

AI & TECHNOLOGY POLICY (AY 2026-27)

UAE School Inspection Framework Alignment

This policy aligns with the UAE School Inspection Standard

- 4.1 Curriculum Design and Implementation: Elements
 - 4.1.1 Rationale, Balance and Compliance and
 - 4.1.4 Cross-curricular Links and Standard
- 5.1 Health and Safety, Including Arrangements for Child Protection/Safeguarding: Element
 - 5.1.2 Arrangements to Ensure Health, Safety and Security.

Policy

1. AI and Digital Literacy

- 1.1 **Curriculum Integration:** Bright Riders School is committed to developed students' AI and digital literacy through their curriculum with increasing technical complexity, in line with [Appendix A. AI Literacy Requirements](#).
- 1.2 **AI Learning Outcomes Monitoring and Reporting:** BRS has adopted a Learning Management System (LMS) that integrates AI standards and learning outcomes, ensuring that student AI literacy data is accessible to ADEK for regulatory monitoring.
- 1.3 **AI Literacy Assessment:** BRS is working continuously to ensure that every student graduates with demonstrated AI literacy, assessed through students' application of knowledge and skills in authentic, real-world contexts and adapted for students with additional learning needs, in line with the [Inclusion Policy](#).

2. AI Learning Tools

- 2.1 **AI-Powered Personalized Learning:** Bright Riders School is committed to implement at least one of the AI-powered personalized learning tools ("AI learning tools" including chat or non-chat-based AI tutors) that meets the requirements of Appendix B. AI Learning Tool Criteria and obtain ADEK approval before deploying any tool by completing the "ADEK AI Learning Tool Vetting Form". School has set screen time limitations to maximize learning.

- 2.2 **Foundational “AI for Teaching” Competency:** Bright Riders school has ensured that all relevant teaching and teaching support staff complete foundational training on the use of AI learning tools to identify students’ strengths and weaknesses and adapt teaching methods to address learning gaps, in line with [Appendix C. Pedagogical Requirements for the Use of AI Learning Tools](#).
- 2.3 **AI Learning Tool Training for Students:** BRS is committed to train all students on the use of their deployed AI learning tools, ensuring students’ ability to navigate the tool, use the tool to support their own learning, prompt (if applicable), abide by safety guardrails, and engage in responsible use.

3. Institutional Readiness

- 3.1 **Digital Strategy:** BRS has developed and implemented an annual school-wide digital strategy for the use of AI and technology to improve student achievement, teaching pedagogy, and school operations.
- 3.2 **Continuous Professional Development (CPD) in AI:** The school ensures staff attendance at all ADEK-mandated training (general and role-specific, when applicable). The staff is also provided CPD opportunities in human-centered AI use, ethical and responsible AI practices, AI systems and applications, AI-enabled pedagogy, AI for professional growth and improvement, and cybersecurity and digital safety.
- 3.3 **Digital Infrastructure and Systems:** BRS is committed to maintain reliable digital infrastructure and systems (e.g., networks, applications, devices, and services), in line with [Appendix D. Technical Requirements](#), including but not limited to secure school-issued devices and safety measures for Bring Your Own Device (BYOD) arrangements, staff access to digital systems and platforms provided by ADEK, readiness for ADEK-approved distance learning, and any assistive technologies, in line with the [Inclusion Policy](#).

4. Responsible Use

- 4.1 **Responsible Use Policies:** BRS regulates the responsible use of AI and technology to protect and maximize learning, ensure ethical academic behavior and oversight, and safeguard user wellbeing, including the requirements in [Appendix E. Responsible Use and Safeguarding Elements](#) through age- and culturally-appropriate policies for students, staff, parents, and other users.
- 4.2 **Student Phone Usage:** Students are not authorized to use personal mobile phones on school premises during the school day (unless explicitly and exceptionally authorized by a teacher for learning purposes). BRS ensures that other SIM-enabled devices (e.g., smart watches) are communication-disabled and that devices necessary for learning (e.g., tablets, laptops) are only used for learning purposes and actively monitored to prevent distraction.

- 4.3 **Student Social Media Usage:** Students are not authorized to use social media, in line with Cabinet Resolution No. (106) of 2026 Regarding the Regulation of Children's Access to social media and its amendments.
- 4.4 **Virtual Private Networks (VPNs) Usage:** BRS does not authorize the use of VPNs on any device on school premises and networks.
- 4.5 **Parent Partnership:** We, at Bright Riders School, regularly inform parents of their obligation to monitor their child's digital behavior outside school and limit social media use for children aged 15 and under, in line with Federal Decree Law No. 26 of 2025 on Child Digital Safety and Cabinet Resolution No. (106) of 2026 Regarding the Regulation of Children's Access to Social Media and their amendments.

5. Security

- 5.1 **Vendor Selection:** BRS has established procedures for selecting and managing external technology vendors, products, and services that meet ADEK requirements and UAE laws.
- 5.2 **Digital Incidents:** We identify, manage, document, respond to, and report digital incidents, supporting affected students and informing parents as applicable, in line with [Student Protection Policy](#), [Student Behavior Policy](#), [Records Policy](#), and applicable UAE laws.
- 5.3 **Data Protection and Cybersecurity:** BRS is committed to implement and maintain data protection and cybersecurity measures, in line with [Appendix D. Technical Requirements](#), Federal Decree Law No. 45 of 2021 on the Protection of Personal Data, Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes, and Federal Decree Law No. 26 of 2025 on Child Digital Safety, and their amendments, and any other laws and requirements issued by relevant government authorities.
- 5.4 **Digital Communication and Social Media:** Bright Riders School has implemented the secure storage and appropriate use of digital media, establish controls for official school social media accounts, monitor official and unofficial school-related communication channels, and obtain parental consent before recording or publishing identifiable student digital media.
- 5.5 **Staff Personal Communication Practices:** BRS has informed staff of unauthorized practices, including the use of personal email or social media accounts to communicate with current students, former students aged below 18, or parents, or the use of personal social media accounts to disseminate confidential school information or content that may be inappropriate, discriminatory, harmful, or perceived as endorsed by the school.

6. Communications

- 6.1 **School Website:** Bright Riders School maintains an updated school website containing all ADEK-mandated information.

Appendix A. AI Literacy Requirements

Bright Riders School is committed to implement the [ADEK K-12 AI Literacy Framework](#) as follows:

1. **Integrating AI Literacy into the Curriculum:** Ensure that students develop the four interconnected AI literacy strands through their curriculum: AI Conceptual Understanding; Critical Evaluation and Informed Interaction; AI Creation, Engineering, and System Design; and Responsible Governance, Data Privacy, and Societal Impact.
2. **AI Learner Profiles and Phasing:** BRS is committed to introduce the four AI literacy strands across four developmental phases and learner profiles, progressing with increasing technical complexity. The core competencies that students should aim to meet for each of the four AI learner profiles are defined in [Table 1. AI Learner Profiles and Phases](#):

[Table 1. AI Learner Profiles and Phases](#)

Phase/Cycle	AI Learner Profile	Core Competency Milestone
Phase 1/KG: KG1–KG2/FS2-Year 1	AI Aware Explorer	Explores inputs and responses through play Students distinguish between human senses and basic machine inputs and understand cause-and-effect relationships. Learning is unplugged with no direct AI tool use.
Phase 2/Cycle 1: Grades 1–5/Year 2-6	AI Literate Thinker	Applies rules, logic, and data to generate and evaluate outputs. Students progress from rule-based thinking to multi-step logic, develop understanding of how data influences outcomes, and begin interacting with AI tools to refine outputs.
Phase 3/Cycle 2: Grades 6–8/Year 7-9	AI Solution Builder	Designs and improves AI-powered solutions using data, models, and workflows. Students build, evaluate, and refine solutions using structured processes and foundational ML concepts.
Phase 4/Cycle 3: Grades 9–12/ Year 10-13	AI Systems & Solutions Designer	Designs and governs integrated AI systems. Students develop real-world solutions using systems thinking and ensure effectiveness, responsibility, and alignment with societal and governance expectations.

3. **Learning Objectives and Competencies:** BRS has adopted a spiral learning design for its AI curriculum, revisiting foundational concepts with increasing complexity across grades.
4. **Mode of Integration:** BRS has integrated AI literacy into their curriculum using one of the following modes:
 - a. Stand-alone: AI is taught as a single, stand-alone unit or module as part of a dedicated ICT subject (e.g., Computer Science, Technology, ICT, etc.) with a specified minimum number of credit hours each year for each phase.
 - b. Embedded: AI is embedded in multiple subjects and topics, rather than limited to stand-alone subjects (e.g., AI in Math, Science, etc.), to support authentic learning experiences and the application of AI understanding in real-world and interdisciplinary contexts.
 - c. Hybrid: AI is taught both through the school's dedicated ICT subject and also embedded across multiple subjects and topics.

Appendix B. AI Learning Tool Criteria

BRS committee to apply [Table 1. Mandatory AI Learning Tool Criteria](#) when evaluating AI learning tools.

Table 1. Mandatory AI Learning Tool Criteria

Criterion	Evaluation Questions and Requirements
Safety and Self-Harm Detection	1. Does the tool detect expressions of self-harm, suicidal ideation, abuse, or severe distress (if applicable)? 2. Upon detection, does it immediately alert the teacher and/or the school administrator (if applicable)? 3. Does the tool allow teachers to customize safety/self-harm guardrails through prompting and/or configuration features?
Cultural Content Filtering	1. Does the tool detect and filter out culturally inappropriate content through chat-based customization or configuration set-up? Culturally inappropriate content includes: • human reproduction and evolution dogma • alternative gender identity and sexual orientation • alcohol and drugs • religious/political indoctrination 2. Does the tool alert the teacher and/or the administrator?
Academic Integrity	1. Does the tool detect and block plagiarism attempts?

Teaching Pedagogy	- Does the tool employ evidence-based pedagogical approaches, including one or more of: - Socratic questioning (guiding students to answers through probing) - mastery learning (requiring proficiency before advancing) - spaced repetition (scheduling review at intervals for long-term retention) - retrieval practice (testing recall rather than re-reading) - Does it guide students to think and reason rather than simply providing answers?
Curriculum and Content Integration	- Does the tool integrate your school's curriculum standards (e.g., UAE Ministry of Education (MoE), UK National, US Common Core, International Baccalaureate (IB), and CBSE)? OR Can the school or teacher upload customized standards/learning outcomes? - Does the tool link/tag and report on the mastery of curriculum standards/learning outcomes
Assessment and Learning Resources	- Does the tool provide pre- and post- assessments capturing students' learning outcomes at the start and end of each unit? - Can the teacher use the tool to generate customized lesson plans, presentations, practice sets, quizzes, differentiated tasks, and formative assessment items aligned to their curriculum standards and class needs (if applicable)? - Can the teacher edit, adapt, or reject AI-generated content before publishing to students (if applicable)?
Teacher Interface: Student-Level Activity	- Can the teacher view all of the below for each individual student: - learning gaps - student engagement - time spent on tool - completion progress for assigned tasks - completion rates for assigned tasks - student attainment by learning outcome - student progress by learning outcome - full conversation log/chat history (if applicable) - performance trends over time - Are learning concerns identified to the teacher? - Does the tool generate detailed progress reports showing mastery trends over time?

Teacher Interface: Class-Level Activity	• Can the teacher view class-level analytics including all of the below: • learning gaps • student engagement • time spent on tool • completion progress for assigned tasks • completion rates for assigned tasks • performance trends over time • comparison of individual student performance against the class baseline
Administrator Access	1. Can the school administrator view: • teacher usage and interactions with the tool • student engagement • student completion of assigned tasks • full conversation log (chat history) for students flagged on safety, self-harm, and cultural inappropriateness (if applicable) 2. Can the administrator manage user accounts, permissions, and tool configurations at school level? 3. Can ADEK be granted system-level administrative access to conduct quality assurance reviews?

Guardrail Prompt for AI Learning Tools

Teachers copy/paste or embed this prompt within the AI learning tool interface, including in chat instructions for class and space creation, lesson and assignment generation, and/or system prompt settings to guide and constrain the AI's responses before student interaction.

Prompt:

You are an AI tutor configured for use in UAE schools. You must comply with UAE cultural and legal norms at all times.

Core rules:

1. *Restrict all responses to the assigned lesson topic only.*
2. *Decline any questions about human reproduction and evolution dogma, alternative gender identity and sexual orientation, alcohol and drugs, religious/political indoctrination.*
3. *Do not provide any contact numbers for support to students in any case.*
4. *For any child protection or safeguarding concerns detected, encourage students to reach out to a teacher, principal, school counselor, or other responsible adult.*
5. *Never engage with anything that could harm a student. Always direct concerns to a trusted adult or school counselor.*
6. *Encourage respectful, positive communication. Calmly redirect rude or off-topic messages back to the lesson.*
7. *Reflect UAE values in every response. Avoid anything that conflicts*

with Islamic values or UAE norms. Never criticize any religion, culture, or nationality.

8. *When food comes up, promote healthy, balanced eating. Never reference foods prohibited under Islamic dietary guidelines. Support positive body image.*

Appendix C. Pedagogical Requirements for the Use of AI Learning Tools

Teachers and teaching assistants using AI learning tools meet the following requirements:

Curriculum Alignment:

1. Ensure guardrails for safety and cultural appropriateness are in place for safety, self-harm, and cultural appropriateness using the prompt outlined in [Guardrail Prompt for AI Learning Tools \(Appendix B\)](#).
2. Assign age-appropriate learning tasks that are directly aligned to the curriculum standards/learning outcomes.
3. Adapt tasks by ability level to ensure all students, including those with additional learning needs, receive tasks appropriate to their skill level.

Content and Lesson Generation:

1. Generate lesson plans, presentations, practice sets, and differentiated learning materials using AI learning tools.
2. Verify factual accuracy and ensure curriculum alignment of AI-generated lesson plans and resources.

Monitoring Student Learning:

1. Screen and monitor student- and class-level performance utilizing the AI learning tool to identify learning gaps and introduce interventions, as needed:
 - a. If a majority of students are showing learning gaps on a specific concept (e.g., calculating areas under curves, understanding how enzymes work, writing using active voice), teachers cover these concepts in more details during the subsequent synchronous lessons to close the gap at the class-level (Tier 1).
 - b. If only one or a few students are having difficulties, teachers provide more targeted 1:1 or small-group interventions (Tier 2 or 3) as required (e.g., brief 5-minute sessions through individual office hours, a synchronous 5–10-minute sub-session for the target group or individual while the rest of the class is working on asynchronous work).
2. Reconfigure the AI learning tool to test whether students have understood the concepts and to validate if the intervention was effective in closing the learning gaps.
3. Review student-level data on AI learning tools weekly to ensure student engagement and completion of assignments, while monitoring off-topic inappropriate content on the AI learning tool.

4. Review overall class-level student data on AI learning tools daily to identify emerging learning gaps and adjust upcoming lesson plans accordingly.
5. Use performance data to guide 1:1 check-ins and small-group interventions. AI data is informed, not replaced, teacher professional judgement about a student's progress.
6. Alert the Student Welfare Lead (during distance learning) or Child Protection Coordinator (during on-site learning) immediately if a student shows distress, self-harm ideation, abuse disclosures, or seriously inappropriate messaging via AI interactions.
7. Monitor for over-reliance on AI (cognitive offloading), such as verbatim submissions or skipped reasoning, and address it by reinforcing expectations for genuine effort.

Appendix D. Technical Requirements

Data Protection and Privacy

BRS collects, processes, stores, shares, retains, and disposes of personal data lawfully, fairly, transparently, and securely. Accordingly, BRS is committed to implement the following:

1. **Data Protection Plan:** Outlining the categories of personal data authorized for collection and processing, procedures for obtaining parental consent (where required), data classification and access authorization requirements, data retention, backup, recovery, and disposal requirements, and conditions and safeguards for sharing personal data with third parties.
2. **Consent and Data Sharing Process:** Including confidentiality, non-disclosure, and data protection requirements in agreements with third parties that process personal data, including obtaining written parental consent (as part of the Parent School Agreement) for all digital tools that the school may use that collects, processes, or stores student personal data.
3. **Student Digital and AI Tools:** Collecting separate, explicit consent for AI learning tools, clearly informing parents regarding the purpose, use, storage, and sharing of student personal data, and the ability to opt out (with alternative learning arrangements). Tools do not use student personal data for commercial purposes, profiling, unauthorized third-party sharing, or AI model training, and shall delete or anonymize student personal data within 90 days of a student leaving the school, with written confirmation from the service provider upon request.

Cybersecurity

Bright Riders School has implemented and maintained cybersecurity measures that protect digital systems, information assets, and users from unauthorized access, misuse, loss, disruption, and cyber threats, including:

1. **Access Controls:** Multi-factor authentication across critical services and defined/enforced role-based access controls to ensure users have appropriate permissions.
2. **Data Encryption:** Encryption for data in transit and at rest to safeguard sensitive information.
3. **Network Security:** Next-generation firewalls and intrusion detection/prevention to protect against unauthorized access, ensuring enforcement of web filtering policies, ability to block inappropriate content and detect infected machines across the network, identity-based firewalls for granular visibility on user browsing activity, unified security edge architecture for all internet browsing.
4. **Endpoint Protection:** Updated anti-virus/malware software of all school-managed devices and hard disk device encryption (ensuring regular security patching).
5. **Data Backup and Recovery:** Automated regular backup procedures for critical data, software, and configuration settings are performed in line with the ADEK School Records Policy with regard to frequency and appropriate period of time (ensuring backups are vaulted and stored offline, securely and separately from the school network), a robust disaster recovery plan to minimize downtime in case of a security incident, and cloud-synced data for schools that use external cloud systems for storage.
6. **Data Security:** Data classification controls across school and student data, with Data Loss Prevention Tools to protect against data leaks or exfiltration.
7. **Security Awareness Training:** Regular training for staff and students to raise awareness about cybersecurity threats and best practices.
8. **Incident Response and Business Continuity Plans:** Updated plans to address security breaches promptly and effectively, performing a tabletop cyber-attack simulation and exercise with school management involvement, and guiding staff on process for maintaining business continuity.
9. **Physical Security:** Secure access to physical servers, networking equipment, and other critical infrastructure.
10. **Regulatory Compliance:** Compliance with local and international data protection regulations and standards.
11. **Monitoring and Logging:** Comprehensive monitoring systems to detect and respond to security incidents in real time, maintaining detailed logs for auditing and analysis purposes.
12. **Secure Software Development:** Secure coding practices when developing or procuring educational software, regularly update and patch software to address

vulnerabilities.

13. **Cloud Security:** If using cloud services, ensure the selected providers adhere to stringent security standards. Implement proper configuration and access controls for cloud resources, integrating Cloud Services – Software as a Service (SaaS) with school identity services where possible, and establish Cloud SaaS Security Posture Management capabilities.
14. **Collaboration Security:** Secure communication and collaboration platforms to protect sensitive educational information shared among students and staff.
15. **Third-Party Security:** Vet and monitor third-party vendors providing educational technology solutions to ensure they meet security standards.
16. **System Maintenance:** Regularly maintained and updated digital infrastructure, operating systems, security systems, and software, including antivirus protection software, tested regularly to ensure good working condition.
17. **Safe Use of External Learning Applications:** Safeguarding mechanisms in place (e.g., single sign-on systems) to protect student and system security in the use of external learning applications.

Appendix E. Responsible Use and Safeguarding Elements

1. **Cognitive Development:** BRS committed to ensure school-based AI and technology use serves a clear educational purpose and that strategies are in place to protect and develop students' cognitive ability, agency, and autonomy, and does not enable cognitive offloading that undermines learning.
2. **Academic Integrity:** BRS verifies that the use of AI and technology supports academic integrity and does not undermine the validity, reliability, or fairness of assessments, in line with the [Assessment Policy](#) and the Federal Decree Law No. 33 of 2023 Concerning Combating Cheating and Violation of Examination Systems.
3. **Human Oversight:** BRS guarantees meaningful human oversight of any AI-supported decision affecting a student's educational path, rights, or wellbeing, with a designated staff member reviewing, exercising professional judgement on, and signing off on the final decision.
4. **Content Safety and Cultural Consideration:** The school safeguards students by verifying that AI and technology tools do not expose students to age-inappropriate content or to content that does not comply with the [Cultural Consideration Policy](#).
5. **Algorithmic Bias and Fairness:** BRS identifies, evaluates, monitors, and addresses bias in AI tools to ensure fair, inclusive, and culturally appropriate outcomes for

all students and staff, including teaching staff and students how to recognize bias.

Definitions

Agency	The capacity of individuals to make informed decisions, exercise autonomy and control, and retain meaningful involvement in actions and outcomes, including the ability to understand, question, and influence the use and impact of AI systems (UNESCO, 2023).
AI Literacy	The technical knowledge, durable skills, and future ready attitudes required to thrive in a world influenced by AI. It enables learners to engage, create with, manage, and design AI, while critically evaluating its benefits, risks, and ethical implications (OECD, 2025).
AI Learning Tool	An AI-powered personalized learning system that adapts content, difficulty level, and/or pacing according to students' needs (based on their performance, engagement, and/or progress).
Algorithmic Bias	Systematic and unfair outcomes produced by AI systems as a result of biased data, design choices, or deployment practices (UNESCO, 2021).
Artificial Intelligence (AI)	Computer-based systems designed to perform tasks that normally require human intelligence, such as recognising patterns, making decisions, learning from experience, and generating content (UNESCO, 2021).
Autonomy	The ability of individuals to retain control over decisions and actions, make informed choices, and exercise independent judgement when interacting with AI systems, ensuring that AI supports, rather than overrides, human decision-making, responsibility, and agency, particularly in educational contexts (UNESCO, 2021).
Bring Your Own Device (BYOD)	Practice wherein schools allow staff and/or students to do their work on personally owned digital devices.
Data Protection	The process of safeguarding data from corruption, compromise, unauthorized access, or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable (SNIA, n.d.).

Digital Incident	Any internal or external incident involving the inappropriate use of digital technology that negatively impacts the school's systems and/or community. This includes a breach of the reasonable usage policies, a cybersecurity incident, the accessing of inappropriate content, inappropriate behaviors or communications, cyberbullying, and/or any other breach of school regulations in a digital setting.
Responsible Use	The careful, considered, and risk-aware use of digital tools and systems by students, staff, and school leaders in educational settings, in ways that maximize educational benefits while ensuring safety, safeguarding, and appropriate evaluation of risks and benefits before adoption (UK Department for Education, 2025).

Compliance

Bright Riders School is committed to full compliance with this policy by AY 2027/28 (Fall term).

Approved By:

Rachna Prakash
Principal
Bright Riders School-Abu Dhabi
Next Review: AY 2027-2028

