AUSTRALIAN SCHOOL OF ABU DHABI

DIGITAL POLICY

Contents

1. School Vision 4
2. School Mission 4
3. Introduction 4
4. Purpose 4
5. Scope 5
6. Definitions 5
7. Policy 7

7.1 Required Documentation 7

7.1.1 Digital Strategy 7
7.1.2 Responsible Usage Policies 8
7.1.3 External Provider and Products 8
7.1.4 Data and Cybersecurity Infrastructure 8
7.1.5 Cybersecurity Incident Response 8
7.1.6 Data Protection Policy and Plan 8
7.1.7 Digital and Social Media Policy 8

7.2 Digital Strategy and Oversight 9

7.2.1 Digital Strategy 9
7.2.2 Oversight and Review 9
7.2.3 Liaison With ADEK 10

7.3 Digital Competencies 10

7.3.1 Student Digital Learning Outcomes 10
7.3.2 Staff Digital Capacity And Training 10

7.4 Responsible Usage and Digital Safeguarding 11

7.4.1 Responsible Usage Policy 11
7.4.2 Digital Safeguarding and Student Wellbeing 12
7.4.3 Digital Incidents 13
7.4.4 Parental Responsibilities 13

7.5 Digital Infrastructure 13

7.5.1 Digital Devices 13
7.5.2 Digital Systems for Staff 14
7.5.3 Distance Learning Readiness 14
7.5.4 Assistive Technology 14
7.5.5 External Providers and Products 14

7.6 Data Protection and Cybersecurity 15

7.6.1 Secure Digital IT Architecture 15
7.6.2 System Maintenance 16
7.6.3 Safe Use of External Learning Applications 16
7.6.4 Safe Virtual Interactions with Invited Visitors 16

7.6.5 Backup and Storage 16
7.6.6 Cybersecurity Incidents and Business Continuity 17
7.7 Data Protection 17
7.7.1 Data Protection Policy 17
7.7.2 Data Sharing with ADEK 18
7.7.3 Data Protection Plan 18
7.8 Digital Communications 18
7.8.1 Digital Media Policy 18
7.8.2 Social Media Policy 19
7.8.3 Monitoring and Moderation of School Communications 19
7.8.4 Personal Social Media Accounts for Staff 19
7.8.5 Communication via Email 20
7.8.6 School Website 20
8. Compliance 20
9. References 21
10. Ratification & Revision History 21

1. SCHOOL VISION

Australian School of Abu Dhabi (ASAD) fosters globally minded graduates through inclusive education, nurturing a sense of belonging, understanding, and respect. We empower students with skills, empathy, and awareness to contribute locally and globally.

2. SCHOOL MISSION

Australian School of Abu Dhabi (ASAD) provides a diverse curriculum with global perspectives to all students. We foster inclusion, embrace diversity, promote understanding, and empower students to excel academically and socially. Our commitment to inclusivity ensures every student feels valued and supported.

3. INTRODUCTION

Digital technologies play an integral role in contemporary teaching and learning by enhancing access to information, supporting innovation and enabling collaboration within and beyond the school community. Australian School of Abu Dhabi (ASAD) recognises its responsibility to ensure that digital tools are used effectively, ethically and securely to support student learning, wellbeing and academic integrity.

In alignment with the Abu Dhabi Department of Education and Knowledge (ADEK) *School Digital Policy* framework and relevant UAE regulations, this Digital Policy establishes the principles and expectations governing the use of digital technologies at ASAD. It reflects the school's commitment to embedding digital competence across all areas of teaching and learning, fostering responsible digital citizenship and promoting safe, inclusive and respectful online behaviour.

This policy sets out the minimum requirements for the development and implementation of ASAD's digital strategy, the provision of age-appropriate learning related to digital safety and wellbeing and the secure and responsible use of digital systems, platforms and data. It also clarifies the roles and responsibilities of students, staff, school leadership and the wider school community in maintaining a safe and effective digital learning environment that protects privacy, supports cybersecurity and complies with ADEK requirements, UAE legislation and the expectations of the International Baccalaureate (IB).

Through this policy, ASAD affirms its commitment to preparing students to navigate the digital world with confidence, resilience and integrity, ensuring that digital technologies are used to enhance learning, uphold ethical and academic standards and support the highest expectations of educational practice.

4. PURPOSE

The purpose of this Digital Policy is to:

- Set out the requirements for ASAD to develop, implement and regularly review a comprehensive digital strategy that governs the effective use of technology, defines goals related to digital competencies and infrastructure and ensures appropriate digital security measures and resourcing are in place.
- Ensure that ASAD invests in the development of students' digital skills and competencies to enhance teaching and learning, maximise meaningful learning opportunities, support innovation and prepare students for future education, work and life in an increasingly digital world.
- Ensure that students are educated in the responsible, ethical and safe use of digital technologies and online environments, including the responsible use of digital tools for learning, research and

assessment, while upholding academic integrity and protecting students from digital content, interactions and behaviours that may be inappropriate, harmful or pose risks to their wellbeing.

- Ensure that ASAD establishes and maintains systems, mechanisms and procedures that are safe, balanced and appropriate to safeguard digital security, support cybersecurity and reduce the risk of digital incidents.
- Ensure that ASAD complies with all relevant ADEK requirements and applicable UAE legislation, including the Monitoring and Control Center requirements and Federal Decree Law No. (45) of 2021 on the Protection of Personal Data, in relation to the collection, processing, storage and protection of personal information.

5. SCOPE

This Digital Policy applies to all members of the ASAD school community and governs the use of digital technologies, systems and online environments associated with the school.

The policy applies to students, staff, parents, visitors and external providers and covers the use of ASAD-owned or ASAD-managed digital devices, networks and systems, as well as personal devices used for school-related purposes.

This policy applies to digital activities conducted on school premises, during school-related activities and through authorised off-site or virtual learning environments.

It operates in conjunction with other ASAD policies, including those related to safeguarding, behaviour, staff conduct and use of personal devices and aligns with all relevant ADEK requirements and applicable UAE legislation.

6. DEFINITIONS

TERM	DEFINITION
Additional Learning Needs	Individual requirements for additional support, modifications, or accommodations within a school setting on a permanent or temporary basis in response to a specific context. This applies to any support required by students of determination and those who have special educational needs and/or additional barriers to learning, access, or interaction in that specific context (e.g., dyslexic, hearing or visually impaired, twice exceptional, or gifted and/or talented). For example, a student with restricted mobility may require lesson accommodations to participate in Physical Education and building accommodations to access facilities but may not require any accommodations in assessments. Equally, a student with hearing impairment may require adaptive and assistive technology to access content in class and may also require physical accommodations (e.g., sit in the front of the class to be able to lip read) to access learning.
Assistive Technology	Any item, piece of equipment, software program, or product system that is used to increase, maintain, or improve the functional capabilities of persons with disabilities (ATIA, n.d.).
Bring Your Own Device (BYOD)	Practice wherein schools allow staff and/or students to do their work on personally owned digital devices.

Bullying	Repeated physical, social, or verbal aggression exercised by students who feel they are in a position of power against other students who are perceived weaker or powerless, to achieve specific gains or draw attention, in a way that hurts the student physically and/or emotionally. Bullying can be committed by groups or individuals, in online (cyberbullying) or offline settings. The National Policy for the Prevention of Bullying in Educational Institutions (MoE, n.d.) provides a complete framework for bullying and cyberbullying.
Cyberbullying	Bullying that takes place online "using the means of communication and information technology to insult, use profanity towards, threaten with violence, slander, or blackmail someone" (MoE, 2020). Online bullying can follow the bullied student wherever they go via social networks and mobile phones and has a wider reach than bullying in the real world.
Cybersecurity Incident	A breach that threatens the confidentiality, integrity or availability of an organization's information systems or sensitive data (IBM, n.d.).
Data Protection	The process of safeguarding data from corruption, compromise, unauthorized access, or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable (SNIA, n.d.).
Digital Device	A device used for audio, video, or text communication, or any other type of computer or computer-like instrument, including, but not limited to cell phones, smart watches, tablets, and laptops.
Digital Incident	An instance where a member of the school community engages in the inappropriate use of digital technology. This includes a breach of the reasonable usage policies, the accessing of inappropriate content, inappropriate behaviors or communications, cyberbullying, and/or any other breach of school regulations in an online setting.
Digital Fluency	The state of being a competent, confident, safe, responsible, creative, and curious user of technology.
Documented Learning Plan (DLP)	A plan which outlines any personalized learning targets, modifications to curriculum, additional support, or tools for learning which are agreed by school staff, parents, and students (where appropriate), including Individual Educational Plans (IEP), Individual Support Plans (ISP), Individual Learning Plans (ILP), Behavior Support Plans (BSP), Advanced Learning Plans (ALP), etc. This may be to address any specific identified academic, behavioral, language, or social and emotional need.
Parent	The person legally liable for a child or entrusted with their care, defined as the custodian of the child as per the Federal Decree Law No. 3 of 2016 Concerning Child Rights (Wadeema).
Personal Information	Information relating to individuals who are identifiable directly from the information in question, or who can be indirectly identified from that information in combination with other information.
Risk Assessment	A systematic process of evaluating the potential risks that may be involved in an activity or undertaking.
Safeguarding	Protecting students from the risks of harm, including maltreatment and other types of risks that impact their overall health and development, wellbeing, and safety.

SaaS Security Posture Management (SSPM)	A type of automated security tool for monitoring security risks in software-as-a-service (SaaS) applications. It also identifies misconfigurations, unnecessary user accounts, excessive user permissions, compliance risks, and other cloud security issues.
Social Media	A means of social interaction in which people create, share, and/or exchange information and ideas in virtual communities and networks, including, but not limited to, platforms such as Facebook, Twitter, Instagram, LinkedIn, and YouTube (Tufts University, n.d.).
Visitor	For the purpose of this policy, a visitor is any temporary visitor (e.g., a parent or a relative of a student, prospective student and their parents, inspectors, contractors, etc.) entering the school premises. An invited visitor is anyone visiting the school on a temporary basis to interact with students (i.e., a speaker, career fair representative, etc.) and includes volunteers, who are engaged by an educational institution on a non-remunerated basis to interact with students (e.g., parent chaperones, etc.).

7. POLICY

7.1 Required Documentation

ASAD maintains a structured digital policy framework that governs the safe, effective and ethical use of digital technologies across the school and supports compliance with ADEK requirements, UAE legislation and the school's educational priorities.

The following other documents form part of ASAD's digital governance framework:

1. Digital Strategy
2. ICT Acceptable Use Policies, including the Bring Your Own Device (BYOD) Policy
3. External Digital Providers and Educational Technology Risk Assessment Framework
4. Data & Cybersecurity Infrastructure and Incident Response Plan
5. Information and Data Protection Policy
6. Data Protection Plan
7. Digital and Social Media Policy
8. Privacy Notice

These documents are reviewed on a regular basis to ensure continued alignment with regulatory requirements, technological developments and the needs of the school community.

7.1.1 Digital Strategy

ASAD maintains a documented Digital Strategy that sets out the school's approach to using technology to enhance teaching and learning, support student wellbeing and enable effective school operations. The strategy defines goals related to student digital competencies, staff capability, infrastructure development, cybersecurity and future readiness and is reviewed annually to reflect emerging technologies and evolving school needs.

7.1.2 Responsible Usage Policies

ASAD implements ICT Acceptable Use and BYOD Policy for students, staff and parents that define expectations for the appropriate use of digital devices, systems and online platforms. These policies address safe and ethical online behaviour, academic integrity, responsible use of digital tools for learning and assessment and the appropriate use of artificial intelligence and copyrighted materials.

Age-appropriate guidance is provided to students, with full versions of the policies available to staff and parents.

7.1.3 External Provider and Products

ASAD applies a structured framework for the selection, approval and review of external digital service providers and educational technology products. This framework ensures that approved providers meet ASAD's requirements for data protection, cybersecurity, educational value, age-appropriateness and compliance with UAE laws and ADEK regulations.

7.1.4 Data and Cybersecurity Infrastructure

ASAD operates a secure digital infrastructure designed to protect school systems, data and users. This includes defined access controls, network security measures, device management protocols and ongoing monitoring to maintain system reliability and security.

7.1.5 Cybersecurity Incident Response Plan

ASAD maintains a Cybersecurity Incident Response Plan that outlines procedures for identifying, reporting and managing digital security incidents. The plan defines roles, escalation pathways and reporting requirements, including communication with ADEK where required.

7.1.6 Data Protection Policy and Plan

ASAD maintains a Data Protection Policy and Data Protection Plan that govern the collection, processing, storage and sharing of personal data. These documents support compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data and define consent processes, data security measures and procedures for responding to data breaches.

7.1.7 Digital and Social Media Policy

ASAD maintains a Digital and Social Media Policy that regulates the creation, use and publication of digital content involving the school community. This policy ensures that appropriate consent is obtained, content reflects UAE cultural values and school expectations and digital communication is managed responsibly and professionally.

7.2 Digital Strategy and Oversight

7.2.1 Digital Strategy

ASAD maintains a documented Digital Strategy that provides a clear rationale for the school's use of technology to support student achievement, enhance teaching and learning and enable the effective operation of the school.

The Digital Strategy sets out ASAD's strategic direction for the use of digital technologies and includes:

- The purposeful deployment of technology to enhance teaching and learning, support effective assessment and feedback and promote student engagement and collaboration.
- Consideration of assistive and adaptive technologies to support inclusion and equitable access to learning for all students.
- Defined goals related to the development of students' digital skills and competencies across year levels.
- Planning for the development, procurement and implementation of digital infrastructure, software and hardware.
- Measures to support the security, reliability and resilience of the school's digital systems.
- Consideration of sustainability and future readiness in relation to digital infrastructure and emerging technologies.
- Identification of resources and investment required to support the effective delivery of the Digital Strategy.
- Staff professional learning priorities related to digital teaching practices, cybersecurity and the ethical use of technology.
- Increased awareness and understanding of emerging technologies, including artificial intelligence, and their appropriate and responsible use in teaching, learning and assessment.

The Digital Strategy is reviewed on a regular basis to ensure continued alignment with school priorities, regulatory requirements and technological developments.

7.2.2 Oversight and Review

Oversight of ASAD's Digital Strategy and associated digital policies, including their implementation, is provided through school leadership and a designated lead staff member with responsibility for digital learning, wellbeing and information technology.

This oversight supports the consistent and effective implementation of the Digital Strategy and includes:

- Monitoring progress in relation to student digital competencies and learning outcomes.
- Monitoring progress against digital development and procurement plans to ensure alignment with school priorities and available resources.
- Evaluating the suitability, effectiveness and educational value of digital tools, software and online platforms used across the school.
- Reviewing the security, resilience and fitness for purpose of digital systems and infrastructure, including backup and recovery processes.

- Conducting risk assessments of ASAD's digital systems and infrastructure, including where appropriate testing of controls and recovery processes, to confirm that systems remain secure and fit for purpose.
- Reviewing the effectiveness of data protection and cybersecurity measures.
- Considering feedback from staff, students and parents to inform digital development and procurement decisions.
- Identifying staff professional learning needs related to digital technologies, digital safety and emerging tools.

Where required, ASAD reviews and updates related policies and procedures to ensure ongoing alignment with ADEK requirements and UAE legislation.

7.2.3 Liaison with ADEK

ASAD designates an appropriate staff member to liaise with the Abu Dhabi Department of Education and Knowledge (ADEK) in relation to matters of digital competency, digital safety and cybersecurity, ensuring effective communication and compliance with regulatory requirements.

7.3 Digital Competencies

7.3.1 Student Digital Learning Outcomes

ASAD defines clear digital competencies and expected learning outcomes for students across year levels and integrates these within the school's curriculum and teaching practices. These competencies support students in developing the knowledge, skills and behaviours required to use digital technologies confidently, responsibly and effectively for learning.

Student digital competencies at ASAD include, but are not limited to:

- Digital literacy skills, including effective online research, evaluation of digital information and responsible communication.
- The ethical and responsible use of digital tools for learning, research and assessment, including an understanding of academic integrity and appropriate use of artificial intelligence.
- The ability to collaborate, create and problem-solve using digital technologies in age-appropriate and meaningful ways.
- Awareness of digital safety, wellbeing and responsible online behaviour.

ASAD ensures that appropriate digital infrastructure, systems and learning resources are in place to support students in achieving these outcomes. This includes consideration of assistive and adaptive technologies to support students with additional learning needs, in line with the ADEK *School Inclusion Policy* and the school's inclusive education practices.

7.3.2 Staff Digital Capacity and Training

ASAD supports staff to develop and maintain the digital knowledge and skills required to promote the objectives of this policy and to effectively support student learning in a digital environment. Staff training and professional learning at ASAD are aligned with staff roles and responsibilities and include:

- Familiarisation with the school's digital infrastructure, systems and relevant digital policies.

- Understanding of student digital learning outcomes and how digital competencies are embedded within teaching and learning.
- Guidance on data protection, cybersecurity and safeguarding responsibilities.
- Awareness of digital safety measures and responsible use expectations for staff and students.
- Consideration of emerging technologies, including artificial intelligence, and their ethical and appropriate use in educational contexts.

Professional learning opportunities are reviewed on a regular basis to ensure they remain relevant to evolving technologies, regulatory requirements and the needs of the school community.

7.4 Responsible Usage and Digital Safeguarding

7.4.1 Responsible Usage Policy

ASAD maintains and communicates an ICT Acceptable Use and BYOD Policy for students, staff, parents and visitors that define expectations for the appropriate, safe and ethical use of digital technologies.

These policies apply to the use of digital devices, networks, systems, software and online platforms on school premises, through ASAD-managed systems and during school-related activities, including off-site and virtual learning contexts.

Responsible usage at ASAD includes:

- The appropriate use of school-issued digital devices, shared devices, school networks, software and online services in ways that support learning, wellbeing and school operations.
- Compliance with expectations for the care, security and responsible handling of school-owned digital equipment.

Rules relating to personal devices, including Bring Your Own Device (BYOD), are clearly defined and include:

- Conditions under which personal devices may be used on the school network and on school premises.
- Expectations for the use of personal devices during school-related activities conducted off-site, such as excursions and field trips.
- Restrictions on activities that compromise digital safety, learning or wellbeing.
- Prohibition of the use of Virtual Private Networks (VPNs) on any device on school premises or through school networks, without exception, including for educational or administrative purposes.

Standards relating to digital conduct and security at ASAD include:

- Expectations for the use of personal social media accounts by staff, including professional boundaries, safeguarding considerations and restrictions on interaction with students, in line with the school's Digital and Social Media Policy.
- Requirements for the secure creation, use and protection of passwords for school accounts, including restrictions on password sharing.

- Standards governing the sharing, storage and transmission of school-related data, including student and staff information, and the approved channels through which such data may be shared when permitted.
- Requirements relating to the use of external applications, platforms and learning tools, including restrictions on uploading student data without appropriate approval and safeguards in place.

Responsible usage policies at ASAD explicitly address:

- Academic honesty and integrity in digital contexts, including expectations related to plagiarism, appropriate referencing and original work.
- The responsible and ethical use of copyrighted material, digital content and online resources, in accordance with Federal Decree Law No. (38) of 2021 on Copyrights and Related Rights.
- The appropriate use of digital tools, including artificial intelligence, for learning, research and assessment, in alignment with school expectations and regulatory requirements.

Responsible Usage Policies are communicated to students, staff, parents and visitors through appropriate channels. Policies applicable to students and parents are published on the school website and included in the Parent Handbook, in line with the ADEK *School Parent Engagement Policy.*

Age-appropriate versions of the ICT Acceptable Use and BYOD Policy are provided to students up to Grade 6 / Year 7, with full versions made available to parents and staff.

7.4.2 Digital Safeguarding and Student Wellbeing

ASAD implements education programs, systems and procedures designed to protect students from online risks and to promote safe, balanced and responsible engagement with digital technologies.

Online risks addressed by ASAD include:

- Exposure to content that is inappropriate, illegal or harmful to student wellbeing.
- Unsafe online interactions, including engagement with unknown users or fake profiles.
- Harmful online behaviours, including cyberbullying and misuse of digital communication tools.
- Financial and scam-related risks, including phishing, gambling and fraudulent activity.

To safeguard students and promote digital wellbeing, ASAD implements the following measures:

- Age-appropriate digital safety and awareness programs for all students that address the benefits of technology, identification of online risks, self-assessment of digital behaviour, online safety strategies and the impact of digital habits on wellbeing.
- Filtering and monitoring systems to supervise student internet use on school-managed devices and networks.
- Regular review and analysis of internet usage data and filtering alerts to identify potential concerns or adverse trends.
- Procedures to identify and support students who may be developing risky, excessive or harmful digital behaviours, including digital dependency or engagement in illegal online activities, in alignment with the ADEK *School Student Mental Health Policy* and the ADEK *School Student Behaviour Policy.*
- Safeguarding mechanisms for virtual learning and online activities, including controls to manage communication features and reduce safeguarding risks.

ASAD ensures that student access to the internet during school hours is purposeful and linked to defined educational outcomes.

7.4.3 Digital Incidents

A digital incident at ASAD occurs when a member of the school community engages in inappropriate or unsafe use of digital technologies. This includes breaches of the ICT Acceptable Use and BYOD Policy, access to inappropriate content, harmful online behaviour, cyberbullying or other violations of school rules in digital environments.

When a digital incident occurs within contexts covered by this policy, ASAD responds in accordance with relevant school policies and ADEK requirements. Responses may include intervention, support and follow-up actions involving students, staff and parents, as appropriate.

Where required, ASAD reports digital incidents to ADEK and cooperates with relevant authorities, including the Abu Dhabi Police, in line with regulatory expectations. All digital incidents are recorded, documented and reviewed, with records signed by the Principal and securely stored for auditing purposes, in accordance with the ADEK *School Records Policy.*

7.4.4 Parental Responsibilities

ASAD recognises the important role of parents and guardians in supporting safe and responsible digital behaviour.
Parents are expected to monitor and guide their child's use of digital devices and online services outside school premises and school hours to promote safe, balanced and appropriate digital engagement.

7.5 Digital Infrastructure

7.5.1 Digital Devices

ASAD operates a Bring Your Own Device (BYOD) framework for students and staff, under which personal devices are used to access school networks, systems and digital learning platforms.

ASAD defines and communicates digital safety and security requirements for personal devices used for school-related purposes. These requirements include, where applicable:

- Minimum device and operating system specifications to ensure compatibility with school systems.
- Expectations for the use of appropriate security measures, including antivirus and device protection software.
- Responsible use expectations to safeguard devices, data and access credentials.

In addition to BYOD, ASAD provides shared digital devices and fixed computing resources on school premises, including computer laboratories and other school-managed equipment. These devices are configured with appropriate security controls and are managed in line with the school's digital safety, data protection and cybersecurity requirements.

7.5.2 Digital Systems for Staff

ASAD ensures that relevant staff have access to required digital systems to support teaching, learning and school operations. This includes access to systems provided or required by ADEK, as well as school-approved platforms used for learning management, administration and communication.

Access to staff digital systems is role-based and managed in line with ASAD's data protection and cybersecurity requirements.

7.5.3 Distance Learning Readiness

ASAD maintains arrangements to support distance learning where required, including during emergency situations such as temporary school closures or to support individual students in exceptional circumstances, such as prolonged medical absence or emergency travel.

Distance learning arrangements are implemented in a manner that prioritises continuity of learning, safeguarding, accessibility and data security.

7.5.4 Assistive Technology

ASAD provides assistive and adaptive technologies to support students with additional learning needs, as identified in their Documented Learning Plans (DLP).

The selection and use of assistive technology align with the ADEK *School Inclusion Policy* and support equitable access to learning, participation and assessment for all students.

7.5.5 External Providers and Products

ASAD applies a structured third-party risk assessment framework when selecting and approving external digital service providers and products, including learning applications, system providers and open-source tools.

This framework considers, where applicable:

- Compatibility with existing school systems and infrastructure.
- Secure management, storage and processing of data.
- Compliance with cybersecurity standards and protection against cyber threats.
- Service reliability, continuity and backup or recovery provisions.
- The reputation, capability and financial stability of the provider.
- Compliance with Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and ADEK requirements relating to data privacy, copyright and information use.
- Educational value, quality and age-appropriateness of content, where relevant.

ASAD communicates relevant data protection, privacy and cybersecurity obligations to external providers and ensures that approved vendors understand their responsibilities in relation to the collection, use and protection of school and student data.

7.6 Data Protection and Cybersecurity

7.6.1 Secure Digital IT Architecture

ASAD maintains a secure digital IT architecture designed to protect school systems, data and users from unauthorised access, data loss and cyber threats. Appropriate cybersecurity controls are implemented across digital systems in line with ADEK requirements and applicable UAE legislation.

Key elements of ASAD's secure digital architecture include:

Access Control

- Access to digital systems is controlled through defined authentication measures for critical services.
- Role-based access controls are applied to ensure users have permissions appropriate to their role and responsibilities.

Data Encryption

- Measures are in place to protect sensitive data through encryption or equivalent safeguards for data in transit and at rest, where applicable.

Network Security

- Network security controls are implemented to protect against unauthorised access and cyber threats.
- Web filtering measures are applied to restrict access to inappropriate content and support safeguarding requirements.
- Systems are in place to identify potentially compromised or infected devices on the school network.
- Network activity is monitored to detect unusual or potentially harmful patterns of use.

Endpoint Protection

- School-managed devices are protected through appropriate security software and regular system updates.
- Security patching and device protection measures are applied to reduce vulnerability to known threats.

Data Backup and Recovery

- Backup procedures are in place for critical school data and systems.
- Backup arrangements support data recovery and continuity of operations in the event of system failure or security incidents.

Data Security

- Data handling practices reflect defined controls for different types of school and student data.
- Measures are in place to reduce the risk of unauthorised data loss or disclosure.

Security Awareness

- Staff and students receive guidance and awareness relating to cybersecurity risks, safe digital behaviour and protection of information.

Incident Response

- ASAD maintains an incident response approach to support timely identification, escalation and management of cybersecurity incidents.

Physical Security

- Physical access to critical IT infrastructure, including servers and networking equipment where applicable, is restricted and managed.

Regulatory Compliance

- Digital systems and practices align with UAE data protection, cybersecurity and information security requirements.

Monitoring and Logging

- Monitoring mechanisms are used to support the detection and investigation of potential security incidents.
- Logs are maintained where appropriate to support review and auditing processes.

Secure Software and Systems

- Security considerations are applied when developing, configuring or procuring digital systems and software.
- Software and systems are updated as required to address security vulnerabilities.

Cloud and Collaboration Security

- Where cloud-based or collaboration platforms are used, appropriate security and access controls are applied.
- Integration with identity and access management systems is implemented where available.

Third-Party Security

- External service providers are subject to security and data protection requirements as part of ASAD's third-party risk management processes.

7.6.2 System Maintenance

ASAD maintains digital infrastructure, operating systems, security tools and software through regular updates and maintenance activities. Digital systems are reviewed and tested to ensure they remain operational, secure and fit for purpose.

7.6.3 Safe Use of External Learning Applications

ASAD implements safeguarding and security measures to protect students and school systems when using external learning applications and platforms.

Where applicable, measures such as controlled access, single sign-on or equivalent authentication mechanisms are used to support secure and appropriate access to approved learning applications.

7.6.4 Safe Virtual Interactions with Invited Visitors

ASAD seeks parental consent for live virtual interactions involving invited visitors, whether conducted within or outside the classroom environment.

Such interactions are approved and managed in accordance with ADEK requirements, including the ADEK *School Extracurricular Activities and Events Policy* and the ADEK *School Student Protection Policy*, to ensure safeguarding and student wellbeing.

7.6.5 Backup and Storage

ASAD ensures that backups of important data, systems and configuration settings are maintained in line with the ADEK *School Records Policy*.

Where on-site storage systems are used, backups are stored securely and separately from the main school network. Where cloud-based storage systems are used, data synchronisation and backup arrangements support data availability and recovery.

7.6.6 Cybersecurity Incidents and Business Continuity

ASAD maintains response and business continuity arrangements to guide staff in the event of a cybersecurity incident. These arrangements outline procedures for internal reporting, escalation to school leadership and notification to ADEK where required.

Communication relating to cybersecurity incidents is limited to relevant service providers and ADEK, in line with regulatory expectations.

ASAD adheres to all applicable UAE laws and directives relating to cybersecurity and digital conduct, including Federal Decree Law No. (34) of 2021 on Combatting Rumours and Cybercrimes and guidance issued by relevant authorities.

7.7 Data Protection

7.7.1 Data Protection Policy

ASAD maintains a Data Protection Policy that sets out how personal information is collected, processed, stored, shared and protected in a secure and lawful manner. The policy supports compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data and relevant ADEK requirements.

The Data Protection Policy specifies:

- The types of personal information that may be collected by the school, including student, parent, staff and visitor data, and the purposes for which such data is collected.
- The requirement for consent in the collection, processing and storage of personal information, where applicable.
- Procedures for obtaining consent that ensure it is freely given, specific, informed and unambiguous.
- The right of individuals to withdraw consent at any time, in accordance with applicable legal requirements.

The policy also defines the conditions under which personal information may be shared with other parties, including regulatory authorities and service providers, and the safeguards that apply to such sharing.

Where personal data is shared with third parties, ASAD ensures that appropriate contractual and confidentiality provisions are in place. International transfers (including cloud hosting or remote access from outside the UAE) will only occur where permitted under UAE data protection law and ADEK requirements, and where the school has implemented appropriate safeguards and approvals (including any approvals or notifications required by ADEK).

7.7.2 Data Sharing with ADEK

ASAD provides accurate and up-to-date data to authorised ADEK personnel when requested, in accordance with Federal Decree Law No. (18) of 2020 on Private Education and its amendments, Law No. (9) of 2018 concerning the establishment of the Department of Education and Knowledge and ADEK's terms and conditions relating to data privacy and information sharing.
Parents are informed of the school's obligations to share relevant data with ADEK as part of regulatory compliance and school operations.

7.7.3 Data Protection Plan

ASAD maintains a Data Protection Plan that outlines the measures in place to safeguard organisational, student and staff data. The plan is reviewed on an annual basis and aligns with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data and the ADEK *School Records Policy.*

The Data Protection Plan addresses:

- Data classification practices to identify and manage different categories of information.
- Defined authorisation levels to control access to personal and sensitive data.
- Measures to protect data against cybersecurity risks, unauthorised access and other threats.
- Procedures for data backup, retention and secure storage.
- Processes for restoring data and maintaining continuity in the event of data loss, breaches or system failures.

The Data Protection Plan operates in conjunction with ASAD's cybersecurity and incident response arrangements to ensure a coordinated and effective approach to data protection. Detailed requirements relating to acceptable and responsible use of digital technologies, digital media, social media use, email communication and website content are set out in Section 7. 8: Digital Communications and associated policies.

7.8 Digital Communications

7.8.1 Digital Media Policy

ASAD maintains a Digital and Social Media Policy that governs the creation, use, storage and publication of digital media involving members of the school community. The Digital and Social Media Policy provides detailed operational requirements governing consent, content creation, publication, moderation and professional conduct in digital communication contexts.

The policy defines requirements for the recording and publication of photographs, video recordings and other digital media and includes:

- The requirement to obtain written parental consent before taking photographs or video recordings of students.
- Clear communication to parents regarding the purposes for which digital media involving students is collected or used.
- The requirement to obtain written parental consent prior to publishing digital media involving students. Where applicable, consent processes specify whether a student may be identified by name in published content.

- Procedures for the provision, management and withdrawal of consent in relation to digital media.
- Conditions governing the secure storage, retention and protection of digital media.
- Conditions relating to the use of personal devices and personal accounts for recording or publishing school-related digital content.

The Digital and Social Media Policy operates in alignment with ASAD's data protection, safeguarding and cultural expectations.

7.8.2 Social Media Policy

ASAD maintains a Digital and Social Media Policy governing the use of social media by the school and the management of official school social media accounts.

The policy defines:

- Approved social media platforms and official accounts used by ASAD.
- Access, security and password protection arrangements for school-managed social media accounts.
- Expectations for content, language use and engagement with other accounts to ensure communications are respectful, accurate and appropriate.
- Conditions relating to the use of student names, photographs and video recordings, in alignment with the Digital and Social Media Policy and parental consent requirements.
- Procedures for moderating third-party content posted on school social media pages, including the management of inappropriate, disrespectful or harmful content.
- Procedures for responding to adverse social media activity, including impersonation or misuse of the school's identity or branding.

7.8.3 Monitoring and Moderation of School Communications

ASAD monitors official school communication channels, including newsletters, website content, social media platforms and other school-related communication spaces, to ensure compliance with this policy and relevant ADEK requirements.

ASAD designates moderators to manage school social media platforms, where applicable. Moderators are responsible for reviewing, approving or removing third-party content in line with school guidelines. Content that is inappropriate, inconsistent with UAE cultural values or that constitutes bullying, harassment, discrimination or intimidation is managed in accordance with the ADEK *School Values and Ethics Policy* and the ADEK *School Cultural Consideration Policy.*

7.8.4 Personal Social Media Accounts for Staff

ASAD recognises staff members' right to maintain personal social media accounts. Expectations relating to such accounts are defined to safeguard students, staff and the school.

Staff members are expected to:

- Not use school-issued email addresses to create personal social media accounts.
- Apply the highest possible privacy settings on personal social media accounts.

- Not identify themselves as being associated with ASAD on personal social media accounts, except on professional platforms such as LinkedIn.
- Not accept or send friend, connection or follow requests involving current students or former students under the age of 18.
- Not accept friend, connection or follow requests from current students and parents of current students.
- Not use personal social media accounts or messaging applications to communicate with current students, parents or former students under the age of 18.
- Assume that content shared through personal accounts may be publicly visible and exercise appropriate professional judgement.
- Ensure that content shared is appropriate, culturally respectful and does not constitute bullying, harassment, discrimination or intimidation.
- Ensure that content shared does not give the impression of being endorsed by ASAD.
- Not share confidential or sensitive school-related information through personal social media accounts.

7.8.5 Communication via Email

ASAD requires staff to use school-issued email accounts for all professional communication with students and parents.

Personal email addresses are not used for communication with students or parents in relation to school matters.

7.8.6 School Website

ASAD maintains an official school website that serves as a key source of information for the school community.

The website is kept up to date and includes, at a minimum:

- School contact information.
- Information about services provided by the school.
- Fees, including transportation fees and fees for optional activities.
- School inspection reports.
- Aggregate student achievement data or individual achievements, where applicable and with appropriate consent.
- Public versions of the annual report, in line with the ADEK *School Reporting Policy.*
- School policies relevant to parents and students.
- Any additional content required under ADEK policies.

ASAD ensures that website content is accurate, appropriate and aligned with the ADEK *School Values and Ethics Policy* and *digital media policy* requirements.

8. COMPLIANCE

ASAD is committed to ensuring that the use of digital technologies across the school complies with all applicable regulatory, legal and policy requirements. This Digital Policy aligns with ADEK requirements and

relevant UAE legislation and is implemented in conjunction with other ASAD policies and procedures relating to safeguarding, inclusion, wellbeing, behaviour, data protection, cybersecurity and records management. Compliance with this policy is mandatory for all members of the ASAD community, including students, staff, parents, visitors and external service providers where applicable.

Any failure to comply with the requirements of this policy is addressed in accordance with relevant ASAD policies and procedures and, where applicable, regulatory expectations.

This policy is reviewed on a regular basis to ensure it remains compliant, effective and responsive to changes in regulatory requirements, technological developments and identified risks. Approved updates are communicated to the school community through official channels.

9. REFERENCES

- Abu Dhabi Department of Education and Knowledge (ADEK). 2024 (September) ADEK_School_Digital Policy_v.1.1
- Abu Dhabi Department of Education and Knowledge (ADEK). 2026 (July) ADEK_AI and Technology Policy
-
- Abu Dhabi Department of Education and Knowledge (ADEK). (n.d.). Terms of Condition of Use, and Privacy Statement for Information.
- Assistive Technology Industry Association (ATIA). (n.d.). What is AT?
- Federal Decree Law No. (3) of 2016 Concerning Child Rights (Wadeema).
- Federal Decree Law No. (18) of 2020 on Private Education and its amendments.
- Federal Decree Law No. (31) of 2021 Promulgating the Crimes and Penalties and its amendments.
- Federal Decree Law No. (34) of 2021 on Combatting Rumors and Cybercrimes.
- Federal Decree Law No. (38) of 2021 on Copyrights and Related Rights.
- Federal Decree Law No. (45) of 2021 on the Protection of Personal Data.
- IBM. (n.d.). What is Incident Response?
- Law No. (9) of 2018 Concerning the Establishment of the Department of Education and Knowledge.
- Ministry of Education (MoE). (2020). Student Behaviour Management Distance Learning.
- Ministry of Education (MoE). (2022). Code of Conduct for Professionals in General Education.
- Ministry of Education (MoE). (n.d.). National Policy for the Prevention of Bullying in Educational Institutions.
- Storage Networking Industry Association (SNIA). (n.d.). What is Data Protection?
- Tufts University. (n.d.). Social Media Overview.

10. RATIFICATION & REVISION HISTORY

Document Title	Digital Policy
Version	v.2
Ratification Date	5th November 2026
Next Review Date	November 2028
Ratified By	Director: Mr. Adel Salman