SCHOOL DIGITAL POLICY

Introduced:	December 2015
Review 1:	December 2021
Review 2:	December 2023
Review 3:	July 2024
Review 4:	December 2025
Next review:	July 2026

1. Introduction

Dunes International School recognizes the critical role of digital literacy, safety, and responsible technology use in preparing students for success in an increasingly digital world. In alignment with the ADEK School Digital Policy, the school commits to embedding digital skills across all aspects of teaching, learning, and school operations while ensuring the highest standards of digital safety, data protection, cybersecurity, and responsible use. This policy outlines the school's systems, procedures, and expectations for the safe, secure, and effective use of digital tools by students, staff, parents, and visitors.

2. Purpose of the Policy

This Digital Policy aims to:

- Establish a comprehensive digital strategy for the effective and secure use of technology across the school.
- Enhance students' digital competencies and overall digital fluency.
- Ensure the safe, ethical, and responsible use of digital technologies.
- Protect students and the school community from online risks.
- Ensure compliance with ADEK regulations, UAE Federal Laws, and international best practices regarding data protection and cybersecurity.

3. Required Documentation

Dunes International School will maintain and publish the following documents on our school website to comply with ADEK:

- Digital strategy (see Section 3.1 Digital Strategy).
- Responsible usage policies (see Section 4.1 Responsible Usage Policies).
- Framework for the selection of external providers and products (see Section 5.4 External Providers and Products).
- Data and Cyber security (see Section 6.1 Secure Digital IT Architecture).
- Response plan in relation to cyber security incidents (see Section 6.6 Cybersecurity Incidents).
- School data protection plan and policy (see Section 7. Data Protection).
- Digital media policy and social media policy (see Section 8. Digital Communications)

4. Digital Strategy and Oversight

4.1 Digital Strategy

A comprehensive digital strategy has been drafted and adopted, clearly outlining the institution's long-term digital vision and providing a strong rationale for its digital goals over a five-year period. The strategy shall include:

- Defines how technology will be used to improve student learning and support efficient school operations.
- Outlines the school's approach to providing assistive technologies that promote inclusion.
- Set goals for developing students' digital skills and competencies.
- Guides to the selection, development, and implementation of digital infrastructure, software, and hardware.
- Establish measures to ensure the security and protection of all digital systems.
- Specifies training requirements to build staff digital capacity.
- Promotes awareness and responsible use of emerging technologies, including Artificial Intelligence.

4.2 Oversight

The Lead shall have the following responsibilities in relation to oversight of the school's digital strategy and associated policies:

- Develop and implement the school's digital strategy.
- Conduct an annual review of the digital strategy and its implementation.
- Monitor progress against student learning goals and school development and procurement plans.
- Evaluate technology, software, and online platforms to ensure that they meet the objectives of the strategy.
- Test and conduct risk assessments of the school's digital systems and infrastructure (e.g., backup recovery) to ensure that they are secure and fit for purposes.
- Review the effectiveness of the school's data and cybersecurity provisions.
- Re-evaluate the technological needs of the school based on feedback from staff, parents, and students, and plan procurement and digital development accordingly.
- Re-evaluate staff digital development needs and identify additional training required. Develop and implement and review other school policies required to be created in line with this policy. Engage with relevant stakeholders to inform them of their decisions.

5. Digital Competencies

5.1 Student Outcomes:

Our school clearly defines digital competencies and expected outcomes for students by grade/year and integrates these into the school's curriculum. Ensure that they have the appropriate digital infrastructure and resources in place to support students in achieving these outcomes, including students with additional learning needs, in line with the ADEK Inclusion Policy.

5.2 Staff Training:

We provide relevant training for staff in line with their designation to enable them to promote the objectives of this policy. The training shall cover topics such as the school's digital infrastructure and policies, student digital learning outcomes, data protection, cyber security, and the digital safety measures implemented by the school.

4. Responsible Usage and Digital Safeguarding

4.1 Responsible Usage Policies: Develop and communicate responsible digital usage policies for students, parents, staff, and visitors.
These policies shall set out what these groups are permitted/prohibited to do on the school's premises, network, and systems, and include:

- The definition of responsible usage of school software, network, services, and digital devices issued by the school, including shared devices.
- Rules on the permitted and restricted use of personal devices on the school network and school premises, and during extracurricular activities that take place outside school (e.g., field trips). Restrict the use of Virtual Private Networks (VPNs) by students on school premises or through school networks unless explicitly authorized for specific educational or administrative purposes.
- Standards in relation to the use of personal social media accounts by staff (see Section 8.3. Personal Social Media Accounts for Staff).
- The school's rules in relation to the setting and sharing of passwords for school accounts.
- Standards in relation to the sharing of data related to the school or school community, and the channels via which such data can be shared when permitted. This includes standards related to the uploading of student data on external applications and learning tools, where applicable.
- Standards in relation to academic honesty, plagiarism, and the responsible use of copyrighted material and digital tools (e.g., artificial intelligence), in line with the Federal Decree-Law No. (38) of 2021 on Copyrights and Neighboring Rights and the ADEK terms and conditions, copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.
- Communicate the relevant responsible usage policies to students, parents, staff, and visitors via appropriate channels.
- Publish responsible usage policies applicable to students and parents on the school website and in the Parent Handbook, as per the Parent Engagement Policy.
- For all younger students up to Grade 6/Year 7, school shall provide age-appropriate versions of the policy to students, and a full version of the policy to parents.

4.2 Safeguarding Students:

Provide educational programs and maintain effective systems to protect our students from the online risks listed below.

- Exposure to content that is inappropriate, illegal, or may harm their wellbeing. Exposure to unsafe online interaction (e.g., interaction with users with fake profiles). Personal online behavior can lead to harm for self or others (e.g., engaging in cyberbullying).
- Scams and finance-related risks such as gambling and phishing. Organize the following programs, systems, mechanisms, and procedures to safeguard students against online risks and promote their wellbeing.
- An age-appropriate awareness program for all students, covering the benefits of technology, awareness of online risks, self-assessment of online risks when using technology, online safety measures, and the impact of digital habits on
- Wellbeing (e.g., the impact of duration of usage of digital devices). Appropriate filtering and monitoring systems to monitor student internet use on school devices and systems.
- Regular analysis of students' internet usage and web filter violations to identify potential adverse trends or problems.
- Procedures to identify and support students who appear to be developing risky, excessive, or illegal digital habits, such as digital addiction or gambling, in line with the Student Mental Health Policy and the Student Behavior Policy.
- Mechanisms to enable safeguarding during activities conducted virtually (e.g., disabling private chat for students).
- School shall ensure there is a developmental purpose before allowing students to use the Internet during school hours.

4.3 Digital Incidents:

1. A digital incident occurs when a member of the school community engages in inappropriate use of digital technology. This includes a breach of reasonable usage policies, the accessing of inappropriate content, inappropriate behaviors or communications, cyberbullying, or any other breach of school regulations in an online setting.

2. Where a digital incident occurs during school hours or in settings covered in school digital policies and make interventions and provide support to students and/or staff in line with the relevant policy (e.g., ADEK Employment Policy, Staff Wellbeing Policy, Student Administrative Affairs Policy, Parent Engagement Policy, Student Behavior Policy, and the Student Protection Policy). Where required, the school shall report digital incidents to ADEK and cooperate with the Abu Dhabi Police for investigations.

3. We ensure that every digital incident is recorded, documented, and signed by the principal, and stored securely for auditing purposes in accordance with our Records Policy.

4. We require parents to monitor their children's use of digital devices outside school hours and premises to support safe and responsible digital behavior.

5. Digital Infrastructure

5.1 Digital Devices: We ensure that digital devices issued to members of the school community have appropriate security features. Where a school allows staff to access school related data or systems on other devices or has a Bring Your Own Device (BYOD) policy for staff or students, the school shall define and implement digital safety precautions (e.g., minimum device specification, and antivirus requirements).

5.2 Digital Systems for Staff: Ensure that relevant staff members have access to digital systems provided by ADEK, including the Learning Management System.

5.3 Distance Learning Readiness: To ensure uninterrupted learning during **emergency situations**, including temporary school closures, public health crises, environmental emergencies, or **individual student circumstances** such as extended medical leave, travel, or hospital stays. This plan outlines the school's readiness to provide high-quality **distance learning through Microsoft Teams**.

5.3.1 Platform for Delivery: Microsoft Teams

Microsoft Teams is the school's official platform for online learning. It enables:

- Live Interactive Classes
- Assignment Management
- Digital Resources & Content Repository
- Communication Tools - Notifications through Teams mobile app

5.3.2 Teacher Readiness & Training

Teachers receive continuous training on:

- Creating and managing Teams Classrooms
- Delivering live lessons effectively
- Using Teams Assignments & Class Notebook
- Digital assessment tools (Forms quizzes, rubrics)
- Supporting SEN students through differentiated digital resources
- Microsoft Teams User guide for teachers

5.3.3 Student Readiness

Students are trained in:

- Joining online sessions
- Submitting assignments
- Using digital tools (OneNote, Forms, Whiteboard)
- Online behavior expectations & digital citizenship

5.3.4 Parent Support

- Guides shared for accessing Teams via mobile/laptop
- Clear communication on distance learning routines
- Dedicated helpline for technical support during emergencies

5.4 Assistive Technology: Provide assistive technology to students with additional learning needs as indicated in their Documented Learning Plan, in line with the Inclusion Policy.

5.5 External Providers and Products:

1. Develop a third-party risk assessment framework for selecting external IT service providers and products related to the school network, system, and infrastructure, including learning application providers and open-source applications.
2. This framework shall include the following, at a minimum:
   a) Compatibility with existing school systems.
   b) Secure management of data.
   c) Compliance with cybersecurity standards and frameworks.
   d) Security against cyber threats.
   e) Service delivery and backup/ recovery provisions.
   f) Reputation and financial stability of the provider.

6. Data and Cybersecurity

6.1 Secure Digital IT Architecture: School shall establish a robust secure digital infrastructure and ensure the relevant cybersecurity controls are implemented as follows:

1**. Access Control**

a. Implement multi-factor authentication mechanisms across critical services.
b. Define and enforce role-based access control to ensure users have appropriate permissions.

2**. Data Encryption**

a. Employ encryption for data in transit and at rest to safeguard sensitive information.

3. **Network Security**
   a. Deploy next-generation firewalls and intrusion detection/prevention systems to protect against unauthorized access.
   b. Ensure web filtering policies are enforced.
   c. Ensure the ability to block inappropriate content.
   d. Ability to detect infected machines across the school network.
   e. Ensure identity-based firewalls are implemented to provide granular visibility on user browsing activity.
   f. Established a unified security edge architecture for all internet browsing.
   g. Regularly monitor and audit network traffic for unusual patterns.
4. **Endpoint Protection**
   a. Install and update anti-virus/ anti-malware software on all managed school devices.
   b. Implement hard disk device encryption and ensure regular security patching.
5. **Data Backup and Recovery**
   Establish automated regular backup procedures for critical data. Ensure backups are vaulted and stored offline. Develop a robust disaster recovery plan to minimize downtime in case of a security incident.
6. **Data Security**
   a. Establish data classification controls across school and student data.
   b. Implement Data Loss Prevention Tools to ensure data leaks or exfiltration is prevented.
7. **Security Awareness Training**
   a. Conduct regular training sessions for staff and students to raise awareness about cybersecurity threats and best practices.
8. **Incident Response Plan**
   a. Develop and regularly update an incident response plan to address security breaches promptly and effectively.
   b. Perform a tabletop cyber-attack simulation and exercise with school management involvement.
9. **Physical Security**
   a. Ensure secure access to physical servers, networking equipment, and other critical infrastructure.
10. **Regulatory Compliance**
    a. Ensure compliance with local and international data protection regulations and standards.
11. **Monitoring and Logging**
    a. Implement comprehensive monitoring systems to detect and respond to security incidents in real time. b. Maintain detailed logs for auditing and analysis purposes.

12. Secure Software Development

a. Follow secure coding practices when developing or procuring educational software.
b. Regularly update and patch software to address vulnerabilities.

13. Cloud Security

a. If using cloud services, ensure the selected providers adhere to stringent security standards.
b. Implement proper configuration and access controls for cloud resources.
c. Integrate Cloud Services - Software as a Service (SaaS) with school identity services where possible.
d. Establish Cloud SaaS Security Posture Management capabilities.

14. Collaboration Security

a. Secure communication and collaboration platforms to protect sensitive educational information shared among students and staff.

15. Third-Party Security

a. Vet and monitor third-party vendors providing educational technology solutions to ensure they meet security standards.

6.2 System Maintenance:

Maintain and regularly update digital infrastructure, operating systems, security systems, and software, including antivirus protection software. Regularly test their digital infrastructure and systems to ensure they are in good working condition.

6.3 Safe Use of External Learning Applications:

Implement safeguarding mechanisms in place (e.g., single sign-on systems) to protect student and system security in the use of external learning applications.

6.4 Safe Virtual Interaction with Invited Visitors:

School shall seek parents' consent for any live virtual interactions with invited visitors, inside or outside of class. All such interactions shall also be approved by ADEK, in line with the Extracurricular Activities and Events Policy and the Student Protection Policy.

6.5 Backup and Storage:

School that have onsite data storage systems shall ensure that backups of important information, software, and configuration settings are performed at an appropriate frequency and retained for an appropriate period of time to allow for business continuity.

1. School shall ensure that such backups are stored securely and separately from the school network.
2. School that use external cloud systems for storage shall ensure that their data is synced to the cloud.

6.6 Cybersecurity Incidents:

School shall develop response and business continuity plans to guide staff in the event of a cybersecurity incident, including the protocols for reporting the incident to the school leadership team and to ADEK, and the process for maintaining operational continuity.

1. School shall not communicate any cybersecurity incident to external parties except for the service provider involved and ADEK.
2. School shall adhere to all applicable laws and policies set out by the Abu Dhabi Digital Authority and any other relevant authorities in the UAE, including the Federal Decree Law No. (34) of 2021 on Combatting Rumors and Cybercrimes.

7. Data Protection

7.1 Data Protection Policy: School shall develop a Data Protection Policy, setting out how the school shall ensure that personal information is dealt with correctly and securely, and in compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data, which shall include, at a minimum:

1. The specification of the types of personal information that may be collected.
2. The requirement and procedures for individual consent in the collection, processing, and storage of personal information.
    a. Consent must be freely given, specific, informed, and unambiguous.
    b. Consent may be withdrawn by the individual at any time.

3. The conditions under which personal information may be shared by the school with other individuals or entities (e.g., with ADEK).
a. School shall have a non-disclosure agreement built into any agreements with contractors in which personal data cannot be shared within or outside the country for any purposes, without the explicit consent of ADEK.

7.2 Sharing Data with ADEK: School shall provide accurate and up-to-date data to authorized ADEK personnel on request, in line with the Federal Decree Law No. (18) of 2020 on Private Education and Law No. (9) of 2018 Concerning the Establishment of the Department of Education and Knowledge and in line with the ADEK terms and conditions, and data privacy policy with regard to the collection, use, and disclosure of information.

And inform parents of their obligations to share data with ADEK accordingly.

7.3 Data Protection Plan:

Develop and annually review a data protection plan, in compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data and the Records Policy. The data protection plan shall set out the steps taken by the school to safeguard its organizational data, including data classification methods, authorization levels, protections against cybersecurity and other threats, and procedures for restoring backed-up information in case of breaches.

8. Digital Communications

8.1 Digital Media Policy:

Develop, implement, and monitor a Digital Media Policy governing the creation and publication of digital media. The policy shall include, at a minimum:

1. The requirement to obtain consent before recording and publishing digital media:
   a. School shall only take photographs and/or video recordings of students after obtaining written consent from parents. In obtaining consent, school shall inform parents about the purposes for which the photographs and/or video recordings are being taken.
   b. School shall obtain written consent from parents before publishing digital content involving students. School shall clearly specify if the student will be identified by name in the publication when obtaining consent.
2. The procedures for the provision and withdrawal of consent.
3. Conditions related to the storage and security of digital media.
4. Conditions related to the use of personal devices and accounts for recording or publishing school content.

8.2 Social Media Policy:

Develop and implement a social media Policy in relation to the use of social media by the school.

1. The policy includes
   a. Social media platforms and accounts to be used by the school.
   b. Access, security, and password protection procedures for the school's social media accounts.
   c. Conditions related to content, language use, and engagement with other accounts.

d. Conditions related to the use of names, photos, and videos of students, in accordance with Section 8.1. Digital Media Policy. e. Guidelines for moderators (see Section 8.2.2. Moderators) in relation to content posted by third parties on the school's social media pages, including procedures to manage disrespectful content and trolling.
f. Procedures for addressing other adverse social media behaviors, such as impersonation of the school's accounts.

2. Monitoring School Communications: School shall regularly monitor all official and unofficial school-related communication channels (newsletters, social media, parent communication groups, etc.) to ensure their compliance with this policy.

3. Moderators: School shall appoint moderator(s) to pre-approve or remove content posted by other users on the school's social media pages, where possible, in line with the school's guidelines. Moderator(s) shall reject or remove, where possible, content that is inappropriate, not in line with the UAE cultural values, or amounts to bullying, harassment, discrimination, or intimidation, in line with the Values and Ethics Policy and the Cultural Consideration Policy.

8.3 Personal Social Media Accounts for Staff:

Authorize members of staff to create and maintain existing personal social media accounts. In relation to these, staff members shall:

1. Not use email addresses issued by the school to create such accounts.
2. Use the tightest possible privacy settings.
3. Not identify themselves as being associated with the school, except on professional social media platforms (e.g., LinkedIn).
4. Not accept invitations to friend, connect with, or follow from current students or former students under the age of 18, or send such requests to current students or former students under the age of 18.
5. Not accept invitations from parents of current students to friends, connect with, or follow them.
6. Not use such accounts to communicate with current students, their parents, or former students under the age of 18. This applies to messaging applications (e.g., WhatsApp, Telegram, Signal).
7. Assume that content posted through such accounts (including online reviews and comments) is publicly visible and searchable, regardless of the privacy settings, and exercise appropriate discretion.

8. Ensure that content shared through such accounts is appropriate, in line with the Cultural Consideration Policy, and does not amount to bullying, harassment, discrimination, or intimidation, in line with the Values and Ethics Policy.
9.Ensure that content shared through such accounts does not give the impression of being endorsed by the school.
10. Ensure that they do not share any confidential information related to the school through such accounts.

8.4 Communications via Email: Inform staff members that they are not authorized to use personal email addresses to communicate with students or parents.

8.5 School Website:

Create a dedicated website and keep it up to date to serve as a reference for members of the school community.

1. School website contains the following information
   a. Contact information.
   b. Services provided by the school.
   c. Fees, including transportation fees and fees for optional activities.
   d. Inspection reports.
   e. Aggregate student achievement data or individual achievements (e.g., awards), with consent.
   f. School policies that are relevant to parents and/or students.
   g. Any other required content, as defined by ADEK policies.

2. Ensure that the content published on their website is accurate and appropriate, in line with the Values and Ethics Policy.

3. Ensure that content published on their website is in line with the requirements for digital media.

Prepared By	Date
ICT Coordinator	December 2015

Amendments:

Review	Date	Reviewed by	Amendments
Review 1	December 2021	Academic Vice Principal/ICT Coordinator/Health and safety Officer/Admin Officer	No Changes
Review 2	December 2023	Academic Vice Principal/ICT Coordinator/Health and safety Officer/Admin Officer	No Changes
Review 3	July 2024	Academic Vice Principal/ICT Coordinator/Health and safety Officer/Admin Officer	No Changes
Review 4	December 2025	Academic Vice Principal/ICT Coordinator/Health and safety Officer/Admin Officer	Changes in 8.5 School website

Approved By	Signature
Mr. Paramjit Ahluwalia, Principal