YASMINA
BRITISH ACADEMY

Digital Policy 2025-26

Overview

At Yasmina British Academy (YBA), we believe that digital literacy and fluency are essential to preparing our students for their futures. Our digital approach empowers students and staff to use technology with confidence, creativity, and responsibility.

We are committed to developing a safe, secure, and innovative digital learning environment that supports student achievement, wellbeing, and digital citizenship, while ensuring compliance with all ADEK, UAE, and international data protection standards.

Summary

Policy First Issued on	September 2022
Next Policy Review Date	June 2028
Policy Amended	September 2026
Lead Professionals	Paul Dallyn
Signature(s)	
Approved by ELT	
Date	**September 2026**

Additional Documentation

1. Digital strategy

2. Responsible usage policies

3. Framework for the selection of external providers and products

4. Data and Cybersecurity Infrastructure

5. Response plan in relation to cybersecurity incidents

6. School data protection plan and policy

7. Digital media policy and social media policy

1. Digital Strategy Policy

PURPOSE

This Digital Strategy document outlines our vision, principles, and operational framework for integrating digital technologies into teaching, learning, and administration, ensuring compliance with UAE regulatory standards and international best practices.

Throughout this document, reference will be made to the ADEK Digital Policy sections via the use of [ ] brackets.

STRATEGIC DIRECTION

Purpose and Vision

Our schools are committed to leveraging technology to deliver improved student achievement and outcomes. We ensure that technology is used to enhance teaching and learning while supporting efficient and effective school administration. We recognise that digital competence is essential for students to thrive in education, work, and life, and we are dedicated to embedding digital skills across all aspects of our educational provision.

Key Strategic Elements

Enhancing Teaching and Learning

- Integrate digital tools and platforms into the curriculum to foster interactive, personalised, and engaging learning experiences.
- Define clear digital competencies and expected outcomes for each grade level, ensuring alignment with ADEK requirements.
- Provide differentiated digital resources and support to accommodate diverse learning needs, including students with additional educational requirements.
- Regularly review and update digital learning materials and methods to reflect emerging technologies and best practices.

Developing Digital Skills and Safety

- Invest in the development of students' digital skills and competencies to empower them to maximise learning opportunities presented by technology.
- Educate students on responsible, safe, and ethical use of digital resources, protecting them from inappropriate or harmful content and interactions.
- Foster digital citizenship and critical thinking to prepare students for participation in a digital society.

Supporting School Administration

- Deploy digital solutions to streamline administrative processes, improve communication, and support data-driven decision-making.
- Ensure that our digital infrastructure, including hardware, software, and connectivity, is robust, secure, and accessible to all staff and students.

Ensuring Digital Security and Compliance

- Establish and maintain systems, mechanisms, and procedures that safeguard digital security, data protection, and privacy in accordance with the Federal Decree Law No. (45) of 2021 on the Protection of Personal Data.
- Conduct regular risk assessments and reviews of our digital ecosystem to ensure it is secure and fit for purpose.
- Appoint a designated staff member of evert school to act as the main point of contact with ADEK on matters relating to our digital strategy.

Continuous Improvement and Stakeholder Engagement

- Form a Digital Wellbeing Committee or appoint a Digital Lead to oversee the implementation and annual review of the digital strategy.
- Gather feedback from staff, students, and parents to inform ongoing development and procurement of digital resources.
- Provide ongoing professional development and training for staff to ensure they are equipped to deliver digital learning objectives and maintain digital safety standards.

ASSISTIVE TECHNOLOGIES [2.1.2]

- Inclusive learning tools, including screen readers, text to speech, speech to text.
- Customisable accessibility settings to accommodate diverse learning needs.
- Assistive hardware integration, provide access to alternative input devices.
- Teacher training and support deliver ongoing professional development.

STUDENT DIGITAL SKILLS & COMPETENCIES [2.1.3]

- Digital Competencies curriculum embedded in core subjects.
- Cyber wellness programs promoting safe and ethical online behaviour.
- Opportunities for students to lead digital initiatives (e.g., coding clubs, innovation labs).

DIGITAL INFRASTRUCTURE, SOFTWARE & HARDWARE [2.1.4]

- Use of learning platforms (e.g., Microsoft Teams, LMS).
- Blended and remote learning protocols.
- 1:1 device programs.
- AI tools used ethically to personalise learning and assist teaching.
- High-speed internet in all campuses.
- Cloud-based systems for collaboration and storage.
- Assistive technologies for students with determination.
- Secure BYOD (Bring Your Own Device) policies.

SECURITY OF SCHOOLS' DIGITAL SYSTEMS [2.1.5]

- Secure storage of student, staff and school data in compliance with UAE law.
- Regular cybersecurity audits and vulnerability assessments.
- Mandatory training for staff and students on digital safety.
- Incident response plan for data breaches.
- Secure storage of student, staff and school data in compliance with UAE law.
- Regular cybersecurity audits and vulnerability assessments.
- Mandatory training for staff and students on digital safety.
- Incident response plan for data breaches

FUTURE-PROOFING THE SCHOOLS DIGITAL INFRASTRUCTURE [2.1.6]

- Adopt scalable cloud solutions, continued use of cloud-based platforms for storage, learning, and collaboration to support flexible access and future growth.
- Maintain up-to-date devices, standardise hardware across schools and implement a regular refresh cycle to keep technology current and consistent.
- Strengthen network infrastructure, ensure fast, secure Wi-Fi and broadband with capacity to support increasing numbers of users and devices.
- Enhance cybersecurity, apply strong data protection policies, reliable security tools, and provide regular training to reduce digital risks.
- Ensure system compatibility, choose digital tools and platforms that integrate smoothly, allowing for efficient data sharing and future upgrades.
- Provide ongoing staff training, equip staff with regular training and support to build confidence in using current and emerging technologies.
- Plan for sustainability and budgeting, include long-term planning for costs, energy efficiency, and responsible disposal or recycling of outdated equipment.

RESOURCES & INVESTMENT [2.1.7]

- Ensure all students and staff have equitable access to devices, digital tools, and reliable internet.
- Maintain sustainable budgeting for hardware, software, licences, and infrastructure upgrades.
- Prioritise scalable, cloud-based technologies to support long-term growth and flexibility.
- Invest in ongoing staff training to build digital confidence and capability.
- Monitor and evaluate the impact of digital investments to ensure value and alignment with learning goals.

STAFF TRAINING REQUIREMENTS [2.1.8]

- Annual digital skills assessments for staff
- Training in blended learning, AI integration, cybersecurity awareness.
- Instructional Technology Coaches are designated at each school.

EMERGING TECHNOLOGIES [2.1.9]

- Foster Innovation across schools, encourage the exploration and controlled implementation of emerging technologies - such as AI, AR/VR, and data analytics—to enhance learning, personalise

instruction, and improve operational efficiency.

- Align with Aldar Education's Strategic Goals, ensure that all new technologies directly support Aldar Education's vision for future-ready learners, innovative pedagogy, and world-class digital infrastructure
- Implement Ethical and Responsible Use, develop clear governance frameworks for the safe, ethical, and age-appropriate use of emerging tools, ensuring compliance with UAE regulations and global best practices.
- Empower Educators and Leaders, provide targeted CPD to equip staff with the knowledge and confidence to trial and integrate emerging technologies in the classroom and across school operations
- Evaluate Impact and Scalability, use evidence-based evaluation to assess the educational value and sustainability of emerging technologies, with a clear pathway for group-wide adoption where appropriate.

DIGITAL WELLBEING [2.2]

- Responsible Use agreements signed by staff (all), students and parents. There should also be one for SGC members and all visitors to school sites.
- Termly workshops for parents on EdTech tools and safety.
- Transparent reporting on digital initiatives and performance.
- Encourage healthy screen time, promote balanced use of digital devices through age-appropriate screen time guidelines and regular breaks.
- Teach responsible online behaviour, embed digital citizenship into the curriculum, covering online safety, privacy, respect, and cyberbullying prevention.
- Support student well-being, use digital tools to monitor and support student mental health and provide access to wellbeing resources where needed.
- Involve parents and staff, provide training and resources to help staff and families guide students in building healthy digital habits.
- Review and improve, regularly assess the impact of digital technology on well-being and adjust practices to ensure positive outcomes.

MONITORING AND EVALUATION

- Annual digital strategy review with KPI tracking.
- Technology usage metrics, from both staff and students.
- Student learning outcomes
- Staff satisfaction and readiness
- Incident reports (cybersecurity/digital misuse)

Additional resources can be access here

BYOD Specifications

ADEK Digital Policy

MDM Installation Guides

Online Platforms at YBA

2. Digital media policy and social media policy

1. Purpose

This policy is designed to:

- Ensure the safety and protection of students, staff and the wider YBA community when using social media.
- Provide clear guidelines for responsible use of social media platforms by all stakeholders.
- Educate students, staff and parents about digital citizenship, online reputation and ethical use of media.
- Safeguard personal information and uphold privacy in our digital communications.
- Maintain and enhance the reputation of YBA and reflect our values (Empower, Community, Culture of Innovation, Future-Proof, Dynamic).

2. Scope

This policy applies to all students, staff, governors, volunteers, contractors and any individual posting on behalf of, or representing, YBA.
It covers all forms of social media and digital communication including (but not limited to):

- Social networking sites (e.g., Facebook, Instagram, LinkedIn)
- Media-sharing platforms (e.g., YouTube, TikTok)
- Blogs, vlogs and micro-blogs (e.g., Tumblr, WordPress)
- Messaging and collaboration tools (e.g., WhatsApp, Teams, Slack)

3. Official YBA Social Media Platforms

YBA's official social media channels are authorised and managed by our PRE and the Executive Leadership Team (ELT). These platforms are the only ones representing YBA publicly.

- Facebook, Instagram, LinkedIn, ALDAR Live App
- Only designated and authorised staff members may post content on these official platforms.

4. Procedures for Access, Security and Password Protection

To ensure the integrity and security of YBA's social media accounts:

1. **Access Control**

- Access is restricted to authorised staff as approved by the Principal and the Digital IT Team
- A register of authorised users will be maintained and reviewed by IT and Communications teams.
- Any request for temporary access (e.g., for an event campaign) must be formally approved and revoked after use.

1. **Account Security Measures**

- All YBA social media accounts must use official school email addresses, not personal accounts.
- Multi-factor authentication (MFA) must be enabled wherever possible.
- Passwords shall be updated regularly (e.g., every three months) or immediately after a suspected breach.

2. **Password Protection Protocol**

- Passwords must be strong (minimum 12 characters, include uppercase & lowercase letters, numbers and special characters).
- Passwords must be securely stored (in an approved encrypted password manager).
- When authorised staff leave the organisation or change roles, their access is immediately revoked and passwords updated.

3. **Monitoring & Incident Response**

- The IT & PRE teams will conduct regular audits of account access and usage.
- Any suspected breach or unauthorised access must be reported immediately to the Principal and the Head of Operations. The response will include resetting passwords, reviewing logs, and implementing remediation measures.

5. Content Guidelines - Language, Engagement and Tone

To ensure that all content aligns with YBA's mission, ethos and community standards:

- **Accuracy & Relevance:** All posted content should be accurate, relevant, reflect YBA's vision, values and the school's culture of innovation.
- **Cultural Sensitivity:** Content must respect the cultural norms and values of the UAE and ensure inclusivity and respect across all posts.
- **Privacy Considerations:** Before posting names, photos or videos of students, parents or staff, explicit written consent must be obtained in line with YBA's Digital Media Policy.
- **Educational Value:** Priority should be given to posts which support educational development, highlight student achievement, innovation, entrepreneurship and the futures-oriented curriculum.
- **Professional Tone:** Use respectful, inclusive, clear and concise language. Avoid discriminatory, defamatory or inflammatory remarks.
- **Engagement With Other Accounts:** Interactions with other organisations, institutions and the community must reflect YBA's professionalism, avoid conflicts or negative public discourse and handle criticism through internal channels.

6. Use of Student Names, Photographs and Videos

To safeguard student privacy and ensure appropriate use of digital media:

- Written consent from parents/legal guardians must be secured before using any student's name, image or video on social media, website or promotional materials. Consent to be obtained at enrolment and renewed annually
- By default, only first names may be used when referring to students unless explicit parental consent is given for full name use.
- Images/videos must be carefully selected so as not to compromise student privacy (e.g., not reveal personal identifying info or location)

- All media must be stored securely and accessed only by authorised staff prior to publication.
- No manipulations or edits should mis-represent students, or potentially embarrass or diminish their wellbeing.
- Student-related media must only be published on official school-approved platforms by authorised staff; posting on personal social media by staff/parents without approval is strictly prohibited. Live-streaming of students requires prior leadership approval and must adhere to ADEK guidance.

7. Guidelines for Personal Social Media Use by Staff

Staff have personal social media accounts, but must be aware of how their online behaviour interacts with their professional role at YBA:

- Personal accounts should use tight privacy settings; staff should avoid identifying themselves as representing YBA on personal accounts (except professional platforms like LinkedIn).
- Staff must not accept "friend" or connection requests from current students (or former students under 18) via personal accounts, nor initiate them.
- Communication with current students or parents through personal social media or messaging apps is prohibited.
- Content shared on personal accounts must align with YBA values, must not breach confidentiality, must not constitute bullying, harassment or discrimination and must comply with UAE cultural considerations.
- No confidential or sensitive school information should be posted or shared via personal accounts.

8. Monitoring, Enforcement & Consequences

- YBA reserves the right to monitor social media activities on official platforms and intervene when necessary.
- Violations of this policy may lead to disciplinary action, which could include suspension, dismissal or expulsion depending on severity.
- The Communications & Digital Strategy Lead and IT Department are jointly responsible for moderating content, investigating incidents, removing inappropriate content and ensuring compliance with YBA and ADEK policies.
- Regular audits of social media platforms will be carried out. Incidents must be reported promptly through the formal incident-reporting process.

9. Education & Support

As part of our 'Digital Wellbeing Strategy, YBA will provide ongoing training, workshops and resources for students, staff and parents on safe and effective social media use, digital reputation, online wellbeing and cyber-citizenship.

10. Alignment with YBA's Digital Strategy & Values

This policy supports YBA's three-year Digital Strategy and our published vision emphasising: Culture of Innovation, Community, Empowerment, Dynamic learning and Future-Proof students. It complements our broader frameworks such as the 'Futures' curriculum and the Digital Wellbeing Strategy.

3. Responsible Use Policy

1. Rationale

YBA recognises that personal mobile and portable digital devices, together with network connectivity, offer significant opportunities for learning and innovation. At the same time, we acknowledge the responsibilities associated with Bring Your Own Device (BYOD) usage and online safety. This policy sets out clear guidelines for the responsible, secure and effective use of student-owned devices and networked resources within our school environment.

2. Strategic Context

As part of our Digital Strategy (focusing on Culture of Innovation, Empower, Community, Dynamic and Future Proof), YBA is committed to:

- leveraging a robust BYOD provision to enhance teaching and learning;
- supporting student digital fluency and wellbeing;
- ensuring safeguarding, data protection and compliance with our policy frameworks (including Abu Dhabi Department of Education and Knowledge - ADEK);
- establishing clearly defined responsibilities for students, staff and parents in relation to device use and online safety.

3. Scope

This policy applies to all students of YBA (Years 5-13), their parents/guardians, and staff. It covers the use of all personal electronic devices brought into the school setting for educational purposes (e.g., tablets, laptops, Chromebook, iPad) as part of our BYOD programme, and their use on the school network or in blended/remote learning modes.

4. BYOD Specification & Access

4.1 Device Specification

- Students from Years 2-8: a tablet device (recommended: Apple iPad) meeting recommended minimum specifications published by the school each year.
- Students from Years 9-13: a laptop or tablet device suitable for secondary curriculum requirements (minimum specification to be published).
- Mobile phones and smart watches: The school policy prohibits the use of mobile phones in class and may restrict smart watch functionalities (e.g., messaging) unless used for authorised educational purposes.

4.2 Network & Management

- All BYOD devices must be registered with and managed through the school's Mobile Device Management (MDM) system (e.g., Jamf School & Jamf Parent) to ensure secure configuration, filtering, monitoring and safe access.

- Only devices compliant with the school's BYOD specification and software profile may access the school network.
- Students must bring devices fully charged; the school does not guarantee charging facilities.
- The network access for BYOD is restricted to one personal device per student unless otherwise authorised.

5. Responsible Use of Devices & Network

Students, staff and parents must adhere to the following principles:

- Ethical Use: Devices and network resources must be used honestly, lawfully and in alignment with the school's values.
- Respectful Behaviour: Online interactions must be courteous, considerate and free from cyber-bullying, harassment or other inappropriate conduct.
- Educational Focus: Device use must support learning. Personal or recreational use that distracts from learning or the teaching environment is not permitted during lesson time.
- Security & Privacy: Users must protect login credentials, adhere to data protection protocols, and follow school guidance on device and network security (including virus protection, updates and backups).

6. Permitted Use & Areas of Access

- Devices may be used in the classroom under the direction of a teacher or member of staff.
- Devices must remain in bags (and powered off or in silent mode) when outside supervised classroom lessons—e.g., corridors, playground, canteen, toilets—unless explicitly permitted by staff.
- Use outside of class (e.g., for collaborative work on interactive displays) is permitted only under teacher supervision.
- Parents/guardians must not contact students via their BYOD device during school hours except via approved school communication channels.

7. Loss, Damage & Responsibility

- Ownership of the BYOD device remains with the student/parent. YBA accepts no liability for loss, theft or damage to the device whilst on school premises, on school-sponsored trips or during transit to/from school.
- It is recommended that devices are protected with cases, a "Find My Device" service is enabled and suitable insurance considered.
- Students are responsible for the physical security, maintenance and software integrity of their device.

8. E-Safety and Prohibited Use

8.1 Prohibited Content & Activities

The school network and student-owned devices must not be used for:

- Accessing, storing, creating, transmitting or receiving material which is illegal, abusive, harassing, defamatory, obscene, indecent, pornographic, age-inappropriate, of extremist nature, discriminatory, or otherwise objectionable;

- Cyber-bullying, harassment, trolling, impersonation, arranging to meet individuals first met online without parent/staff approval;
- Unauthorized uploading or downloading of software, games, peer-to-peer file sharing, hacking, altering system settings, introducing malware, or other activity that disrupts network services;
- Commercial activity (unless as part of an approved educational project), gambling, scams, phishing, misuse of copyrighted material or intellectual property rights violation.

8.2 School Responsibilities

YBA will:

- Provide age-appropriate education and training on online safety, digital citizenship, risks and responsible behaviour;
- Ensure appropriate filtering and monitoring of the school network and devices;
- Maintain incident reporting and response protocols for misuse, including escalation to safeguarding leads and external agencies when required.

8.3 Student Responsibilities

Students must:

- Use BYOD devices and network access only with teacher permission and in alignment with this policy;
- Only access curriculum-relevant resources, sites and applications;
- Seek permission before connecting removable storage or linking devices to the school network;
- Respect other users, report any concerns or security breaches, and avoid sharing personal details, images or videos without consent.

8.4 Staff & Parent Responsibilities

- Staff: model responsible use, monitor student behaviour, reinforce policy expectations and report breaches;
- Parents/guardians: support safe and appropriate device use at home/outside school hours, engage with training and policy reminders, and monitor their child's digital behaviour in partnership with the school.

9. Sanctions & Consequences for Misuse

Any breach of this policy may result in:

- Removal of network access for the student's device;
- Temporary or long-term confiscation of the device by staff pending parent discussion;
- Referral under the school's Behaviour for Learning Policy and, if necessary involving ADEK or law enforcement agencies in serious cases of misuse.
  YBA reserves the right to inspect, search or delete materials on student-owned devices if there is a reason to believe that misuse has occurred.

3. Framework for the selection of external providers and products

1. Purpose

The purpose of this framework is to ensure that all external providers, vendors, applications, and digital products used by Yasmina British Academy (YBA) are selected, implemented, and reviewed through a consistent, transparent, and secure process that:

- Aligns with **ADEK**'s Digital Policy (Section 5.5);
- Protects student and staff data in compliance with UAE Federal Decree Law No. (45) of 2021 on the Protection of Personal Data;
- Safeguards the cybersecurity, wellbeing, and privacy of the school community;
- Ensures educational value, inclusion, and age appropriateness of digital tools;
- Supports the school's strategic priorities under its Digital Strategy and Culture of Innovation vision.

2. Scope

This framework applies to the evaluation and approval of all third-party digital systems, software, applications, learning platforms, hardware vendors, and IT service providers that:

- Interact with YBA's data, systems, or network;
- Are used by students or staff for teaching, learning, communication, or administration;
- Form part of procurement, subscription, or licence agreements entered into by the school.

It applies to all departments, including academic, operational, and support functions.

3. Principles

1. Educational Value: The product or service must directly enhance learning, teaching, wellbeing, or operational efficiency.
2. Safety and Compliance: All vendors must comply with UAE data protection laws, ADEK requirements, and YBA safeguarding standards.
3. Security and Reliability: All systems must demonstrate strong cybersecurity practices, business continuity, and reliability.
4. Inclusivity: The provider must offer accessibility features that support diverse learners, including students of determination.
5. Transparency and Accountability: Procurement and evaluation processes must be documented and auditable.

4. Selection and Approval Process

4.1 Initial Evaluation

The requesting department (e.g. teacher, faculty, or admin unit) must submit a Digital Product Proposal Form to the Digital Strategy Team, including:

- Purpose and intended educational use;
- Target user group (staff, students, parents);
- Type of data collected and stored;
- Required integrations with existing systems;
- Estimated cost, duration, and vendor contact details.

No new application or platform may be trialled or purchased without prior approval.

4.2 Technical and Security Review

The IT Manager and Digital Strategy Lead will evaluate the product against the following criteria:

Criterion	Key Requirements
Compatibility	Interoperability with existing YBA systems and infrastructure (e.g., LMS, MDM, email domains).
Data Security	Encryption (in transit and at rest), secure data storage location (preferably within UAE / GCC region), data deletion controls.
Access Control	Multi-factor authentication, user role management, single sign-on (SSO) if applicable.
Cybersecurity Compliance	Conformance with recognised standards (ISO 27001, NIST, or equivalent).
Vendor Credibility	Demonstrated track record in the education sector; references from other UAE or international schools.
Support & Maintenance	Availability of local support, updates, and service-level agreements (SLAs).
Cost & Licensing	Transparent pricing model, clear renewal terms, and absence of hidden fees.
Educational Suitability	Content is age-appropriate, inclusive, culturally sensitive, and pedagogically sound.

4.3 Data Protection Assessment

The **Data Protection Officer (DPO)** must verify that:

- The provider complies with Federal Decree Law No. (45) of 2021;
- Any transfer of data outside the UAE meets legal adequacy standards;
- A Non-Disclosure Agreement (NDA) or Data Processing Agreement (DPA) is signed;
- Consent requirements (parent/student) are identified where applicable;
- The provider's data retention, deletion, and breach notification processes are documented.

4.4 Educational Evaluation

The **Academic or Department Lead** will assess:

- Alignment with curriculum objectives and learning outcomes;
- Usability, accessibility, and inclusivity for all learners;
- Pedagogical impact (including feedback from pilot users if available);
- Potential duplication with existing tools.

4.5 Approval and Registration

Once all reviews are complete, the Digital Strategy & Wellbeing Committee will:

- Approve or reject the application;
- Record the decision in the Digital Product Register, noting purpose, data type, licence details, and review dates;
- Ensure communication to relevant stakeholders (teachers, IT, admin).

No external digital service may be deployed without this recorded approval.

5. Ongoing Monitoring and Review

- All approved vendors and products must be reviewed annually to confirm continued compliance with security, functionality, and educational value.
- Usage data, performance feedback, and any incidents will be logged and assessed.
- Products that no longer meet YBA or ADEK standards will be phased out.
- Any data breaches, misuse, or vendor non-compliance will trigger immediate review and escalation to ADEK where required.

6. Roles and Responsibilities

Role	Responsibility
Principal	Final authority for approving major procurements and ensuring compliance with ADEK policy.
Assistant Principal - Digital Strategy	Oversees implementation of the framework, ensures alignment with digital strategy.
IT Manager	Conducts technical and cybersecurity assessments; maintains product inventory.
Data Protection Officer (DPO)	Ensures all vendors meet legal and data-protection standards.
Department Leads / Teachers	Identify educational needs, propose tools, and ensure responsible classroom use.
Procurement / Finance Team	Manage financial due diligence and contract terms.

8. Compliance

Failure to follow this framework may result in:

- Withdrawal of system access;
- Disciplinary measures for staff where due process has not been followed;
- Vendor contracts being terminated where compliance issues are identified.
  YBA reserves the right to report serious data or security breaches to **ADEK** and relevant authorities as per legal requirements.