Sharjah American International School

2026 - 2027

SAIS

DIGITAL POLICY

Abu Dhabi Branch



Approved By	Principal
Applies To	Students, parents, staff, contractors, volunteers, visitors, and external service providers
Effective Date	August, 2025
Review Date	June 2026

This policy supports safe, responsible, inclusive, and secure use of digital technology across all areas of school life.

عـــام الأســـــرة ٢٠٢٦
YEAR OF FAMILY 2026

DOCUMENT CONTROL

ROLE	NAME	SIGNATURE	DATE
Prepared By	Digital Wellbeing Committee	Principal, Ms.Jamila/ CPO Mr.Naufal / Portal Manager Mr.Ahmed Khader/ Middle school boys' supervisor Ms.Asma Al Hosani/ social media & Website coordinator Mr.Saad/ Head Of Innovation	August,2025
Approved By	Principal		August,2025
Next Review Due		N/A	June,2026

1- POLICY STATEMENT

Sharjah American International School Abu Dhabi (SAIS-AD) is committed to ensuring the safe, responsible, secure, and effective use of digital technology across all aspects of school life. The school recognizes that digital fluency is essential for students' learning, wellbeing, future readiness, and participation in society.

SAIS-AD will promote the ethical and educational use of digital technology while protecting all members of the school community from digital harm, misuse, privacy breaches, and cybersecurity risks. This policy is aligned with current ADEK digital policy requirements for schools in Abu Dhabi.

2- PURPOSE

- To promote digital fluency, responsible online behavior, and digital citizenship.
- To safeguard students and staff from online risks and inappropriate digital conduct.
- To ensure secure use of digital systems, devices, platforms, and communications.
- To protect personal data and uphold confidentiality in line with UAE legislation.
- To establish clear expectations, roles, procedures, and accountability measures for digital use within the school community.

3- SCOPE

This policy applies to all students, parents, staff, school leaders, contractors, volunteers, and visitors. It applies to all school-owned and personal devices used for school-related activities, and to all school digital platforms, systems, networks, learning tools, email systems, websites, and social media accounts. It covers digital activity on school premises, during school hours, extracurricular activities, field trips, distance learning, and any school-affiliated digital platform or communication channel.

4- DEFINITIONS

TERM	DEFINITION
Digital Device	Any device used for audio, video, text communication, or computer-based activity, including laptops, tablets, mobile phones, and smartwatches.
Digital Incident	Any inappropriate use of digital technology, including breaches of acceptable use, cyberbullying, access to harmful or inappropriate content, inappropriate communication, or unauthorized access to systems.
Digital Fluency	The ability to use technology competently, confidently, safely, responsibly, creatively, and effectively.
Cyberbullying	Bullying that takes place online using communication technologies to insult, threaten, blackmail, harass, or humiliate others.
Personal Information	Information relating to an identifiable person, directly or indirectly.
BYOD	Bring Your Own Device; the use of personally owned digital devices for school-related activities.
Assistive Technology	Any device, equipment, software, or system used to increase, maintain, or improve the functional capabilities of students with disabilities or additional learning needs.

5. DIGITAL WELLBEING COMMITTEE

The Digital Wellbeing Committee shall oversee implementation of the school's digital strategy, review it annually, evaluate infrastructure and platforms, conduct digital risk assessments, review data protection and cybersecurity provisions, and identify staff training needs.

6. ROLES AND RESPONSIBILITIES

6.1 Principal

- Ensure implementation and monitoring of this policy.
- Approve and sign all digital incident records.
- Ensure corrective action is taken when breaches occur.

6.2 Digital Wellbeing Committee

- Monitor digital safety and responsible use.
- Coordinate awareness and staff training.
- Review digital risks, incidents, and trends.

6.3 IT Department

- Maintain secure infrastructure and filtering systems.
- Enforce updates, patching, backups, and access controls.
- Support digital monitoring and incident response.

6.4 Staff

- Use approved digital tools and communication channels only.
- Maintain confidentiality and protect personal data.
- Model responsible digital behavior and report digital incidents immediately.

6.5 Students

- Use digital tools safely, respectfully, and responsibly.
- Protect passwords and personal information.
- Report unsafe or harmful content immediately.

6.6 Parents

- Support safe digital usage at home.
- Monitor students' digital behavior outside school hours.
- Cooperate with the school in matters related to digital safety and online conduct.

7. DIGITAL COMPETENCIES

SAIS-AD shall define and integrate age-appropriate digital competencies into the curriculum by grade level. The school shall ensure students have access to appropriate digital resources and support, including students with additional learning needs.
Staff shall receive role-appropriate training on digital fluency, cybersecurity, student online safety, and data protection.

8. RESPONSIBLE USE

8.1 General Expectations

- All members of the school community must use digital devices, systems, accounts, and platforms responsibly, ethically, securely, and in ways that support learning, wellbeing, and school operations.

8.2 Student Responsible Use

- Communicate respectfully online.
- Protect personal information and that of others.
- Use school-approved tools responsibly.
- Report unsafe or inappropriate content.
- Avoid cyberbullying, plagiarism, and misuse of devices or platforms.
- Do not attempt unauthorized access to any system or account.
- Do not use VPNs on school premises or school networks unless explicitly authorized by the school.

8.3 Staff Responsible Use

- Use only school-approved tools, platforms, and systems.
- Protect student data and confidentiality.
- Do not use personal email addresses to communicate with students or parents.
- Keep school accounts secure.
- Separate personal and professional digital identities.
- Do not store or share school data on unauthorized apps or devices.

8.4 Parent Responsible Use

- Reinforce safe and appropriate digital behavior at home.
- Respect school policies on digital conduct, privacy, and communication.
- Use school communication channels appropriately and respectfully.

8.5 Visitor and Contractor Use

- Visitors, contractors, volunteers, and invited speakers must follow school expectations related to digital use, confidentiality, and safeguarding while on site or while interacting with students or school systems.

9. DIGITAL SAFEGUARDING

SAIS-AD shall implement systems and programs to protect students from online risks, including exposure to inappropriate content, unsafe online interactions, cyberbullying, phishing, scams, gambling, and other harmful digital behaviors.
The school shall provide age-appropriate digital safety education, web filtering and monitoring systems, regular analysis of internet usage and filter violations, support procedures for risky or excessive digital habits, and safeguards for virtual learning activities.

10. DIGITAL INCIDENTS

10.1 Reporting

- All digital incidents must be reported immediately to the relevant line manager, safeguarding lead, Digital Wellbeing committee, or SLT depending on the nature of the concern.

10.2 Investigation and Response

- The school shall investigate and respond to digital incidents in line with relevant school and ADEK policies, including safeguarding, behavior, wellbeing, staff conduct, and records requirements.

10.3 Recording

- Every digital incident shall be recorded in writing, reviewed by SLT, signed by the Principal, and stored securely for auditing purposes.

10.4 External Reporting

- Where necessary, the school shall report incidents to ADEK and cooperate with Abu Dhabi Police or other relevant authorities.

11. DIGITAL INFRASTRUCTURE AND CYBERSECURITY

SAIS-AD shall maintain secure digital infrastructure and implement cybersecurity controls including multi-factor authentication for critical services, role-based access permissions, encryption of sensitive data, firewalls, filtering systems, malware protection, patching, secure backups, disaster recovery measures, monitoring, logging, cloud security controls, and third-party security checks.

12. BYOD AND SCHOOL DEVICES

At SAIS, students are permitted to use personal devices for school-related purposes under a Bring Your Own Device (BYOD) approach. Accordingly, the school requires that all such devices meet established digital safety standards, including up-to-date antivirus protection, regular software updates, password security, secure access to school systems, and compliance with the school's filtering, monitoring, and safeguarding requirements.

13. DISTANCE LEARNING READINESS

SAIS-AD shall maintain systems and procedures to support emergency distance learning, temporary school closure, or exceptional remote access for individual students.
This shall include approved digital learning platforms, safeguarding expectations for virtual lessons, attendance and engagement procedures, communication arrangements, continuity planning, and technical support measures.

14. INCLUSION AND ASSISTIVE TECHNOLOGY

The school shall provide assistive technology to students with additional learning needs in accordance with their documented learning plans and the ADEK School Inclusion Policy.

15. EXTERNAL PROVIDERS AND DIGITAL PRODUCTS

Before using any third-party digital platform, software, app, or provider, SAIS-AD shall assess compatibility with school systems, secure data handling, cybersecurity compliance, protection against cyber threats, service reliability, provider reputation, legal compliance, and educational value or age-appropriateness where relevant.
No external tool may be used with students unless approved by the school leaders.

16. DATA PROTECTION

SAIS-AD shall maintain and annually review a Data Protection Policy and Data Protection Plan in line with UAE legislation and ADEK requirements.
These documents shall define the types of personal data collected, consent procedures, access and authorization controls, data-sharing conditions, retention and restoration procedures, protections against unauthorized disclosure or data breach, and annual review mechanisms.

17. DIGITAL MEDIA

SAIS-AD shall obtain written parental consent before taking photographs or videos of students, publishing student digital media, or identifying students by name in digital publications where relevant. The school shall define procedures for obtaining consent, withdrawing consent, secure storage of digital media, and restrictions on personal devices or accounts being used for recording or publishing school content.

18. SOCIAL MEDIA

SAIS-AD shall maintain a Social Media Policy governing the school's use of social media. This shall include approved platforms and official accounts, account security, standards for content and engagement, moderation procedures, and procedures for misuse, impersonation, or culturally inappropriate content.

19. PERSONAL SOCIAL MEDIA USE BY STAFF

Staff members using personal social media accounts shall not use school-issued email addresses to create such accounts, shall use strong privacy settings, and shall not represent personal content as endorsed by the school.
Staff shall not connect with current students or former students under 18 on personal social media, shall not connect with parents of current students on personal social media, and shall not use personal accounts or messaging apps to communicate with current students, parents, or former students under 18.
Confidential school information must not be shared through personal accounts.

20. SCHOOL WEBSITE

The school website shall be maintained as an up-to-date official reference for the school community. It shall include contact information, services provided, fees and optional charges, inspection reports, student achievement information where consent exists, public annual reports where applicable, relevant policies, and any additional content required by ADEK.

21. ACCEPTABLE USE AGREEMENTS

SAIS-AD shall issue and collect age-appropriate acceptable use agreements for students and communicate relevant responsible use expectations to parents, staff, and visitors.
For students up to Grade 6 , an age-appropriate student version shall be provided, while parents shall receive the full version.

22. MONITORING, COMPLIANCE, AND REVIEW

This policy shall be monitored through annual review by the Digital Wellbeing Committee, review of digital incidents and trends, audit of training and system readiness, review of approved digital tools and vendors, website publication checks, and stakeholder feedback where relevant.

25. KEY SCHOOL CONTACTS

ROLE	EMAILS AND NAMES
Social Media & Website Coordinator	Asma Alhosani asma.alhosani@saisabudhabi.com
Principal	Ban Al Duri principal@saisdubai.com
Child Protection Officer	Djamilla Meziane djamillameziane@gmail.com
Inclusion Lead	Marwa Aly marwa.aly@saisabudhabi.com
School Portal Coordinator	Mr.Naufal naufal.naushad@saisabudhabi.com
Innovation Head	Mr.Saad saad.salama@saisabudhabi.com

APPENDICES

The following appendices are included to support policy implementation and school-level monitoring.

- Appendix 1: Primary Student Acceptable Use Agreement
- Appendix 2: Secondary Student Acceptable Use Agreement
- Appendix 3: Staff Digital Responsible Use Agreement
- Appendix 4: Digital Incident Reporting Form
- Appendix 5: Third-Party Digital Tool Risk Assessment Checklist

Digital Policy Appendices Forms

Appendix 1: Student Acceptable Use Agreement

Grades 3 & 4 Student Acceptable Use Agreement

STUDENT NAME	----------
GRADE / CLASS	----------
ACADEMIC YEAR	----------

At SAIS-AD, I agree to use digital devices and online platforms in a safe, respectful, and responsible way.

I agree that I will:

1. Be kind and respectful when I communicate online.
2. Use school devices, websites, apps, and platforms for learning purposes only.
3. Keep my personal information safe, including my full name, address, phone number, passwords, and photos.
4. Not sharing any information without permission.
5. Tell a teacher or trusted adult if I see anything online that makes me feel worried, upset, or unsafe.
6. Not send or post unkind, rude, or bullying messages.
7. Take care of any device I use at school.
8. Only use websites, apps, and games that my teacher allows.
9. Keep my passwords private unless my parent or teacher asks for them.
10. Not try to open, change, or damage another person's work, account, or device.

I understand that:

- My use of digital technology at school must follow school rules.
- The school may check my use of digital systems, devices, and accounts to keep everyone safe.
- If I do not use technology safely and responsibly, the school may take action in line with school rules.

Student Signature:
_____

Date:
_____

Parent/Guardian Name:
_____

Parent/Guardian Signature:
_____

Digital Policy Appendices Forms

Appendix 2: High School Student Acceptable Use Agreement

High School Student Acceptable Use Agreement

STUDENT NAME	----------
GRADE / CLASS	----------
ACADEMIC YEAR	----------

As a student at SAIS-AD, I understand that I must use digital devices, school systems, and online platforms safely, responsibly, and respectfully.

I agree that I will:

1. Use digital technologies for educational purposes in a responsible and ethical manner.
2. Communicate respectfully with staff and students in all online spaces.
3. Protect my passwords and not use another person's login details or account.
4. Protect my personal information and respect the privacy of others.
5. Not participate in cyberbullying, harassment, intimidation, or inappropriate online behavior.
6. Not access, store, create, or share inappropriate, offensive, violent, or illegal content.
7. Not use unauthorized VPNs, software, applications, or websites on school devices or networks.
8. Not attempt to bypass school filtering, monitoring, or security controls.
9. Follow copyright, plagiarism, and academic honesty rules, including when using AI tools and digital resources.
10. Immediately report unsafe content, suspicious online activity, or digital incidents to a teacher or school leader.
11. Use my personal device for school purposes only in line with school expectations.
12. Keep my device secure with password protection and required updates.

I understand that:

- My use of digital technology on school premises, school systems, and school-related activities may be monitored.
- I must follow the school's Digital Policy, safeguarding expectations, and code of conduct.
- Breach of this agreement may result in disciplinary action in line with school policy.

Student Signature: _____ Date: _____

Parent/Guardian Name: _____ Parent/Guardian Signature: _____

Digital Policy Appendices Forms

Appendix 3: Staff Digital Responsible Use Agreement

Staff Digital Responsible Use Agreement

STAFF NAME	----------
POSITION	----------
DEPARTMENT	----------
ACADEMIC YEAR	----------

As a staff member of SAIS-AD, I acknowledge my responsibility to use digital systems, devices, and communications safely, professionally, ethically, and in accordance with school expectations.

I agree that I will:

1. Use only school-approved digital systems, platforms, and communication tools for school-related work.
2. Protect the confidentiality, privacy, and security of student, parent, and staff information.
3. Use strong passwords and keep login credentials secure.
4. Not use personal email addresses to communicate with students or parents.
5. Not use personal social media or messaging applications to communicate with current students, parents, or former students under the age of 18.
6. Maintain appropriate professional boundaries in all digital communications.
7. Follow school procedures for recording, storing, sharing, and publishing digital content.
8. Not share confidential school information on unauthorized applications, devices, or accounts.
9. Immediately report digital incidents, data breaches, safeguarding concerns, or cybersecurity risks to school leadership or the designated lead.
10. Ensure that my personal device, where used for school purposes, complies with school cybersecurity expectations, including updates, antivirus, password protection, and secure access.
11. Follow school guidance regarding acceptable use, copyright, data protection, AI tools, and online conduct.
12. Model safe, respectful, and responsible digital behavior at all times.

I understand that:

- School systems, devices, and accounts are subject to monitoring and audit where appropriate.
- Failure to comply with the school's Digital Policy may result in disciplinary action.
- I am responsible for maintaining professional conduct in all digital and online environments connected to my role.

Staff Signature: _____
Line Manager Name: _____
Date: _____

Date: _____

Signature : ----------

Digital Policy Appendices Forms

Appendix 4: Digital Incident Reporting Form

This form is to be completed for any digital incident and filed securely for audit purposes.

DATE OF INCIDENT	----------
REPORTED BY	----------
STUDENT / STAFF INVOLVED	----------
TYPE OF INCIDENT	----------
SUMMARY OF INCIDENT	----------
IMMEDIATE ACTION TAKEN	----------
FOLLOW-UP REQUIRED	----------
PRINCIPAL SIGNATURE / DATE	----------

Digital Policy Appendices Forms

Appendix 5: Third-Party Digital Tool Risk Assessment Checklist

DATE OF INCIDENT	YES /NO	NOTES
COMPATIBLE WITH SCHOOL SYSTEMS		
SECURE MANAGEMENT OF PERSONAL DATA		
MEETS CYBERSECURITY REQUIREMENTS		
INCLUDES BACKUP AND RECOVERY PROVISIONS		
AGE-APPROPRIATE FOR STUDENTS		
ALIGNED WITH EDUCATIONAL PURPOSE		
VENDOR REPUTATION VERIFIED		
LEGAL AND PRIVACY COMPLIANCE CONFIRMED		