Aldar Education

Aldar Education Information Systems Responsible Use Policy Manual

Instrument Information	
Name	Aldar Education Information Systems Responsible Use Policy Manual
Reference	ALDED-EDT-GEN-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 Information Systems Responsible Use Policy Manual (“the Policy”).

2. PURPOSE

2.1. This Policy has been written to establish the following controls:

2.1.1. To ensure appropriate use of Aldar Education’s information systems and facilities in the conduct of business.

2.1.2. To create an environment that fosters sound security practices and the effective use of business resources.

2.1.3. To ensure that the Company has access to reliable and robust technology resources that are safe from unauthorised or malicious use.

3. GOVERNING INSTRUMENT

3.1. This Policy Manual must be read in conjunction with the following:

3.1.1. Federal Decree-Law No. (38) of 2021 on Copyrights and Neighboring Rights, and

3.1.2. ISO 27001:2022.

4. SCOPE

4.1. Except to the extent that a contrary intention is expressed, this Policy binds and applies to:

4.1.1. All Employees across Aldar Education HQ, Aldar Training Academy (ATA) and its Operated Schools, students, contractors, as well as any other individuals or entities that may use information and information technology resources belonging to Aldar Education (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.

4.1.2. Information systems owned or leased by Aldar Education (hereafter referred to as “AE”) and to any privately-owned equipment connected to the AE’s network and include, but is not limited to, computers, tablets, software, operating systems, storage media, and the internet.

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. Roles and Responsibilities,

4.3.2. Usage of Aldar Education Information Systems / Resources,

4.3.3. Use of Unauthorised Copies of Licensed Software and Hardware,

4.3.4. Use of Freeware and Shareware Applications,

4.3.5. Use of Copyrighted Material and Digital Tools,

4.3.6. Introduction of Pornographic Material,

4.3.7. Introduction of Destructive Programs,

4.3.8. Privacy and Confidentiality,

4.3.9. Working Off-Site,

4.3.10. Actions upon Termination of Contract or Leaving School,

4.3.11. Internet Usage,

4.3.12. Information Protection,

4.3.13. Public Representations,

4.3.14. Electronic Mail (Email),

4.3.15. Anti-Virus,

4.3.16. Data Storage on OneDrive / SharePoint,

4.3.17. Instant Messaging (IM),

4.3.18. Due Diligence, and

5. COMPLIANCE

5.1. Violations of this Policy and supporting Instruments may result in corrective action by the relevant management authorities. The disciplinary investigation will be conducted in accordance 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 the 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. Printed copies are uncontrolled and will not be considered valid.

B. POLICY STATEMENTS

1. ROLES AND RESPONSIBILITIES

1.1. Every User of AE's Digital & Technology Services (DTS) resources are required to know the relevant Policies and to conduct their activities within the scope of these Policies.

2. USAGE OF ALDAR EDUCATION INFORMATION SYSTEMS / RESOURCES

2.1. Any work-related exploration or search of the public domain is acceptable provided the Users comply with the AE Policy, standards, and Procedures regarding such usage, whilst also complying with the Policies, standards, and Procedures of the explored site.

2.2. Usage of information systems and resources must be in line with the Company's People and Culture Policies and Aldar Group Code of Business Conduct Policy.

2.3. End Users must not:

2.3.1. Use AE information systems for purposes other than Company / School related activities.

2.3.2. Use resources for personal reasons or on behalf of a third party (i.e., personal client, family member, political / religious / charitable or school organisations, etc.).

2.3.3. Use someone else's User ID and password to access (AE's) DTS systems.

2.3.4. Leave their User accounts logged in at an unattended and unlocked computer.

2.3.5. Leave their password unprotected (for example writing it down).

2.3.6. Perform any unauthorised changes to (AE's) DTS systems or information.

2.3.7. Attempt to access data that they are not authorised to use or access.

2.3.8. Exceed the limits of their authorisation or specific business need to access the system or data.

2.3.9. Connect any non-AE authorised device to the AE internal network or DTS system.

2.3.10. Transfer AE data on any unauthorised device.

2.3.11. Use AE information systems to store, process, download or transmit data that can be construed as biased (politically, religiously, racially, ethnically, etc.) or supportive of harassment.

2.3.12. Download, redistribute and print copyrighted articles, documents or other copyrighted materials through AE information systems.

2.3.13. Receive, print, transmit, or otherwise disseminate proprietary data, Company secrets, or other confidential information in violation of Company Policy or proprietary agreements.

2.3.14. Download inappropriate material such as picture files, music files or video files for personal use.

2.3.15. Engage in unsafe online interactions, including communication with users presenting fake or misleading profiles.

2.3.16. Exhibit personal online behavior that may cause harm to oneself or others, such as engaging in or encouraging cyberbullying.

2.3.17. Participate in or be exposed to financial risks through AE systems, including online scams, gambling, or phishing activities.

2.4. Students at AE Schools must use personal devices on AE network in accordance with the Aldar Education BYOD Policy. This will include School premises and usage during any extracurricular activities that take place outside the School premises.

2.5. Students must purchase a Digital Safety Package to enrol their devices in the AE Mobile Device Management (MDM) system.

2.6. Only AE provided VPN connection must be used to connect to School DTS systems. The use of VPNs by students will be restricted on School premises or through School networks unless explicitly authorised for specific educational or administrative purposes.

3. USE OF UNAUTHORISED COPIES OF LICENSED SOFTWARE & HARDWARE

3.1. It is strictly prohibited to:

3.1.1. Use unauthorised copies of licensed software and hardware (piracy / copyright and patent infringement) on AE information systems and copying such material.

3.1.2. Store, process, or transmit unauthorised copies of licensed software and hardware (piracy/copyright and patent infringement).

4. USE OF FREEWARE AND SHAREWARE APPLICATIONS

4.1. The installation and use of freeware or shareware software, whether downloaded from the internet or obtained through any other media, on AE information systems will be permitted only after obtaining the required approval and the User will not be permitted to install such freeware or shareware.

4.2. Freeware and shareware applications will be evaluated and tested by Aldar Education before installation on AE information systems.

4.3. Users must not install any games in the AE information systems.

5. USE OF COPYRIGHTED MATERIAL AND DIGITAL TOOLS

5.1. Responsible Use of Copyrighted Material

5.1.1. The use of copyrighted materials, including but not limited to books, articles, images, videos, and digital content, must comply with Federal Decree-Law No. (38) of 2021 on Copyrights and Neighboring Rights.

5.1.2. Students and School Employees must obtain proper authorisation or licenses before using copyrighted materials for educational or administrative purposes.

5.1.3. Aldar Education will provide training and guidelines on fair use, copyright compliance, and proper attribution of digital and printed materials at least on annual basis.

5.1.4. Unauthorised reproduction, distribution, or modification of copyrighted materials is strictly prohibited and may result in legal and disciplinary consequences.

5.2. Use of Digital Tools, Including Artificial Intelligence (AI)

5.2.1. The use of digital tools, including AI and other emerging technologies, must align with ethical and responsible practices.

5.2.2. AI-generated content must be reviewed for accuracy and must not be used to misrepresent authorship, fabricate research, or bypass academic work.

5.2.3. Aldar Education has established guidelines on how AI tools can be used in learning and assessment, ensuring they complement rather than replace original student work.

5.2.4. Any misuse of AI or other digital tools for deceptive academic practices will be treated as academic misconduct and subject to disciplinary action.

5.3. Academic Honesty and Plagiarism

5.3.1. All students and School Employees must uphold the highest standards of academic integrity by ensuring that all work submitted is their own and properly cited where applicable.

5.3.2. Plagiarism, including copying, improper citation, and the uncredited use of other's work (whether written, digital, or otherwise), is strictly prohibited.

5.3.3. Schools has implemented measures to educate students and staff on plagiarism, proper citation methods, and responsible academic conduct.

5.3.4. Any detected cases of plagiarism or academic dishonesty will be subject to disciplinary action. Users may also be subject to actions as proposed by the relevant authority.

6. INTRODUCTION OF PORNOGRAPHIC MATERIAL

6.1. It is strictly prohibited to:

6.1.1. Introduce pornographic material into any information systems environment.

6.1.2. Store, process, or transmit pornographic material on AE information systems by the Users.

7. INTRODUCTION OF DESTRUCTIVE PROGRAMS

7.1. The introduction of destructive programs (e.g., viruses, self-replicating code) to cause intentional damage, interfere with others, gain unauthorised access, or inhibit production to AE's information systems is strictly prohibited.

8. PRIVACY AND CONFIDENTIALITY

8.1. The privacy of customer information and AE information must always be maintained by all the Users. All customer related information and internal AE information is private and confidential, unless indicated otherwise and in accordance with the Aldar Education Privacy Policy Manual.

8.2. The data stored on the AE information systems is under the ownership of the organisation, the deliverables created by AE Users are also the intellectual property of AE.

8.3. AE has the obligation to share the User's data internally and externally when it is legally required to do so as per the applicable laws.

9. WORKING OFF-SITE

9.1. Laptops and mobile devices may be taken off-site subject to the following controls:

9.1.1. Only secure and AE provided VPN connection must be used to connect to office DTS systems.

9.1.2. AE information systems and media taken off-site must not be left unattended in public places.

9.1.3. Laptops must be carried as hand luggage when travelling and precaution must be taken at airports.

9.1.4. Information must be protected against loss or compromise when working remotely (for example at home or in public places).

9.1.5. Care must be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

10. ACTIONS UPON TERMINATION OF CONTRACT OR LEAVING SCHOOL

10.1. AE information systems and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs (if applicable), must be returned to AE at termination of contract / employment or upon leaving the School.

10.2. AE data or intellectual property developed or gained during the period of employment/engagement remains the property of AE and must not be retained beyond termination/engagement with AE or reused for any other purpose.

11. INTERNET USAGE

11.1. As internet services are a key communication and entry point to the outside world for AE, it is the responsibility of every User to ensure that these services are used appropriately and consistently in accordance with this Policy to facilitate protection of AE against the threats of unauthorised access, theft of information, theft of services and malicious disruption of services.

11.2. Access to the internet through the Company's network is a privilege. Users granted this privilege must adhere to the following strict guidelines concerning the appropriate use of this information resource:

11.2.1. Only authorised personnel may establish internet or other external network connections from within AE / Schools with the approval of the DTS Department.

11.2.2. Users wishing to establish a trusted connection with AE / Schools to access internal systems must be authenticated before gaining access to the internal network.

11.2.3. Communication facilities will be provided on each remote computing devices to connect through a trusted, secure, and authenticated connection.

11.2.4. Users must not attempt to disable, defeat, or circumvent the internet security arrangements.

11.2.5. Users must not violate this privilege by using access to the internet for unsuitable purposes that may bring the Company into disrepute.

11.2.6. Internet access must be through the service provider engaged by AE. Accessing the internet from corporate facilities / Schools through any other means is prohibited.

11.2.7. Other prohibited uses of internet include, but are not limited to:

- Usage of peer-to-peer networks such as Bit-torrent, Limewire, Kazaa, Torrents or any unauthorised internet-based media/file transfer and storage mechanism. Refer to Aldar Education Communications Policy for details on use of personal social media accounts.
- Usage of sites that facilitate proxy avoidance.
- Usage of sites that facilitate VOIP (Voice Over IP), streaming audio and video, unless authorised by Aldar Education.
- Engaging in any blogging activities that may tarnish the AE's image, reputation, and goodwill.

11.2.8. Users who wish to upload, or post or publish AE's proprietary material on internet must be aware that copyright, trademark, libel, slander, and public speech control laws exist in all countries. Care must be taken not to violate any laws that may be enforceable against AE.

11.2.9. Users must not post or place any Company material on any publicly accessible computer without prior written permission from AE Marketing & Brand team.

11.2.10. Users must not:

- Access or display sexually explicit images / documents and racist, terrorist, or similar material on any AE system.
- Archive, store, distribute, edit, or record sexually explicit material and racist, terrorist, or similar material using the AE's network or computing resources.

11.2.11. If the User finds that they have connected to a site that contains such material, they must disconnect immediately, regardless of whether that site has been previously deemed acceptable by any screening or rating program.

11.2.12. Aldar Education has implemented data leakage prevention technology and monitors AE's data shared externally as per the Aldar Education Information Security Policy.

11.2.13. Users may download only software and data that have a direct business use. All such software and data must be properly licensed and registered. Downloaded software must be used only under the terms of its license. No person with access to the AE's facilities may use them knowingly to download or distribute pirated software or data.

11.3. All software downloaded via the internet into the AE's network and systems will become the property of the Company. User must scan any file that is downloaded for viruses before it is opened or run.

11.4. Files containing confidential or private data must be transferred across the internet using only the file transfer channel provided by DTS Department. All the restrictions listed on interactive access to the internet in respect of sites that are sexually explicit, racist, terrorist etc. will also apply to internet email.

11.5. Comprehensive security arrangements are in place to protect the Company. Personnel must not attempt to disable, defeat, or circumvent these internet security arrangements.

12. INFORMATION PROTECTION

12.1. It is strictly prohibited to send sensitive and confidential information over the internet unless expressly authorised by the owner of the information. This includes information such as:

12.1.1. Company credit card numbers, telephone calling card numbers, customer details, Employee details, student details, School community details, login passwords and other information that may be used to gain access to corporate systems, information, or services, etc., must not be sent over the internet in a readable format.

12.1.2. Company material (software, internal memos, etc.) on any publicly accessible internet computer.

12.1.3. Source code unless it is specifically known to be in the public domain.

12.1.4. Network or server configuration information about any AE machine to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types and software version numbers.

13. PUBLIC REPRESENTATIONS

13.1. Users must not indicate their affiliation with AE in bulletin board discussions, chat sessions and other services on the internet.

13.2. Employees or third-party personnel using AE facilities must not publicly disclose internal AE information via the internet which may adversely affect AE, its customer relations and public image.

13.3. Users must ensure that postings to mailing lists, public news groups and related websites do not reveal details of the internal functioning, infrastructure, or potential vulnerabilities in AE's information security infrastructure. Refer to Aldar Education Communications Policy for details on social media guidelines.

14. ELECTRONIC MAIL (EMAIL)

14.1. Email services are a key enabler to the business of AE. Users must ensure that these services are used appropriately and consistently with AE's Information Security Policy.

14.2. Email Usage

14.2.1. Access to email services is limited to authorised personnel only in accordance with the Aldar Education Information Security Policy.

14.2.2. Excessive use of email for personal communication is not permitted.

14.2.3. Emails must follow the Company Policies regarding decency and appropriate content including following restrictions:

- Transmission or subscription to any inappropriate content that is offensive, defamatory, or threatening to others.
- Communication of statements, messages, or images consisting of pornographic material, ethnic slurs, racial epithets, or anything that may be construed as harassing, offensive or insulting to others based on race, religion, national origin, colour, marital status, citizenship status, age, disability, or physical appearance.
- Production or distribution of unsolicited bulk mail messages (also known as chain or spam mail) or to operate a business or make solicitations for personal gain, political or religious causes or outside organisations.
- Users must not forward or otherwise propagate to individuals or group chain letters, pyramid schemes or any other types of data that may unnecessarily consume system resources or otherwise interfere with the work of others.
- Transmittal of or receipt of trade secrets, copyrighted materials or proprietary or confidential information, unless permitted through the conditions of usage of such documents.

14.2.4. Standard legal disclaimers and email signatures must be used in all emails. Any modifications to these are strictly prohibited.

14.2.5. Personnel must exercise the same care in drafting email as they would for any other written communication that bears the AE name.

14.2.6. To maintain appropriate controls over the use of email services, Users must not disclose their User IDs and passwords to anyone. Users must take appropriate precautions to prevent unauthorised use of their email account, such as using complex passwords and not writing down email passwords for reference. Detailed controls for password management are provided in the Aldar Education Information Security Policy.

14.2.7. Impersonation by email is strictly prohibited. Users must not adopt aliases or misrepresent themselves through their email. Users must identify themselves by their real name; pseudonyms not readily attributable to actual Users must not be used.

14.2.8. The forging of header information in an email is strictly prohibited. This includes the alteration of source address, destination address and timestamps.

14.2.9. Users must not publish or distribute internal mailing lists to external parties.

14.2.10. Attachments from unknown or untrusted sources must not be opened. Users must scan the email attachments, regardless of the source or content, for viruses and other destructive programs before being opened or stored on any AE computer system. Any untrusted source or suspected malicious emails must be reported to Aldar Education Service Desk (sd@aldareducation.com).

14.3. Employees, personnel, students or third-party contractors using AE facilities must not modify the security parameters within the email system. Users making unauthorised changes to the email security parameters will be in violation of this Policy.

14.4. Attachment file sizes above 35MB will be blocked by the email system to prevent the blocking of bandwidth for other Users. Error notifications will be automatically sent for undelivered emails to the sender. Non-business-related emails containing large file attachments, such as graphics and multimedia files must not to be sent via email.

14.5. Users must not execute any programs received by email. Users must not install any upgrades or patches received by email.

14.6. With prior approval, AE may, at any time and with or without notice, monitor, search, review, disclose, or intercept this information for any legitimate purpose, including but not limited to the following:

14.6.1. To monitor performance.

14.6.2. Ensure compliance with AE Policies.

14.6.3. Prevent misuse of the email services.

14.6.4. Troubleshoot hardware and software problems.

14.6.5. Comply with legal and regulatory requests for information.

14.6.6. Investigate disclosure of confidential business, proprietary information or conduct that may be illegal or adversely affect AE or its associates.

15. ANTI-VIRUS

15.1. Users must comply with the Aldar Education Information Security Policy and measures put in place to protect against malicious programs, known as computer viruses.

15.2. Depending on the nature of the virus, it may have a minor or major impact on the behaviour or performance of the system, or it may result in the loss of data or confidentiality of information and even loss of trust or reputation from our customers and business partners.

15.3. Users' responsibilities are as follows:

15.3.1. Users must always run the standard anti-virus software provided by AE. All computers (desktops and laptops) are issued pre-installed with the standard anti-virus software.

15.3.2. Users must not attempt to either alter or disable anti-virus software installed on any computer attached to the network.

15.3.3. If a User receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to Aldar Education Service Desk (sd@aldareducation.com) immediately. The following information must be provided, if known, virus name, extent of infection, source of virus, and potential recipients of infected material.

15.3.4. Users must refrain from performing the following actions:

- Attempt to destroy or remove a virus, or any evidence of that virus, without direction from the DTS Department.
- Forward these or any virus warning messages by email to keep network traffic to a minimum.
- Open any files or macros attached to an email from an unknown, suspicious, or non-trusted source.
- Open any files or macros attached to an email from a known source (even a co-worker) if you were not expecting a specific attachment from that source.
- Click on a link sent to the User if they were not expecting a specific link. Users must be suspicious of email messages containing links to unknown websites. It may be possible that the link is a malicious executable (.exe) file disguised as a link.
- Copy, download, or install files from unknown, suspicious, or non-trusted sources.

15.3.5. Files with certain filename extensions are blocked by the outsourced scanning and monitoring services which includes files with extensions *.BAT, *.EXE, *.SYS. Users must contact Aldar Education Service Desk (sd@aldareducation.com) for advice if they require a file that is listed above.

15.4. User must avoid, wherever possible, the sharing of external hard disks with read/write access. Users must always scan removable media for viruses before using it. If personally owned home computers are used for business purposes and files are transferred to a work computer, User must ensure the media and files are scanned before use.

15.5. Viruses And Malicious Software Protection

15.5.1. The introduction of destructive programs (e.g., viruses, self-replicating code) may cause intentional damage, interfere with others, gain unauthorised access, or inhibit production to AE's information systems and is strictly prohibited.

15.5.2. Aldar Education will remove any computer believed to be infected by a virus from the network until it is verified as virus-free.

16. DATA STORAGE ON ONEDRIVE / SHAREPOINT

16.1. File server storage space is governed by the DTS Department to ensure the continual availability of storage space on the network.

16.2. User folder (OneDrive / SharePoint): AE provides each User with a secure OneDrive / SharePoint access as part of the Microsoft Office 365 subscription for the dedicated storage on the cloud with access restricted to that User. User must maintain good housekeeping over their OneDrive / SharePoint folders and must ensure that redundant files, which are no longer needed, are removed.

16.3. Users must use the OneDrive / SharePoint as the primary storage for electronic version of business documents. Usage of data storage system must comply with this Policy. Inappropriate files include non-business-related MP3s, GIF files, games, executables, VBS files and any other User-installed software not approved by Aldar Education.

17. INSTANT MESSAGING (IM)

17.1. IM through Microsoft Teams is currently being used as a form of real-time communication between Employees. IM technology is meant for enhancing productivity while conducting the business.

17.1.1. Acceptable use: IM services must be used for business communications and for fulfilling job duties, in accordance with corporate goals and objectives. Users must exercise sound judgment and common sense while using IM to fulfil their job duties. The use of IM is a privilege, and its abuse or misuse is not acceptable; the Information Systems Responsible Use Policy must be adhered to in the usage of IM.

17.1.2. Personal use: Users may not use AE Corporate IM for personal reasons during normal business hours.

17.1.3. Unacceptable use: The IM service must not be used for purposes that may be reasonably expected to cause excessive strain on systems, such as:

- Viewing, copying, altering, or deleting IM accounts or files belonging to another company or another individual without authorised permission.
- Sharing IM account passwords with another person or attempting to obtain another person's IM account password. IM accounts must be used by the registered User only.
- Excessive personal use of IM resources.

17.1.4. Confidentiality: The transmission of sensitive corporate information through IM for business purposes is discouraged. Users must not send personal information, confidential matters, and other proprietary information through the corporate IM service.

17.1.5. IM conversations and messages created on the corporate IM service and transmitted through corporate systems are considered the property of AE. Although these conversations are not recorded, AE reserves the right to record, monitor, inspect, copy, review, store and audit IM usage and messages generated by or for the organisation. Users must not have a reasonable expectation of privacy when using corporate IM services.

17.1.6. File sharing: External file sharing through IM services is discouraged. Aldar Education provides other approved means to transfer files such as email, file server shared folder, OneDrive, SharePoint, and the FTP facility.

18. DUE DILIGENCE

18.1. Each User has a responsibility to notify the Aldar Education Service Desk (sd@aldareducation.com) immediately of any evidence or suspicion of any security violation related to:

18.1.1. Unauthorised access to network, telecommunications, or computer systems.

18.1.2. The apparent presence of a virus or malware on a Company issued system.

18.1.3. The apparent presence of any inappropriate material prohibited by this Policy.

18.1.4. Apparent tampering with any file for which a User has established restrictive access controls.

18.1.5. Violation of this Policy or any other information security Policies or Procedures by another User.

18.2. User must prevent unauthorised access, including viewing, to information resources or material in their possession or under their control or custody.

C. DEFINITIONS

Term or Abbreviation	Definition
AE or Company	Refers to Aldar Education including all Aldar Education Operated Schools, Managed Schools, and ATA.
AI	Artificial Intelligence.
ATA	Refers to Aldar Training Academy managed by Aldar Education.
/	It implies ‘or’ and is used to link the alternatives.
CD	Compact Disc.
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.
Digital Safety Package	Refers to security measures and controls designed to ensure the safe and responsible use of digital devices and network of AE.
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	Digital & Technology Services.
DVD	Digital Video Disc.
Employee	Includes temporary, permanent, full-time and part-time employees.
Framework	A specialised type of Policy which contains a logical structure developed to organise other Instruments into a plan, hierarchy, or structure.
FTP	File Transfer Protocol.
Function	An operational area within a Department, as set out in its organisational chart.
GIF	Graphics Interchange Format.
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.
IM	Instant Messaging.
Instrument	A document to provide guidance, impose obligations, define responsibilities or delegate authorities, such as Framework, Policy, SOPs, etc.

Term or Abbreviation	Definition
IP	Internet Protocol is a protocol for sending data across networks using IP addresses.
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.
MDM	Mobile Device Management.
MP3	MPEG audio layer 3 is a digital audio encoding format that utilises data compression to reduce the size of audio files.
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 organisational requirements, and by which AE will be guided in the management of its affairs and the development of its procedures.
Procedure / Standard Operating Procedure (SOP)	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	A series of tasks to be undertaken to carry out operational tasks, 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.
PIN	Personal Identification Number.
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. For AE, this may refer to Employees across AE and its Schools, contractors, students, parents, as well as any other individuals or entities that may use information and information technology resources belonging to AE.
USB	Universal Serial Bus is a common platform that allows communication between devices and a host controller such as a computer.
VBS	Virtual Basic Script.
VOIP	Voice Over IP.

Term or Abbreviation	Definition
VPN	Virtual Private Network.