. Acceptable Use,

4.3.4. Security Breaches, and

4.3.5. Training and Awareness.

5. COMPLIANCE

5.1. Violations of this Policy and supporting policies may result in corrective action by the relevant management authorities. Disciplinary investigation will be consistent with the severity of the incident as determined by the investigation.

5.2. Any instance of non-compliance or breaches of this Policy must be reported immediately to Aldar Education Service Desk at sd@aldareducation.com for immediate action and resolution.

5.3. All queries regarding interpretation of this Policy Manual must be addressed to Aldar Education Service Desk at sd@aldareducation.com.

5.4. Only the approved version of this Policy Manual must be used. The printed copies are uncontrolled and will not be considered valid.

B. POLICY STATEMENTS

1. DEVICE REGISTRATION AND USAGE

1.1. General Controls

1.1.1. Personally owned devices accessing the AE data must be registered using the corporate Mobile Device Management (MDM) or Mobile Application Management (MAM) Solution.

1.1.2. End User device must install AE proposed certificate or respective configuration profiles prior to accessing AE resources.

1.1.3. For any issues related to BYOD registration or configuration, school users must contact the Digital & Technology Services (DTS) support team at their campus or Aldar Education Service Desk at sd@aldareducation.com.

1.1.4. End users are responsible for maintaining regular backups of their personal devices.

1.2. BYOD Controls For AE Students

1.2.1. The school follows a structured BYOD program for students, aligned with Apple device strategy.

1.3. Usage by School Employees and Students

1.3.1. Devices must be used for educational purposes only during instructional time.

1.3.2. Users must comply with the Aldar Education Responsible Use Policy.

1.3.3. Activities that are prohibited includes, but not limited to, the following:

- Installation of pirated or illegal software,
- Access to explicit, violent, or inappropriate content, and
- Disruption of teaching or learning through misuse of devices.

2. SECURING THE BYOD

2.1. AE data stored, transferred, or processed on BYOD remains under AE's ownership, and AE retains the right to control such data even if not on AE device.

2.2. End User device must comply with the applicable AE information security standards.

2.3. End User device (registered with the MDM / MAM solution) must not be jail broken, rooted, or tampered in a way that may lead to breach of AE's Information Security Policy.

2.4. Users must meet the Aldar Education Information Security Policy requirements to use the service.

3. ACCEPTABLE USE

3.1. Only authenticated Users must access AE resources and the below services through pre-registered BYOD(s):

3.1.1. AE Email,

3.1.2. Aldar Education Service Desk,

3.1.3. Live Aldar App,

3.1.4. Teaching and learning apps,

3.1.5. ERP, and

3.1.6. Office 365 applications.

3.2. BYOD(s) must not be left unattended whether inside or outside AE premises and must be locked or kept in safe place.

3.3. Registered Users must ensure that information resources in BYOD are not viewed by unauthorized persons.

3.4. Classified information must be additionally protected in accordance with the Information Classification and Labelling controls defined in the Aldar Education Information Security Policy.

4. SECURITY BREACHES

4.1. Users must comply with the terms of this Policy and all other Policies and Procedures published in its support.

4.2. All security breaches e.g., lost, or stolen devices, must be reported immediately to Aldar Education Service Desk at sd@aldareducation.com.

4.3. User must not hold AE accountable for any data loss, if the lost device is recovered later by the User & the User did not inform Aldar Education Service Desk to cancel the remote wipe-operation well in time.

4.4. AE may modify the BYOD Policy and/or BYOD configuration profile to prevent further breaches, if needed.

4.5. AE will not:

4.5.1. pay the allowed Users any fee for using their BYOD(s) for work purposes, or

4.5.2. be held responsible for any personal data loss or external data charges due to the use of BYOD service.

5. TRAINING AND AWARENESS

5.1. DTS Department will conduct:

5.1.1. Cyber security awareness training for all the Users, and

5.1.2. Targeted or role specific awareness sessions for IT Users.

5.2. Aldar Education Service Desk may be contacted for any queries or assistance related to BYOD Policy and configuration at sd@aldareducation.com.

C. DEFINITIONS

Term or Abbreviation	Definition
AE or Company	Refers to Aldar Education including all Aldar Education Operated Schools and Managed Schools.
/	It implies ‘or’ and is used to link the alternatives.
Bring Your Own Device (BYOD)	This includes all personally owned devices that can store, transfer, or process any sensitive information. These include devices such as laptops, smart phones, tablets, including infrastructure controls configured in place to serve or secure these services.
Department	An organisational unit of the Company, which forms part of a Division. A Department falls under the leadership of a head position or higher, who reports directly to the Executive Manager of the Division.
Division	A vertical organisational unit of the Company, which falls under the leadership of an Executive Manager who reports directly to the CEO, and which may have subordinate Departments.
DTS	Refers to Digital & Technology Services Department of Aldar Education.
Employee	Includes temporary, permanent, full-time and part-time employees.
Framework	A specialised type of Policy which contains a logical structure developed to organize other Instruments into a plan, hierarchy, or structure.
Governing Instrument	Governing Instrument is any document that establishes the rules, principles, or guidelines that the Policy/Framework must be aligned with.
HQ	Head Quarters.
Instrument	A document to provide guidance, impose obligations, define responsibilities or delegate authorities, such as, Framework, Policy, SOPs, etc.
Managed Schools	Refers to ADNOC or ADEK schools that are managed by Aldar Education. Specific areas of responsibilities will be governed by the respective legal agreements entered into with these entities.
Mobile Device Management (MDM) / Mobile Applications Management (MAM) Solution	These solutions enable IT and security teams to monitor, manage, and secure the mobile devices connected to their corporate network. That includes corporate-issued and personal (BYOD) devices, various device types, and whichever operating systems those devices are running.
Operated Schools	Refers to schools that are fully owned and directly operated by AE.
Policy / Policy Manual	An Instrument containing statements of principles, business rules, or internal controls articulated and aligned with legal, regulatory, or

Term or Abbreviation	Definition
	organizational requirements, and by which Aldar will be guided in the management of its affairs and the development of its procedures.
Procedure	An Instrument which describes the activities necessary to implement a Policy, focused on the responsibilities and requirements to carry out tasks, activities and processes.
Process / Standard Operating Procedure (SOP)	A series of tasks to be undertaken to carry out operational task, eventually achieve the intended results or outputs, and contribute to the successful operation of the Company. The process also identifies specific responsibilities and Supporting Documents necessary for its full implementation and maintenance.
Supporting Documents	Documents which support the implementation of Instruments. Supporting Documents include but are not limited to guidelines, forms, templates, SOPs or any 'uncontrolled' documents (E.g., system generated or external).
User / End User(s)	An end user, in the context of information technology is defined as the ultimate final consumer or user of a product, system, or service. End users are individuals who interact directly with the final software application, hardware device, or digital service, utilizing its features and functionalities to meet their specific needs or requirements.