AUSTRALIAN SCHOOL OF ABU DHABI

ICT ACCEPTABLE USE & BYOD POLICY

Contents

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

7.1 Principles of Acceptable and Responsible Digital Use 7

7.1.1 Educational Purposes 7
7.1.2 Safety, Wellbeing and Safeguarding 8
7.1.3 Respectful and Ethical Use 8
7.1.4 Security and Privacy 8
7.1.5 Accountability and Responsibility 8

7.2 Acceptable Use of School Digital Systems and Network 8

7.2.1 School Digital Systems and Platforms 9
7.2.2 School Networks and Internet Systems 9
7.2.3 School-Issued and Shared Devices 9
7.2.4 Computer Laboratories and Shared Facilities 9
7.2.5 Prohibited Use 10

7.3 Bring Your Own Device (BYOD) 10

7.3.1 Purpose Of BYOD 10
7.3.2 Conditions For BYOD Use 11
7.3.3 Responsibility, Care and Liability 11
7.3.4 Monitoring, Access and Restrictions 11
7.3.5 Use During School Activities and Off-Site Events 12
7.3.6 Devices Not Covered By BYOD 12

7.4 Use Of Personal Devices On and Off Premises 12

7.4.1 Use During School Hours 12
7.4.2 Using During Co-Curricular and Extracurricular Activities 12
7.4.3 Use During Excursions, Camps and Off-Site Activities 13
7.4.4 Use During Virtual Learning Activities 13
7.4.5 Use Outside School Hours and Premises 13

7.5 Accounts, Passwords and Access Security 13

7.5.1 User Accounts 13
7.5.2 Password Protection 14
7.5.3 Account Use and Security 14
7.5.4 Safeguarding and Security Controls 14
7.5.5 Use of School Issued Email Accounts 14

7.6 Data Sharing, Privacy and Use of External Applications 15
7.6.1 Data Protection and Privacy 15
7.6.2 Sharing of School-Related Information And Data 15
7.6.3 Use of External Applications and Digital Tools 15
7.6.4 Uploading and Storage of Student Information And Data 15
7.6.5 Monitoring and Compliance 16
7.7 Academic Integrity and Responsible Use of Digital Tools 16
7.7.1 Academic Honesty and Plagiarism 16
7.7.2 Copyright and the Use of Digital Content 16
7.7.3 Responsible Use of Artificial Intelligence and Emerging Technologies 16
7.7.4 Use of Devices During Assessments and Examinations 17
7.7.5 Alignment with Academic Integrity Policy 17
7.8 Digital Safeguarding and Online Behaviour 17
7.8.1 Online Conduct and Behaviour 17
7.8.2 Online Risks and Student Protection 18
7.8.3 Safeguarding Measures and Support 18
7.8.4 Reporting Concerns 18
7.8.5 Behavioural Expectations and Consequences 18
7.9 Filtering, Monitoring and Appropriate Supervision 18
7.9.1 Filtering and Access Controls 19
7.9.2 Monitoring of Digital Use 19
7.9.3 Educational Purpose and Supervision 19
7.9.4 Review and Response To Digital Use 19
7.9.5 Limitations of Monitoring 20
7.10 Digital Incidents and Breaches of Acceptable Use 20
7.10.1 Types of Digital Incidents 20
7.10.2 Reporting Digital Incidents 20
7.10.3 Lost, Stolen or Compromised Devices and Accounts 20
7.10.4 Response and Support 21
7.10.5 Escalation and External Reporting 21
7.10.6 Recording and Documentation 21
7.10.7 Review and Improvement 21
7.11 Roles and Responsibilities 21
7.11.1 ASAD Leadership Team 22
7.11.2 Staff 22
7.11.3 Students 22
7.11.4 Parents and Guardians 22
7.11.5 Visitors, Contractors and Other Authorised Users 23
7.12 Parent and Guardian Responsibilities Outside School Hours 23

7.13 Communication, Awareness and Age-Appropriate Access 23
7.13.1 Communication of the Policy 23
7.13.2 Student Awareness and Education 24
7.13.3 Age-Appropriate Access and Adaptation 24
7.13.4 Ongoing Awareness and Review 24
7.14 Monitoring, Review and Policy Availability 24
7.14.1 Monitoring and Oversight 24
7.14.2 Review of the Policy 24
7.14.3 Policy Availability 25
8. Compliance 25
9. References 26
10. Ratification & Revision History 26
Appendix A: ICT Acceptable Use & BYOD Agreement 27

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

Australian School of Abu Dhabi (ASAD) recognises that digital technologies play an essential role in teaching, learning, communication and school operations across the Primary Years Programme (PYP), Middle Years Programme (MYP) and Diploma Programme (DP). The safe, responsible and ethical use of digital systems and devices is fundamental to supporting high-quality learning, student wellbeing and safeguarding.

This ICT Acceptable Use & BYOD Policy sets out ASAD's expectations for the responsible and appropriate use of digital technologies, systems, networks and devices, in line with the ADEK *School Digital Policy*, applicable UAE legislation and recognised international best practice, including expectations of the International Baccalaureate (IB).

The policy applies to the use of school-owned digital systems and devices, shared resources such as computer laboratories, and personally owned devices used under the school's Bring Your Own Device (BYOD) framework. It is designed to support a positive digital culture that promotes learning, respect, safety and accountability.

This policy operates in conjunction with ASAD's Digital Policy, Information and Data Protection Policy, Data Protection Plan, Safeguarding and Student Protection Policy, Academic Integrity Policy, Digital Media and Social Media Policy, Records Management Policy and Student Behaviour Policy.

All students and their parents/guardians are required to acknowledge and comply with the ICT Acceptable Use & BYOD Agreement (Appendix A). Access to school-managed digital systems, networks and devices is conditional upon this acknowledgement and ongoing compliance.

4. PURPOSE

The purpose of this ICT Acceptable Use & BYOD Policy is to establish clear expectations for the safe, responsible and appropriate use of digital technologies at Australian School of Abu Dhabi (ASAD).

This policy is intended to support a positive digital culture that:

- promotes responsible and ethical digital behaviour across the school community;
- enables purposeful, developmentally appropriate use of technology to support teaching and learning across the IB PYP, MYP and DP;
- protects students from online risks and supports their wellbeing and safeguarding;
- ensures the security, integrity and appropriate use of school systems, networks and digital resources;

- clarifies expectations relating to the use of school-issued devices, shared devices and personally owned devices under the school's Bring Your Own Device (BYOD) framework; and
- supports compliance with ADEK requirements, applicable UAE legislation and recognised international best practice, including expectations of the International Baccalaureate.

5. SCOPE

This policy applies to all members of the ASAD community who access or use the school's digital systems, networks or devices, including:

- students across all year levels (PYP, MYP and DP);
- staff, including teaching, administrative and support staff;
- parents and guardians where they access school platforms or systems;
- visitors, contractors and other authorised users.

The policy applies to:

- school-owned and school-managed digital systems and platforms;
- school-issued and shared digital devices, including computer laboratories;
- personally owned devices used on school premises, school networks or during school-related activities under the BYOD framework;
- digital use during school hours, off-site activities, excursions, camps and school-related events.

Different expectations and supports may apply based on students' age, developmental stage and programme of study, in line with IB and ADEK guidance.

6. DEFINITIONS

TERM	DEFINITION
Acceptable Use	The responsible, ethical and lawful use of digital technologies, systems and devices in accordance with school policies and procedures.
Bring Your Own Device (BYOD)	The use of personally owned digital devices by students, staff or other authorised users for approved educational purposes, in accordance with the school's Acceptable Use & BYOD Policy and related procedures.
Consent	A freely given, specific, informed and unambiguous indication by which an individual, or a parent or guardian where appropriate, agrees to the collection and processing of personal information and data. Consent may be withdrawn at any time.
Contractor	An individual or organisation engaged by Australian School of Abu Dhabi (ASAD) under a contract or agreement to provide services to the school, including consultants, service providers and external specialists, who may have access to personal information and data in the course of their work.
Data Breach	An incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information and data.
Data Protection Plan	The school's operational document that sets out procedures, controls and actions to support the implementation of this Information and Data Protection Policy.
Digital Incident	An incident involving the inappropriate, unsafe or unauthorised use of digital technologies, systems or platforms, including breaches of acceptable use, safeguarding concerns or information security incidents.

Digital Technologies	Electronic tools, systems, devices, platforms and applications used to create, access, process, store or share information and data for educational, operational or communication purposes.
Information and Communication Technology (ICT)	All digital devices, systems, networks, software, and online platforms used within the school for teaching, learning, administration, communication, and data management, including school-owned and approved personal devices.
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.
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.
School Digital Systems	Digital platforms, software, networks and services provided or approved by Australian School of Abu Dhabi (ASAD) to support teaching, learning, communication and school operations.
Third Party	Any individual, organisation or entity external to ASAD that processes or has access to personal information and data on behalf of the school, including contractors, service providers and partners.
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 Principles of Acceptable and Responsible Digital Use

Australian School of Abu Dhabi (ASAD) is committed to fostering a safe, respectful and purposeful digital environment that supports learning, wellbeing and safeguarding across all year levels, from Kindergarten to Grade 12.

The following principles underpin all expectations relating to the use of digital technologies, systems, networks and devices at ASAD and apply to students, staff, parents, guardians and other authorised users.

7.1.1 Educational Purposes

Digital technologies will be used to support teaching, learning, assessment and school operations in ways that are purposeful, meaningful and appropriate to students' age, developmental stage and programme of study. Access to digital tools and the internet during school hours will be guided by clear educational intent and learning outcomes.

7.1.2 Safety, Wellbeing and Safeguarding

The safety and wellbeing of students is a priority in all digital contexts. Digital use will support positive behaviour, respectful interaction and student wellbeing, and will seek to protect students from online risks, including exposure to inappropriate content, unsafe online interactions and harmful digital behaviours.

Safeguarding considerations apply to all digital activities, whether conducted on school premises, through school systems or during school-related activities conducted online or off-site.

7.1.3 Respectful and Ethical Use

All users are expected to use digital technologies respectfully and ethically. This includes demonstrating respect for others, maintaining appropriate online conduct, and using digital tools in ways that uphold the values of the school community and the principles of the International Baccalaureate.

The use of digital technologies will also align with ASAD's Academic Integrity Policy, including expectations relating to academic honesty, plagiarism, copyright and the ethical use of digital tools, including artificial intelligence. Harassment, bullying, intimidation, discrimination or any form of harmful behaviour conducted through digital means is not acceptable.

7.1.4 Security and Privacy

Digital use at ASAD will protect the security of school systems and the privacy of personal information and data. Users are expected to follow school requirements relating to account security, password protection and appropriate handling of information, in line with the school's Information and Data Protection Policy and related procedures.

7.1.5 Accountability and Responsibility

All users are responsible for their actions when using digital systems, devices and online platforms. Use of digital technologies at ASAD is a privilege that may be restricted or withdrawn where expectations are not met.

Breaches of ICT acceptable use expectations will be addressed in accordance with this policy and relevant school procedures detailed in the Student Behaviour Management and Wellbeing Policy.

7.2 Acceptable Use of School Digital Systems and Network

Australian School of Abu Dhabi (ASAD) provides access to digital systems, networks and technologies to support teaching, learning, communication and school operations. Access to these systems is provided to authorised users for legitimate educational, safeguarding and operational purposes only.

All users are expected to use school digital systems and networks responsibly, securely and in accordance with this policy and related school procedures.

7.2.1 School Digital Systems and Platforms

School digital systems and platforms include, but are not limited to, school management systems, learning management platforms, communication and collaboration tools, assessment and reporting systems, and other approved educational technologies.

Use of school digital systems and platforms will:

- support teaching, learning, assessment and school operations;
- be consistent with the school's educational objectives and safeguarding responsibilities;
- comply with the school's Information and Data Protection Policy and Academic Integrity Policy.

Users must not:

- access systems or data for which they are not authorised;
- use school platforms for non-school-related, inappropriate or unlawful purposes;
- attempt to bypass security controls or access restrictions.

7.2.2 School Networks and Internet Systems

Access to the school's wired and wireless networks is provided to support educational and operational activities. Use of the school network and internet access will:

- be subject to filtering and monitoring systems designed to promote safe and appropriate use;
- be limited to activities that support learning, wellbeing and school operations;
- be supervised and guided by staff in a manner appropriate to students' age and developmental stage.

Bypassing school filtering and security controls is **not permitted.** This includes the use of VPNs, proxies, anonymisers, MAC spoofing, hotspotting or tethering to avoid school controls, alternate DNS or any other method intended to bypass filtering, monitoring, authentication or access restrictions, unless explicitly authorised by the school for a specific educational or administrative purpose.

7.2.3 School-Issued and Shared Devices

ASAD provides school-issued and shared digital devices, including devices used in computer laboratories and learning spaces, to support access to learning and school activities.
Users of school-issued and shared devices are expected to:

- use devices responsibly and for authorised purposes only;
- take reasonable care to prevent damage, loss or misuse;
- log in using their own credentials and log out after use;
- respect shared access and availability of devices.

School-issued and shared devices remain the property of ASAD and may be monitored, restricted or withdrawn where acceptable use expectations are not met.

7.2.4 Computer Laboratories and Shared Facilities

Computer laboratories and shared digital facilities are provided to support structured learning activities and supervised access to digital resources.
Use of these facilities will:

- be guided by staff supervision and clear learning objectives;
- follow established procedures for access, behaviour and care of equipment;
- support equitable access for all students.

Food, drink or unauthorised software installation is not permitted in computer laboratories or shared digital facilities.

7.2.5 Prohibited Use

The following activities are not permitted on school digital systems, networks or devices:

- accessing, creating, storing or sharing content that is inappropriate, offensive, illegal or harmful;
- engaging in cyberbullying, harassment, intimidation or discrimination;
- attempting to interfere with the operation, security or integrity of school systems or networks;
- using digital systems to breach confidentiality or misuse personal information and data;
- publishing or forwarding harmful misinformation, rumours or content that violates UAE cybercrime provisions;
- using Virtual Private Networks (VPNs), proxy services, anonymisers, personal hotspots or tethering, or other technologies and techniques designed to avoid monitoring or access restrictions;
- any use that compromises the safety, wellbeing or reputation of the school community.

Breaches of ICT acceptable use may be addressed in accordance with this policy and relevant school procedures.

7.3 Bring Your Own Device (BYOD)

Australian School of Abu Dhabi (ASAD) recognises that personally owned digital devices can support learning, independence and digital literacy when used appropriately. The school therefore permits the use of personally owned devices under a Bring Your Own Device (BYOD) framework, subject to the expectations set out in this policy.

BYOD is a privilege that supports learning and may be restricted or withdrawn where acceptable use expectations are not met.

7.3.1 Purpose of BYOD

The purpose of BYOD at ASAD is to:

- support teaching and learning through flexible and responsible use of technology;
- enable students to develop digital skills appropriate to their age and programme of study;
- complement the use of school-issued and shared devices;
- promote responsible digital citizenship in line with IB learner profile attributes.

ASAD does not mandate specific device types, brands or operating systems. Devices used under BYOD must, however, be suitable for educational use and comply with school requirements. Recommended device specifications and requirements are communicated separately by the school and may be updated annually to reflect curriculum needs, platform requirements and changes in technology.

7.3.2 Conditions for BYOD Use

Use of personal devices under the BYOD framework is permitted only where:

- use is authorised by the school and supervised as appropriate;
- the device is used for educational purposes aligned with learning activities;
- the device connects only to the school's approved networks;
- the user complies with this policy and all related school policies and procedures.

Personal devices must not be used to:

- take photographs, record video or capture audio of students, staff or school activities without explicit authorisation from the school;
- capture, store, or share assessment materials, answers, or secure school documents;
- record or share images, video or audio in a manner that compromises privacy, dignity or safeguarding;
- access, store or distribute inappropriate, offensive or unauthorised content;
- disrupt learning, compromise safety or interfere with the operation of school systems.

Expectations relating to photography, video, publication and media use are set out in ASAD's Digital Media and Social Media Policy and Information and Data Protection Policy.

Personal devices used under BYOD must be protected by a passcode and automatic screen locking, kept up to date with current security updates, and use reputable anti-malware/endpoint protection where applicable. Devices must not be jailbroken or rooted. The school may require additional security controls or safety software to enable connection to school systems and networks.

7.3.3 Responsibility, Care and Liability

Students and parents or guardians are responsible for:

- the care, security and appropriate use of personal devices;
- ensuring devices are charged, maintained and fit for purpose;
- backing up personal data stored on devices.

ASAD does not accept responsibility for the loss, theft or damage of personal devices brought onto school premises or used during school-related activities. The school provides technical support for school-managed systems and platforms. Support for personally owned devices is limited and does not extend to hardware repairs, personal software or home network issues.

7.3.4 Monitoring, Access and Restrictions

Use of personal devices on the school network may be subject to monitoring, filtering and access controls in line with safeguarding and security requirements. ASAD reserves the right to:

- restrict or suspend access to the school network or digital systems;
- require devices to be disconnected from the network;
- impose additional controls or conditions on BYOD use,
- where ICT acceptable use expectations are not met or where necessary to protect students, staff, systems or data.

7.3.5 Use During School Activities and Off-Site Events

BYOD expectations apply during:

- school hours;
- co-curricular and extracurricular activities;
- excursions, camps and school events;
- virtual learning activities facilitated by the school.

Staff will provide guidance on when and how personal devices may be used during these activities, taking into account safeguarding, supervision and educational purpose.

7.3.6 Devices Not Covered by BYOD

For the purposes of this policy, smartphones, smart watches and similar wearable or communication devices are not considered BYOD learning devices, unless explicitly authorised by the school for a specific educational purpose.

Expectations relating to the possession and use of mobile phones/smartphones and similar devices during the school day are addressed through school procedures and related policies.

7.4 Use of Personal Devices On and Off Premises

The use of personal digital devices by students, staff and other authorised users is subject to clear expectations that reflect context, supervision and educational purpose.

7.4.1 Use During School Hours

Personal devices may be used during school hours only where:

- use is explicitly authorised by staff;
- use supports identified learning activities or school operations;
- appropriate supervision is in place.

Unless explicitly authorised, mobile phones/smartphones, smart watches and similar devices are not permitted for learning use during the school day. At all other times during the school day, personal devices may be required to be switched off, silenced or stored securely in accordance with school procedures.

7.4.2 Using During Co-curricular and Extracurricular Activities

Use of personal devices during co-curricular and extracurricular activities is permitted only where:

- use is authorised by supervising staff;
- use supports the purpose of the activity;
- safeguarding and supervision requirements are met.

Staff will provide guidance regarding appropriate use during clubs, sports, rehearsals and other school activities.

7.4.3 Use During Excursions, Camps and Off-Site Activities

During excursions, camps and other off-site school activities, use of personal devices:

- will be guided by staff instructions and risk assessments;
- may be restricted or prohibited to support safety, supervision and engagement;
- must comply with this policy and related school procedures.

Additional conditions may apply based on the nature of the activity, location and age of students

7.4.4 Use During Virtual Learning Activities

Where learning activities are conducted virtually or online, personal device use:

- will support educational participation and engagement;
- must reflect respectful and appropriate online behaviour;
- will be subject to safeguarding measures, including supervision and platform controls.

Expectations for virtual learning environments align with those that apply on school premises.

7.4.5 Use Outside School Hours and Premises

While ASAD recognises that personal device use outside school hours and off school premises is primarily the responsibility of parents and guardians, the school may respond to digital behaviour that:

- impacts student wellbeing or safeguarding;
- affects the school community or learning environment;
- involves misuse of school systems, platforms or accounts.

Parent and guardian responsibilities in relation to digital use outside school hours are outlined in Section 7.12 of this policy.

7.5 Accounts, Passwords and Access Security

Australian School of Abu Dhabi (ASAD) provides authorised users with access to school-managed digital systems, platforms and services through individual accounts. The security of these accounts is essential to protecting students, staff, systems and information.

7.5.1 User Accounts

Access to school digital systems will:

- be provided only to authorised users;
- be linked to individual user accounts where applicable;
- be limited to the permissions necessary to fulfil educational or operational responsibilities.

Users must not access, attempt to access or use accounts or systems for which they are not authorised.

7.5.2 Password Protection

Users are responsible for:

- keeping passwords and login credentials confidential;
- creating strong passwords in accordance with school requirements;
- updating passwords when prompted or where there is a risk of compromise.

Passwords must not be shared with other users, including peers, colleagues or family members.

7.5.3 Account Use and Security

Users must:

- use only their own login credentials;
- log out of systems when devices are unattended or shared;
- report any suspected or actual unauthorised access, account misuse or security concerns promptly in accordance with school procedures.

ASAD may monitor account activity and suspend or restrict access where there are concerns relating to security, safeguarding or acceptable use.

7.5.4 Safeguarding and Security Controls

ASAD implements technical and organisational measures to support secure access to systems, including authentication controls, access management and monitoring.

Use of tools or methods designed to bypass security controls, including unauthorised VPNs or anonymisation services, is **not permitted** unless explicitly authorised for educational or administrative purposes.

7.5.5 Use of School Issued Email Accounts

Australian School of Abu Dhabi (ASAD) provides school-issued email accounts to students and staff to support teaching, learning, communication and school operations.

School-issued email accounts must:

- be used for school-related educational and operational purposes only;
- be used in accordance with this policy and related school procedures;
- be used in a respectful, professional and appropriate manner.

Students must communicate with staff only through school-issued email accounts and approved learning platforms. Staff must use school-issued email accounts and approved systems for communication with students and parents/guardians and must not use personal email accounts or personal messaging applications for school communication unless explicitly authorised.

Use of school-issued email accounts may be monitored in a proportionate manner for safeguarding, security and compliance purposes, in line with ASAD's Privacy Notice and Information and Data Protection Policy

7.6 Data Sharing, Privacy and Use of External Applications

Australian School of Abu Dhabi (ASAD) recognises that the responsible handling of information and data is essential to protecting privacy, safeguarding students and maintaining trust within the school community. All use of digital systems, platforms and applications must comply with the school's Information and Data Protection Policy, Data Protection Plan and related procedures.

7.6.1 Data Protection and Privacy

Personal information and data accessed, created or processed through school digital systems will:

- be handled lawfully, securely and responsibly;
- be accessed only by authorised users for legitimate educational or operational purposes;
- be protected in line with applicable UAE legislation and school policies.

Users must not misuse, disclose or share personal information or data in ways that compromise privacy, confidentiality or safeguarding.

7.6.2 Sharing of School-Related Information and Data

Information and data relating to the school, students, staff or the wider school community must be shared only:

- through school-approved systems and communication channels;
- where there is a legitimate educational, safeguarding or operational purpose;
- in accordance with school policies and procedures.

The sharing of school-related information and data through personal email accounts, messaging applications or unapproved platforms is not permitted unless explicitly authorised by the school. The use of personal email accounts or personal messaging applications for school-related communication is not permitted unless explicitly authorised by the school.

7.6.3 Use of External Applications and Digital Tools

External applications, websites and digital tools may be used to support learning where they:

- are approved by the school or used under staff supervision;
- align with educational objectives and safeguarding requirements;
- comply with data protection and privacy expectations.

Staff will ensure that any external applications or digital tools used for learning do not require students to create unauthorised accounts or share personal information without appropriate approval and safeguards.

7.6.4 Uploading and Storage of Student Information and Data

Student information and data must not be uploaded, stored or shared on external platforms or personal devices unless:

- the platform or system is approved by the school;
- appropriate data protection and security safeguards are in place;

- use aligns with the school's Information and Data Protection Policy.

7.6.5 Monitoring and Compliance

ASAD may monitor the use of digital systems and applications to ensure compliance with this policy and related procedures. Concerns relating to data sharing or privacy will be addressed in accordance with school policies and may result in restrictions on access or other action where required.

7.7 Academic Integrity and Responsible Use of Digital Tools

Australian School of Abu Dhabi (ASAD) is committed to upholding high standards of academic integrity and ethical practice in all learning environments, including digital and online contexts.

The use of digital technologies, platforms and tools must support honest, responsible and authentic learning and assessment practices, in line with the values and expectations of the International Baccalaureate and ASAD's Academic Integrity Policy.

7.7.1 Academic Honesty and Plagiarism

Students are expected to:

- produce original work that accurately reflects their own learning;
- acknowledge sources appropriately when using the ideas, words or work of others;
- avoid plagiarism, collusion or other forms of academic misconduct, whether intentional or unintentional.

Digital tools and platforms must not be used to misrepresent learning or assessment outcomes.

7.7.2 Copyright and the Use of Digital Content

All users must respect copyright and intellectual property rights when accessing, using or sharing digital content.
This includes:

- using digital resources, images, media and software lawfully;
- acknowledging and attributing sources where required;
- complying with the Federal Decree-Law No. (38) of 2021 on Copyrights and Related Rights.

Unauthorised downloading, copying, sharing or distribution of copyrighted material is not permitted.

7.7.3 Responsible Use of Artificial Intelligence and Emerging Technologies

Digital tools, including artificial intelligence (AI) and emerging technologies, may be used to support learning where their use:

- is **explicitly** permitted by the school and teaching staff;
- supports understanding, skill development and reflection rather than replacing student thinking;
- aligns with assessment expectations and programme requirements.

The use of AI or digital tools to generate or submit work as a student's own is **not permitted.**

7.7.4 Use of Devices During Assessments and Examinations

During assessments, examinations and other supervised evaluation activities, the use of personal devices under the BYOD framework may be restricted, prohibited or subject to specific conditions. The school may require that personal devices:

- are switched off or placed in airplane mode;
- are handed in, stored securely or removed from the assessment environment;
- are used only under the direct supervision and explicit instruction of the invigilating teacher.

The use of digital tools, including artificial intelligence, translation tools or automated content generators, during assessments is permitted only where explicitly authorised by the school and in accordance with ASAD's Academic Integrity Policy and programme-specific assessment requirements. For external examinations and formal assessments, procedures issued by the school and programme requirements (including IB and MoE regulations where applicable) take precedence.

Any unauthorised use of devices or digital tools during assessments will be treated as a breach of academic integrity and addressed in line with school policies and procedures.

7.7.5 Alignment with Academic Integrity Policy

Expectations relating to academic honesty, assessment practices, use of sources and consequences of academic misconduct are set out in ASAD's Academic Integrity Policy, which applies to all students and staff.

Breaches of academic integrity involving digital tools will be addressed in accordance with that policy and relevant school procedures and policies.

7.8 Digital Safeguarding and Online Behaviour

Australian School of Abu Dhabi (ASAD) is committed to protecting students from online risks and promoting positive, respectful and safe behaviour in digital environments.

Digital safeguarding applies to all use of digital technologies, systems and platforms that are accessed through school networks, school-managed systems or in connection with school activities, whether on or off school premises.

7.8.1 Online Conduct and Behaviour

All members of the school community are expected to:

- engage respectfully and responsibly in online interactions;
- communicate appropriately and consider the impact of digital behaviour on others;
- uphold the school's values and expectations in digital spaces;
- consider the long-term impact of their digital actions, including their digital footprint and online reputation.

Students must communicate with staff only via approved email and learning platforms. Inappropriate online behaviour, including cyberbullying, harassment, intimidation, discrimination or the sharing of harmful or offensive content, is not acceptable.

7.8.2 Online Risks and Student Protection

ASAD recognises that online risks may include:

- exposure to inappropriate or harmful content;
- unsafe online interactions, including contact with unknown or false identities;
- behaviours that may harm self or others, including cyberbullying;
- scams, phishing, gambling and other financial or illegal risks.

The school will implement systems, education and support mechanisms to reduce these risks and to promote student wellbeing.

7.8.3 Safeguarding Measures and Support

ASAD will:

- provide age-appropriate education to students on digital safety, responsible use and wellbeing;
- implement filtering, monitoring and supervision measures on school systems and networks;
- identify and support students who may be experiencing or engaging in harmful or risky digital behaviours.

Safeguarding concerns arising in digital contexts will be managed in line with the school's Safeguarding and Child Protection Policy and relevant ADEK requirements.

7.8.4 Reporting Concerns

Students, staff and parents or guardians are encouraged to report concerns relating to online behaviour or digital safety promptly so that appropriate support and intervention can be provided. Reports will be handled sensitively and in accordance with school safeguarding procedures.

7.8.5 Behavioural Expectations and Consequences

Breaches of digital safeguarding expectations or online behaviour standards may be addressed through:

- support and education;
- behaviour management processes;
- safeguarding interventions;

in line with the school's Student Behaviour Management and Wellbeing Policy and related procedures.

7.9 Filtering, Monitoring and Appropriate Supervision

Australian School of Abu Dhabi (ASAD) recognises the importance of appropriate filtering, monitoring and supervision to support safe, responsible and purposeful use of digital technologies. The school will implement

proportionate technical and organisational measures to protect students, staff and systems while supporting effective teaching and learning.

7.9.1 Filtering and Access Controls

ASAD will implement internet filtering and access controls on school-managed networks and systems to:

- reduce the risk of access to inappropriate, harmful or illegal content;
- support safeguarding and student wellbeing;
- align access with educational purpose and age-appropriateness.

Filtering measures are designed to balance protection with the need to support learning and inquiry and may vary according to year level, programme and learning context.

7.9.2 Monitoring of Digital Use

Use of school-managed digital systems, networks and devices may be monitored to:

- ensure compliance with this policy and related school procedures;
- support safeguarding and identify potential risks or concerns;
- maintain the security and integrity of school systems.

Monitoring is proportionate, safeguarding-led, and limited to school systems and networks, and handled under the Information & Data Protection Policy and Privacy Notice.

7.9.3 Educational Purpose and Supervision

ASAD will ensure that there is a clear educational purpose before allowing students to access the internet or digital tools during school hours.
Staff will:

- provide appropriate supervision and guidance during digital activities;
- support students in developing safe and responsible digital habits;
- adjust levels of access and supervision based on age, developmental stage and learning needs.

7.9.4 Review and Response to Digital Use

The school may review trends in digital use, including access patterns and filter violations, to:

- identify potential risks or concerns;
- inform preventative strategies and education;
- strengthen safeguarding and wellbeing support.

Concerns identified through monitoring will be addressed in line with this policy, the Safeguarding and Student Protection Policy, and relevant school procedures

7.9.5 Limitations of Monitoring

While ASAD takes reasonable steps to filter and monitor digital use on school-managed systems, no filtering or monitoring system can provide absolute protection. Students and parents or guardians share responsibility for promoting safe and responsible digital behaviour, particularly outside school hours and off school premises.

7.10 Digital Incidents and Breaches of Acceptable Use

Australian School of Abu Dhabi (ASAD) recognises that inappropriate or unsafe use of digital technology may occur and is committed to responding to digital incidents in a timely, proportionate and supportive manner. A digital incident occurs where a member of the school community engages in inappropriate, unsafe or unauthorised use of digital technologies, systems or platforms, including breaches of this policy.

7.10.1 Types of Digital Incidents

Digital incidents may include, but are not limited to:

- breaches of acceptable or responsible use expectations;
- accessing, creating or sharing inappropriate or harmful content;
- cyberbullying or harmful online interactions;
- misuse of school systems, accounts or devices;
- breaches of data protection, privacy or information security;
- unauthorised recording, sharing or publication of images, audio or video.

7.10.2 Reporting Digital Incidents

All staff, students, parents and authorised users are encouraged to report actual or suspected digital incidents promptly. Staff are required to report digital incidents in accordance with school procedures so that appropriate safeguarding, behavioural or technical responses can be implemented.

7.10.3 Lost, Stolen or Compromised Devices and Accounts

Where a personal or school-issued digital device is lost, stolen or suspected to be compromised while on school premises or used in connection with school activities, the following actions must be taken promptly:

- **Lost or stolen device:**
  The incident must be reported immediately to school staff or leadership so that appropriate safeguarding, security and access controls can be applied.
- **Suspected account compromise:**
  Users must change their password immediately (where possible) and notify the school's designated IT or data protection lead so that access can be reviewed and secured.
- **Suspected data exposure or unauthorised access to personal information:**
  The incident will be treated as a potential data breach and managed in accordance with ASAD's Information and Data Protection Policy, Data Protection Plan and Cybersecurity Incident Response procedures.
  Prompt reporting supports the protection of students, staff, school systems and personal information and reduces the risk of further harm.

7.10.4 Response and Support

ASAD will respond to digital incidents in a manner that:

- prioritises student safety, wellbeing and safeguarding;
- considers the age, developmental stage and circumstances of those involved;
- provides support, guidance and education where appropriate;
- applies behaviour management or disciplinary measures where required.

Responses will be guided by this policy and relevant school policies, including the Student Behaviour Management and Wellbeing Policy, Safeguarding and Student Protection Policy, Employment Policy, Student Wellbeing Policy and Staff Wellbeing Policy.

7.10.5 Escalation and External Reporting

Where required, digital incidents may be:

- escalated to school leadership;
- reported to the Abu Dhabi Department of Education and Knowledge (ADEK);
- referred to external authorities, including Abu Dhabi Police, in accordance with legal and regulatory requirements.

7.10.6 Recording and Documentation

All digital incidents will be:

- recorded and documented accurately;
- reviewed periodically to identify trends, inform preventative education and strengthen digital safeguarding practices;
- reviewed and signed by the Principal or delegated authority;
- stored securely in accordance with the ADEK *School Records Policy* and the school's Records Management Policy.

7.10.7 Review and Improvement

Digital incidents will be reviewed to:

- identify patterns or risks;
- inform preventative strategies and education;
- strengthen digital safeguarding and acceptable use practices.

7.11 Roles and Responsibilities

Australian School of Abu Dhabi (ASAD) recognises that the effective and responsible use of digital technologies is a shared responsibility across the school community. Clear roles and responsibilities support safe practice, accountability and consistency.

7.11.1 ASAD Leadership Team

School leadership will:

- ensure this ICT Acceptable Use & BYOD Policy is implemented, communicated and reviewed regularly;
- provide oversight of digital safeguarding, acceptable use and compliance with ADEK requirements;
- ensure appropriate systems, controls and resources are in place to support safe and responsible digital use;
- support staff through guidance, training and professional development;
- ensure digital incidents are managed, recorded and escalated where required.

7.11.2 Staff

All staff are expected to:

- model responsible, respectful and ethical digital behaviour;
- use school digital systems and devices in accordance with this policy and related procedures;
- provide appropriate and active supervision of students' digital use during learning activities, in line with age, context and safeguarding requirements;
- promote digital safeguarding, wellbeing and responsible online behaviour;
- report digital incidents, concerns or breaches promptly in line with school procedures;
- only use school-approved communication channels and must not use personal email accounts to communicate with students or parents/guardians;
- comply with ASAD's Digital Media and Social Media Policy, including restrictions on communicating with students and parents through personal social media accounts or messaging platforms.
- comply with data protection, privacy and academic integrity expectations.

7.11.3 Students

Students are expected to:

- use digital technologies, systems and devices responsibly and for authorised purposes only;
- follow staff instructions and school rules relating to ICT acceptable use and BYOD;
- respect the rights, privacy and wellbeing of others in digital environments;
- protect their account credentials and report concerns or misuse;
- engage honestly and ethically with digital tools in line with academic integrity expectations.

Expectations will be applied in an age-appropriate and developmentally appropriate manner across year levels.

7.11.4 Parents and Guardians

Parents and guardians are expected to:

- support the school's expectations for acceptable and responsible digital use;
- reinforce safe and respectful digital behaviour at home;
- ensure personal devices used under BYOD meet school expectations;
- engage with the school where concerns relating to digital use arise.

Parent and guardian responsibilities outside school hours are outlined further in Section 7.12 of this policy.

7.11.5 Visitors, Contractors and Other Authorised Users

Visitors, contractors and other authorised users are expected to:

- comply with this policy when accessing school systems, networks or devices;
- use digital access responsibly and only for authorised purposes;
- respect confidentiality, privacy and safeguarding requirements.

7.12 Parent and Guardian Responsibilities Outside School Hours

Australian School of Abu Dhabi (ASAD) recognises that the primary responsibility for students' use of personal digital devices outside school hours and off school premises rests with parents and guardians.
Parents and guardians are expected to:

- monitor and guide their child's use of digital devices, applications and online services outside school hours;
- support safe, responsible and age-appropriate digital behaviour at home and in the wider community;
- reinforce expectations relating to online safety, wellbeing and respectful behaviour;
- ensure that personal devices used by students comply with school expectations when brought onto school premises or used for school-related activities;
- engage with the school where concerns arise relating to digital behaviour, wellbeing or safeguarding.

While ASAD may respond to digital behaviour that impacts the school community, student wellbeing or safeguarding, this policy does not extend the school's supervision or control to personal device use outside school hours or off school premises.

7.13 Communication, Awareness and Age-Appropriate Access

Australian School of Abu Dhabi (ASAD) is committed to ensuring that expectations relating to acceptable and responsible digital use are clearly communicated, understood and applied across the school community.

7.13.1 Communication of the Policy

This ICT Acceptable Use & BYOD Policy will be:

- communicated to staff through induction, training and internal communications;
- shared with students in age-appropriate formats;
- made available to parents and guardians through appropriate school communication channels, including the school website and Parent Handbook.

The policy will be accessible to visitors and other authorised users where relevant. Access to school-managed digital systems, networks and devices is conditional upon acknowledgement of, and compliance with, this ICT Acceptable Use & BYOD Policy and any associated ICT Acceptable Use Agreement (Appendix A).

7.13.2 Student Awareness and Education

ASAD will support students to develop understanding of:

- responsible and safe use of digital technologies;
- online risks and digital wellbeing;
- expectations relating to behaviour, safeguarding and academic integrity.

Education and guidance will be embedded within the curriculum and pastoral programmes in a manner appropriate to students' age, developmental stage and IB programme.

7.13.3 Age-Appropriate Access and Adaptation

In line with ADEK requirements:

- age-appropriate versions or guidance relating to ICT acceptable use will be provided for younger students, including those in the primary years;
- parents and guardians will have access to the full version of this policy;
- expectations, supervision and access levels will be adjusted based on students' age, maturity and learning needs.

7.13.4 Ongoing Awareness and Review

ASAD will promote ongoing awareness of ICT acceptable use expectations through:

- regular communication and reminders;
- integration into wellbeing, safeguarding and digital citizenship initiatives;
- review of emerging risks and technologies.

7.14 Monitoring, Review and Policy Availability

Australian School of Abu Dhabi (ASAD) is committed to ensuring that acceptable and responsible digital use practices remain effective, current and aligned with legal, regulatory and educational requirements.

7.14.1 Monitoring and Oversight

Compliance with this ICT Acceptable Use & BYOD Policy will be monitored through:

- oversight of digital systems and network use;
- review of digital incidents and safeguarding concerns;
- feedback from staff, students and parents where appropriate.

Where concerns or patterns of non-compliance are identified, ASAD will take appropriate action to strengthen guidance, support or controls. Monitoring is proportionate, safeguarding-led, and limited to school systems and networks, and handled under the Information & Data Protection Policy and Privacy Notice.

7.14.2 Review of the Policy

This policy will be reviewed on a regular basis to ensure:

- ongoing compliance with ADEK requirements and applicable UAE legislation;
- alignment with International Baccalaureate standards and expectations;

- responsiveness to changes in technology, digital risks and school operations.

The policy will be formally reviewed at least annually, or earlier where required due to regulatory change, identified risks or significant incidents.

7.14.3 Policy Availability

This ICT Acceptable Use & BYOD Policy will be:

- made available to staff through internal school systems;
- published for parents and guardians on the school website and in the Parent Handbook, in line with ADEK requirements;
- shared with students in age-appropriate formats.

Related policies, including the Digital Policy, Information and Data Protection Policy, Academic Integrity Policy and Safeguarding and Child Protection Policy, will be referenced and made accessible to support consistent understanding and implementation.

8. COMPLIANCE

Compliance with this ICT Acceptable Use & BYOD Policy is mandatory for all members of the Australian School of Abu Dhabi (ASAD) community who access or use the school's digital systems, networks, platforms or devices. Compliance with this policy includes acknowledgement of, and adherence to, the ICT Acceptable Use & BYOD Agreement (Appendix A). Failure to sign/acknowledge the Agreement may result in restricted access to school digital systems and services.

This policy supports ASAD's obligations under:

- the ADEK School Digital Policy and other applicable ADEK regulations;
- relevant UAE legislation, including laws relating to child protection, cybercrime, copyright and data protection; and
- the International Baccalaureate (IB) standards relating to governance, safeguarding, academic integrity and ethical practice.

ASAD acknowledges that the Abu Dhabi Department of Education and Knowledge (ADEK) has regulatory authority and oversight responsibility for private schools in Abu Dhabi. ASAD will comply with ADEK directives, reporting requirements, inspections and audits relating to digital use, safeguarding, data protection and information security.

All students, staff, parents and guardians, visitors, contractors and other authorised users are required to comply with this policy in conjunction with ASAD's:

- Digital Policy;
- Information and Data Protection Policy;
- Academic Integrity Policy;
- Safeguarding and Student Protection Policy;
- Student Behaviour Management and Wellbeing Policy;
- Records Management Policy; and
- any related procedures or guidance issued by the school.

Failure to comply with this policy may result in appropriate action being taken in accordance with ASAD policies and procedures and, where applicable, ADEK requirements and UAE legislation. Compliance with this policy forms part of ASAD's broader governance, safeguarding, risk management and digital safety framework.

9. REFERENCES

This ICT Acceptable Use & BYOD Policy is informed by, and should be read in conjunction with, the following legislation, regulatory requirements, standards and school policies, as applicable.

- 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). (September). ADEK_School_Records Policy_v.1.1
- Abu Dhabi Department of Education and Knowledge (ADEK). (n.d.). Terms of Condition of Use, and Privacy Statement for Information.
- 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.
- International Baccalaureate Organization (IBO). (2020). *IB Standards and Practices.*
- 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?
- UAE Cybersecurity Council. (n.d.). UAE National Cybersecurity Framework

10. RATIFICATION & REVISION HISTORY

Document Title	ICT Acceptable Use and BYOD Policy
Version	v.1
Ratification Date	11th February 2026
Next Review Date	February 2027
Ratified By	Director: Mr. Adel Salman

APPENDIX A: ICT Acceptable Use & BYOD Agreement

Australian School of Abu Dhabi (ASAD)

I/We acknowledge that we have read and understood the Australian School of Abu Dhabi (ASAD) ICT Acceptable Use & BYOD Policy and agree to comply with the expectations set out in this Policy and in this Agreement.

I/We understand that:

- access to ASAD digital systems, networks, platforms and devices is provided for educational and operational purposes and is conditional upon compliance with school policies and procedures;
- use of ASAD school-managed systems and networks may be filtered and monitored for safeguarding, security and compliance purposes in accordance with ASAD's Privacy Notice and Information and Data Protection Policy; and
- breaches may result in restricted access and/or further action in line with ASAD policies and, where applicable, ADEK requirements and UAE legislation.

Student Name: _____	**Parent/Guardian Name: _____**
Year/Grade: _____	**Parent/Guardian Signature: _____**
Student Signature: _____	**Date: ___ / ___ / _____**
Date: ___ / ___ / _____	