BRIGHTON COLLEGE
AL AIN

AI and Technology Policy

Academic Year 2026/27

curiosity • confidence • kindness

Document control

Document	AI and Technology Policy
Academic year	2026/27
Applies to	Brighton College Al Ain - whole College, FS1 to Year 13
Policy owner	Deputy Head (Teaching, Learning, Sustainability and Digital Strategy), supported by the Digital Lead
Version	2.0
Approval	Headmistress and Governing Board
Review cycle	Annual, and sooner where UAE law, ADEK requirements or College arrangements change

> **Where there is any difference between this policy and a mandatory UAE or ADEK requirement, the UAE/ADEK requirement takes precedence and the College will update this policy accordingly.**

1. Policy statement

Brighton College Al Ain recognises that AI and technology capability is central to the success of its pupils, staff and wider community. The College is committed to using AI and technology safely, responsibly and effectively to improve teaching, learning and administration, while protecting pupils' wellbeing, data and cognitive development.

AI and technology at the College always serve a clear educational purpose. They support, and never replace, the professional judgement of teachers and the effort and thinking of pupils. Every pupil should leave the College AI literate: able to understand, use, create with and critically evaluate AI, and to use it ethically and in line with UAE values.

This policy sets out how the College meets the ADEK AI and Technology Policy, which schools must fully implement by Academic Year 2027/28. The College aims to meet all requirements during 2026/27.

2. Purpose and scope

This policy sets out the College's arrangements for AI and digital literacy, AI learning tools, institutional readiness, responsible use, security and digital communications. It applies to all pupils, staff, volunteers, parents, contractors and visitors who use College technology, College networks or College-approved AI tools, on or off site, and during any distance learning directed by the College.

This policy is read alongside the College's Safeguarding and Child Protection, Behaviour, Inclusion, Assessment, Data Protection, Responsible Use and BYOD, Digital Media and Social Media, Records, and Critical Incident and Disaster Recovery policies.

3. Regulatory framework

Source	College application
ADEK AI and Technology Policy (draft, July 2026)	Primary framework for AI literacy, AI learning tools, responsible use, security and communications. Full compliance required by AY 2027/28.
UAE School Inspection Framework: Standards 4.1.1, 4.1.4 and 5.1.2	Curriculum rationale and cross-curricular links; health, safety and security arrangements.
Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data	Lawful, fair, transparent and secure handling of personal data.
Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes	Expectations for online conduct and reporting of digital offences.

Source	College application
Federal Decree-Law No. 26 of 2025 on Child Digital Safety	Protection of children online, including parental responsibilities.
Cabinet Resolution No. (106) of 2026 on Children's Access to Social Media	Pupils are not authorised to use social media at the College; parents are informed of age limits.
Federal Decree-Law No. 33 of 2023 on Combating Cheating and Violation of Examination Systems	Academic integrity in the use of AI for coursework and assessment.
ADEK Inclusion, Student Protection, Student Behaviour, Records, Assessment and Cultural Consideration policies	Applied wherever AI and technology affect these areas.

4. Key definitions

Term	Meaning
AI literacy	The knowledge, skills and attitudes pupils need to understand, use, create with, manage and critically evaluate AI, including its benefits, risks and ethical implications.
AI learning tool	An AI-powered personalised learning system that adapts content, difficulty or pacing to each pupil's performance, engagement or progress.
Cognitive offloading	Relying on AI to do thinking that a pupil should do, such as copying AI answers or skipping reasoning, in a way that undermines learning.
Algorithmic bias	Unfair outcomes produced by AI systems because of biased data, design or use.
Digital incident	Any incident involving the inappropriate use of technology that harms the College's systems or community, including breaches of responsible use, cybersecurity incidents, access to inappropriate content, cyberbullying and inappropriate communication.
BYOD	Bring Your Own Device: the College allows pupils or staff to use personally owned devices for College work.
Responsible use	The careful, considered and risk-aware use of technology that maximises educational benefit while keeping users safe.

5. Roles and responsibilities

Role	Responsibilities
Headmistress	Overall accountability for this policy and for compliance with ADEK requirements.
Governing Board	Strategic oversight and annual approval of this policy and the Digital Strategy.
Deputy Head (Teaching, Learning, Sustainability and Digital Strategy)	Policy owner. Chairs the Digital Wellbeing Committee and leads the Digital Strategy and annual action plan.
Digital Lead	Day-to-day implementation, AI learning tool administration, staff and pupil training, and AI curriculum mapping.
Designated Safeguarding Lead (Child Protection Coordinator)	Receives and manages all safeguarding concerns arising from AI or technology use, including alerts from AI learning tools.
IT and Bloom Education	Infrastructure, cybersecurity, vendor approval and data protection controls.
Teachers and teaching assistants	Use AI learning tools in line with Section 7, monitor pupil data, protect academic integrity and report concerns.

Role	Responsibilities
Pupils	Use technology responsibly and in line with their Responsible Use Agreement.
Parents	Sign the Responsible Use Agreement, monitor their child's digital behaviour outside school and support the College's approach.

6. AI and digital literacy

6.1 Curriculum integration

The College implements the ADEK K-12 AI Literacy Framework. Pupils develop the four AI literacy strands through the curriculum: AI Conceptual Understanding; Critical Evaluation and Informed Interaction; AI Creation, Engineering and System Design; and Responsible Governance, Data Privacy and Societal Impact. Learning follows a spiral design, revisiting concepts with increasing technical complexity as pupils move through the College.

Phase (College year groups)	AI learner profile	Mode of integration	Core competency
Phase 1: FS2 to Year 1	AI Aware Explorer	[Embedded]	Explores inputs and responses through play. Learning is unplugged, with no direct use of AI tools.
Phase 2: Years 2 to 6	AI Literate Thinker	[Stand-alone / embedded / hybrid]	Applies rules, logic and data, and begins to use AI tools to refine outputs.
Phase 3: Years 7 to 9	AI Solution Builder	[Stand-alone / embedded / hybrid]	Designs and improves AI-powered solutions using data, models and workflows.
Phase 4: Years 10 to 13	AI Systems and Solutions Designer	[Stand-alone / embedded / hybrid]	Designs and governs integrated AI systems for real-world problems.

The College's AI curriculum is also guided by the ISTE, Common Sense Education and National Centre for Computing Education frameworks, and is mapped by year group in InstrucTwin.

6.2 Monitoring and reporting AI learning outcomes

The College uses InstrucTwin as its Learning Management System. InstrucTwin integrates AI standards and learning outcomes, so pupils' AI literacy data is recorded and accessible to ADEK for regulatory monitoring.

6.3 AI literacy assessment

Every pupil graduates with demonstrated AI literacy, assessed through the application of knowledge and skills in authentic, real-world contexts. Assessment is adapted for pupils with additional learning needs, in line with the Inclusion Policy.

7. AI learning tools

7.1 AI-powered personalised learning

The College uses InstrucTwin as its AI learning tool. ADEK approval was obtained through the ADEK AI Learning Tool Vetting Form on [date / reference]. No other AI learning tool is used with pupils unless it has first been approved by ADEK and by the College under Section 10.1.

InstrucTwin meets the ADEK mandatory criteria for: safety and self-harm detection; cultural content filtering; academic integrity; teaching pedagogy; curriculum and content integration; assessment and learning resources; teacher views of pupil-level and class-level activity; and administrator access, including system-level access for ADEK quality assurance.

Lessons follow the College schedule and are enhanced by InstrucTwin, allowing teachers to challenge pupils and support others through bridging units. To protect learning and wellbeing, the College sets screen-time limits for AI learning tools of [limits by phase]. In line with ADEK requirements, pupils in FS2 and Year 1 do not use AI tools directly.

7.2 Safety guardrails

Teachers apply the ADEK Guardrail Prompt for AI Learning Tools to every class, space, lesson and assignment they create in an AI learning tool, before pupils use it. The guardrails keep responses on the lesson topic, filter culturally inappropriate content, reflect UAE values and direct pupils to a trusted adult for any safeguarding concern.

7.3 How teachers use AI learning tools

Teachers and teaching assistants using AI learning tools must:

- assign age-appropriate tasks aligned to curriculum standards, adapted by ability so that pupils with additional learning needs receive suitable tasks
- check AI-generated lesson plans and resources for factual accuracy and curriculum alignment before use
- review class-level data daily and pupil-level data weekly to identify learning gaps, engagement and off-topic or inappropriate content
- respond to gaps through the tiered model: whole-class teaching where most pupils have a gap (Tier 1), and targeted small-group or individual support where only a few do (Tiers 2 and 3)
- use the tool again to check that the intervention has closed the gap
- monitor for over-reliance on AI, such as verbatim submissions or skipped reasoning, and reinforce expectations of genuine effort
- alert the Designated Safeguarding Lead immediately if a pupil shows distress, self-harm ideation, an abuse disclosure or seriously inappropriate messaging through AI interactions

AI data informs, and never replaces, a teacher's professional judgement about a pupil's progress.

7.4 Foundational "AI for Teaching" competency

All relevant teaching and teaching support staff complete foundational training in using AI learning tools to identify pupils' strengths and weaknesses and adapt teaching to close gaps, in line with Section 7.3. Training includes InstrucTwin, Microsoft Educator certification, AI literacy and safeguarding, so that all staff model responsible digital behaviour.

7.5 Pupil training

All pupils are trained to use the College's AI learning tool, including how to navigate it, use it to support their own learning, write effective prompts, keep within the safety guardrails and use it responsibly. The tool is taught explicitly in the first two lessons, and pupils' ongoing use is supported by the pupil Digital Ambassadors.

8. Institutional readiness

8.1 Digital strategy

The Brighton College Al Ain Digital Strategy (2025 to 2030) sets out six priorities: infrastructure procurement and development; software development for administration and the classroom; Microsoft development and enhancement; responsible use and digital safeguarding; data protection and cybersecurity; and staff training. In line with ADEK requirements, the strategy is delivered through an annual school-wide action plan that sets out how AI and technology will improve pupil achievement, teaching and College operations each year.

The Digital Wellbeing Committee, chaired by the Deputy Head (Teaching, Learning, Sustainability and Digital Strategy), meets termly to review progress, update risk assessments and align procurement with strategic goals.

8.2 Continuous professional development in AI

All staff attend ADEK-mandated training, both general and role-specific. The College provides CPD in: human-centred AI use; ethical and responsible AI practice; AI systems and applications; AI-enabled pedagogy; AI for professional growth; and cybersecurity and digital safety. The impact of CPD is evaluated through annual audits, feedback surveys and lesson observations.

8.3 Digital infrastructure and systems

The College maintains reliable digital infrastructure in line with Bloom Education standards and ADEK technical requirements. A rolling three-year procurement plan, informed by annual audits, ensures hardware and connectivity meet teaching and administrative needs, and all systems are tested for security and reliability. The College ensures:

- secure, College-managed devices, and BYOD arrangements with Mobile Device Management, minimum device specifications, antivirus requirements and VPN restrictions
- staff access to all digital systems and platforms provided by ADEK
- readiness for ADEK-approved distance learning
- assistive technologies for pupils who need them, in line with the Inclusion Policy

9. Responsible use

9.1 Responsible use policies

The College has age-appropriate and culturally appropriate Responsible Use Agreements for pupils, staff, parents and other users, covering BYOD, password management and social media. The College also makes sure that its use of AI and technology protects:

- **Cognitive development:** every use of AI has a clear educational purpose and builds pupils' thinking, agency and independence, rather than doing their thinking for them.
- **Academic integrity:** AI use does not undermine the validity, reliability or fairness of assessment, in line with the Assessment Policy and Federal Decree-Law No. 33 of 2023.
- **Human oversight:** any AI-supported decision affecting a pupil's educational path, rights or wellbeing is reviewed and signed off by a designated member of staff.
- **Content safety and cultural consideration:** AI and technology tools do not expose pupils to age-inappropriate content or content that does not comply with the Cultural Consideration Policy.
- **Fairness:** bias in AI tools is identified, monitored and addressed, and staff and pupils are taught how to recognise bias.

Safeguarding measures include termly digital safety lessons in Computing and PSHE, filtering and monitoring of all College networks, clear reporting routes for digital incidents, and work with parents to support safe use at home.

9.2 Pupil mobile phones

Pupils are not permitted to use personal mobile phones on College premises during the school day, unless a teacher explicitly and exceptionally authorises it for learning. All other SIM-enabled devices, such as smart watches, must have communication functions disabled. Devices needed for learning are used only for learning and are actively monitored to prevent distraction.

9.3 Pupil social media

The College does not authorise pupils to use social media, and social media is blocked on College networks, in line with Cabinet Resolution No. (106) of 2026.

9.4 Virtual private networks (VPNs)

VPNs are not permitted on any device on College premises or networks. This is stated in the Responsible Use Agreements signed by pupils and parents, and is explained to pupils in workshops. Any breach is managed under the Behaviour Policy.

9.5 Working with parents

The College regularly reminds parents of their responsibility to monitor their child's digital behaviour outside school and to limit social media use for children aged 15 and under, in line with Federal Decree-Law No. 26 of 2025 and Cabinet Resolution No. (106) of 2026. Parents sign the Responsible Use Agreement each year, are consulted on the College's approach through a parent survey, and are offered training on InstrucTwin and this policy.

10. Security

10.1 Selecting technology vendors

All technology vendors, products and services are approved by Bloom Education through the Kissflow purchase order system and must meet ADEK requirements and UAE law. Before approval, the College checks that the vendor:

- holds the required registration documents: VAT certificate and valid trade licence (GCC vendors) or company registration certificate (non-GCC vendors), and bank details
- meets the College's data protection and cybersecurity requirements, including where data is stored and who can access it
- signs confidentiality, non-disclosure and data protection terms before processing any personal data
- has ADEK approval, where the product is an AI learning tool

Third-party providers are reviewed annually for continued compliance.

10.2 Digital incidents

Digital incidents are identified, managed, documented, responded to and reported in line with the Safeguarding and Child Protection Policy, the Behaviour Policy, the Records Policy and UAE law. All digital incidents are recorded on CPOMS and managed by the Designated Safeguarding Lead, so that online and in-person concerns are handled in the same way. Affected pupils are supported, parents are informed where appropriate, and incidents are reported to the College Leadership Team for monthly review.

10.3 Data protection and cybersecurity

The College handles personal data lawfully, fairly, transparently and securely, in line with Federal Decree-Law No. 45 of 2021, Federal Decree-Law No. 34 of 2021 and Federal Decree-Law No. 26 of 2025. The College Data Protection Plan sets out the personal data that may be collected, consent procedures, data classification and access rights, and retention, backup, recovery, disposal and sharing arrangements, in line with the ADEK Records Policy.

Parents give written consent, as part of the Parent-School Agreement, for digital tools that process pupil data. AI learning tools require **separate, explicit parental consent**, which explains the purpose, use, storage and sharing of data and the right to opt out, with alternative learning arrangements. AI learning tools may not use pupil data for commercial purposes, profiling, unauthorised sharing or AI model training, and must delete or anonymise a pupil's data within 90 days of the pupil leaving the College, with written confirmation from the provider on request.

The College's cybersecurity measures include:

- multi-factor authentication, single sign-on and role-based access controls
- encryption of data in transit and at rest, and encryption of College-managed devices
- next-generation firewalls, intrusion detection and prevention, and web filtering
- up-to-date antivirus and malware protection, with regular security patching
- automated backups, stored offline and separately from the College network, and a disaster recovery plan
- data classification and data loss prevention controls
- regular cybersecurity awareness training for staff and pupils
- a Cybersecurity Incident Response and Business Continuity Plan, tested through an annual tabletop cyber-attack exercise with the College Leadership Team

- secure physical access to servers and network equipment
- continuous monitoring and detailed logging
- secure cloud services integrated with College identity systems

Systems are tested and audited termly.

10.4 Digital communication and social media

The College stores digital media securely and controls access to its official social media accounts, which are managed by the Communications and Marketing Coordinator and the College Social Media Team. Official and unofficial College-related channels are monitored. The College obtains parental consent before recording or publishing any identifiable images or recordings of pupils.

10.5 Staff personal communication

Staff must not use personal email or social media accounts to communicate with current pupils, former pupils under 18, or parents. Staff must not use personal social media to share confidential College information, or content that may be inappropriate, discriminatory, harmful or seen as endorsed by the College. These expectations are set out in the staff code of conduct and shared at induction.

11. Communications

11.1 College website

The College maintains an up-to-date website containing all ADEK-mandated information. The Communications and Marketing Coordinator checks it [termly] against ADEK requirements.

12. Monitoring and review

The Digital Wellbeing Committee monitors the implementation of this policy termly and reports to the College Leadership Team. The College measures the impact of this policy through the ADEK expected outcomes:

- improved AI and digital literacy among pupils
- stronger AI-enabled teaching
- improved pupil attainment and progress through the use of AI learning tools
- more responsible use of AI and technology across the College

This policy is reviewed annually by the Digital Wellbeing Committee and approved by the Headmistress and the Governing Board. Breaches of this policy may lead to action under the College's staff disciplinary procedures or the Behaviour Policy.

13. Related College documents

- Digital Strategy (2025 to 2030) and annual digital action plan
- Responsible Use and BYOD Agreements (pupils, staff and parents)
- Framework for the Selection of External Providers and Products
- Data and Cybersecurity Infrastructure Plan
- Cybersecurity Incident Response and Business Continuity Plan
- Data Protection Policy and Plan
- Digital Media and Social Media Policies
- Safeguarding and Child Protection Policy; Behaviour Policy; Inclusion Policy; Assessment Policy

Change history

Version	Summary	Owner	Date
1.0	Policy created	Richard Brashier	Oct 2026
2.0	Brighton College format; aligned with the ADEK AI and Technology Policy (draft, July 2026), including AI literacy phases, AI learning tool approval and guardrails, responsible use elements, vendor selection and data protection requirements	[Owner]	Nov 2026

Approval and sign-off

Policy owner	Deputy Head (Teaching, Learning, Sustainability and Digital Strategy)
Approved by	Headmistress Sarah Weaver
Approved by Governing Board	Craig Lamshed, General Manager, Bloom Education
Approval date	_____