



هيئة الشارقة للتعليم الخاص
SHARJAH PRIVATE EDUCATION AUTHORITY

Policy on the Safe and Balanced Use of Digital Learning





Table of Contents

1 Introduction	3
2 Terminology and Definitions	3
3 Purpose	5
4 Scope	5
5 Core Principles	6
6 Policy Provisions	7
7 Non-Compliance Procedures	11
8 Roles and Responsibilities	12
9 References	13





1 Introduction

Driven by the Sharjah Private Education Authority's commitment to educational excellence and its recognition of the importance of regulating and monitoring the quality of the educational process within private educational institutions in the Emirate of Sharjah, and in furtherance of its commitment to promoting the responsible use of digital technologies in a manner that serves educational objectives and safeguards the rights and safety of students, this Policy establishes a binding regulatory framework governing the use of digital learning, electronic devices, educational platforms, artificial intelligence, internet networks, media, and digital devices within private educational institutions.

The Policy is intended to ensure that digital technologies are employed as tools that support and enhance the educational process without supplanting direct pedagogical interaction or essential educational, social, and physical activities, and in a manner consistent with the legislation of the United Arab Emirates, its cultural and social values, and the requirements of child protection, digital security, and information security.

2 Terminology and Definitions

Term	Definition
Authority	The Sharjah Private Education Authority.
Private Educational Institutions	Nurseries, early childhood centres, kindergartens, and schools licensed by the Sharjah Private Education Authority.
Digital Learning	The use of digital devices, platforms, and resources to support teaching, learning, and assessment processes.
Digital Device	Any electronic device used to access digital content or educational platforms, including computers, tablets, and smartphones.
Artificial Intelligence	Digital systems and applications capable of generating, processing, or analysing content using machine learning techniques, generative models, or other similar technologies.





Term	Definition
Digital Content	All educational, media, or interactive material provided or used in electronic form.
Protection Officer	The person formally appointed to oversee child protection and digital safety matters within the educational institution.
Digital Balance and Wellbeing	Private educational institutions shall take into consideration students' age, educational stage, and the nature of the activity, and shall ensure the prevention of excessive screen use by providing appropriate breaks as well as non-digital, physical, and social activities.
Digital Educational Platform	Any digital system, application, website, or service used to manage learning, deliver content, administer assessments, or facilitate educational communication.
Digital Safety	The set of measures and controls that ensure the protection of learners and staff while using digital environments, devices, and platforms.
Sensitive Data	Any data whose misuse could cause particular harm to a student or the student's family, such as health data, behavioural data, detailed educational data, data relating to people of determination, location data, or images and recordings.
Cybersecurity	The technical and organizational measures aimed at protecting networks, systems, and data from unauthorized access, breach, disclosure, disruption, or misuse.
Digital Incident	Any occurrence relating to the misuse of technology, data, accounts, content, networks, or platforms, including cyberbullying, hacking, data leakage, or access to harmful content.





3 Purpose

This Policy is intended to:

- 3.1 Regulate the use of digital technologies and platforms within private educational institutions in a manner that fulfils approved educational objectives.
- 3.2 Protect students from digital risks, harmful content, and electronic violations.
- 3.3 Ensure that digital content and educational platforms are consistent with the values and legislation of the United Arab Emirates.
- 3.4 Strengthen cybersecurity and protect personal data and educational information.
- 3.5 Regulate the use of artificial intelligence tools within the educational environment in a responsible and ethical manner.
- 3.6 Define the roles, responsibilities, and obligations of all relevant parties.

4 Scope

This Policy shall apply to:

- 4.1 All private educational institutions licensed by the Sharjah Private Education Authority.
- 4.2 Students, teachers, and administrators when using devices, networks, platforms, or digital resources within private educational institutions, or as part of any educational activity organized or supervised by private educational institutions.
- 4.3 Parents in relation to the obligations stipulated in this Policy.
- 4.4 All digital devices, networks, platforms, and resources used in the educational process, whether owned by the institution or by individuals.





5 Core Principles

This Policy is founded upon the following principles:

- 5.1 Primacy of the Educational Interest: The use of digital technologies shall be limited to circumstances where they provide clear and demonstrable educational value.
- 5.2 Child Protection: Educational institutions shall be committed to providing a safe digital environment that safeguards the psychological, physical, and social wellbeing of students.
- 5.3 Age Appropriateness: All digital applications, platforms, and resources must be suitable for the intended age group.
- 5.4 Cybersecurity and Data Protection: Educational institutions shall be committed to protecting personal data and educational information from unauthorized access, use, or disclosure.
- 5.5 Cultural and Value-Based Compliance: Digital content must be consistent with the national, cultural, religious, and social values of the United Arab Emirates.
- 5.6 Accountability and Transparency: Educational institutions shall bear full responsibility for managing and monitoring the use of digital technologies within their educational environments.





6 Policy Provisions

6.1 Use of Digital Learning

6.1.1 Digital tools shall be employed within private educational institutions as instruments supporting the educational process where required, without supplanting direct instruction, social interaction, physical activity, or fundamental skills such as reading and handwriting, throughout the school day.

6.2 Maximum Limits on Digital Use

6.2.1 A gradual and balanced approach shall be adopted in private educational institutions when using electronic devices and incorporating digital learning tools throughout the school day. The duration of digital use shall be determined progressively according to students' age and educational stage, in alignment with the intended learning outcomes, developmental characteristics, and educational needs of each stage.

Educational Stage	Indicative Maximum of Daily Digital Learning within the Private Educational Institution
early childhood	10%
Grades 1–4	25%
Grades 5–8	50%
Grades 9–12	75%

* The percentages set out in the table above are indicative of the maximum proportion of daily instructional time that may be allocated to digital learning within private educational institutions.

* During the first year of the Policy's implementation, the specified percentages will be reviewed and their effects assessed across the relevant aspects.

6.2.2 The maximum time limits on the use of digital learning within private educational institutions shall be adopted such that the duration of use is lower at the early childhood stage and increases progressively upon advancement to higher educational stages, unless the Sharjah Private Education Authority issues a circular, guide, or regulatory decision providing otherwise.





6.3 Healthy Break Periods

6.3.1 The private educational institution shall provide healthy break periods during continuous screen use, so as to reduce visual and physical strain, diminished concentration, and sedentary behaviour, and such periods shall be incorporated into lesson planning or educational schedules whenever digital devices are used. The following intervals shall be adopted as an indicative guideline, having regard to the individual needs of students.

Educational Stage	Minimum Break Periods during Continuous Digital Use
From early childhood to Grade 4	Every 10–15 minutes
Grades 5–8	Every 20 minutes
Grades 9–12	Every 30–40 minutes

* The time intervals set out in the table below are indicative of the minimum break periods during continuous digital use within private educational institutions.

* During the first year of the Policy's implementation, the specified time intervals will be reviewed and their impact assessed across the relevant aspects.

6.4 Permitted Uses

Digital learning may be used within private educational institutions where it is directly related to approved educational or operational objectives. This includes:

- 6.4.1 E-learning and blended learning.
- 6.4.2 Digital books and approved educational resources.
- 6.4.3 Guided academic research.
- 6.4.4 Programming, robotics, design, and innovation.
- 6.4.5 Approved educational assessments.
- 6.4.6 Support services designated for people of determination.





6.5 Prohibited Uses

Devices, networks, or digital platforms shall not be used for any of the following:

- 6.5.1 Accessing unauthorized social media websites or applications.
- 6.5.2 non-educational electronic games.
- 6.5.3 Entertainment content unrelated to educational objectives.
- 6.5.4 Cyberbullying or digital abuse.
- 6.5.5 Recording or photographing individuals without proper authorization.
- 6.5.6 Circumventing protection systems or using virtual private networks (VPNs) or other technical circumvention methods.
- 6.5.7 Academic cheating, plagiarism, or digital identity impersonation.

6.6 Digital Content Standards

The private educational institution shall ensure that digital content is:

- 6.6.1 Appropriate to the targeted age group.
- 6.6.2 Directly related to educational objectives.
- 6.6.3 Free of violence, extremism, hatred, pornographic material, gambling, drugs, or misinformation, in accordance with the Sharjah Private Education Authority's content-safety policies.
- 6.6.4 Consistent with the national and cultural values of the United Arab Emirates.
- 6.6.5 Free of advertisements or non-educational commercial purposes.

6.7 Child Protection and Digital Safety

Private educational institutions shall ensure the following:

- 6.7.1 The provision of effective systems for reporting digital incidents.
- 6.7.2 The immediate reporting of any threats or violations affecting student safety.
- 6.7.3 The documentation and follow-up of all reports and corrective measures.
- 6.7.4 The notification of parents of any serious incident relating to digital safety.





6.8 Technical Infrastructure and Cybersecurity

Educational institutions shall implement security controls to protect networks, devices, platforms, accounts, and data, including:

- 6.8.1 Digital device management systems.
- 6.8.2 Electronic content filtering systems.
- 6.8.3 Protection software and periodic security updates.
- 6.8.4 Management of user access privileges.
- 6.8.5 Protection of educational and personal data.

6.9 Protection of Student Data in the Use of Artificial Intelligence Tools

Institutions shall refrain from entering students' personal, educational, health, or behavioural data into any public or unapproved artificial intelligence platform or tool, unless the private educational institution has verified the legal basis, privacy safeguards, and educational purpose, and has obtained parental consent where required.

6.10 Use of Personal Devices

The use of students' personal devices within private educational institutions shall not be permitted except in accordance with written and approved controls established by the private educational institution and aligned with any directives issued by the Sharjah Private Education Authority.

Such controls shall take into account students' age, educational stage, and the nature of the educational need, and shall include parental consent, device registration where required, acceptable use rules, protection requirements, and educational and administrative measures applicable in cases of non-compliance.

6.11 Artificial Intelligence Governance

6.11.1 Students' use of digital platforms, applications, and tools shall be confined to those approved internally by the private educational institution, in accordance with criteria including educational value, age appropriateness, data protection, cybersecurity, accessibility, and the absence of harmful material or non-educational advertisements, and such use shall be subject to appropriate human oversight and review.





6.11.2 Private educational institutions shall set out the circumstances in which students may use artificial intelligence tools for assignments, projects, or educational research, and the circumstances in which such use is prohibited or subject to a requirement of disclosure.

The following shall be observed in the use of artificial intelligence tools:

6.11.3 Compliance with intellectual property rights and the principles of academic integrity.

6.11.4 Disclosure of the use of artificial intelligence tools in academic work whenever required.

6.11.5 Human verification of the outputs of artificial intelligence systems prior to their adoption or use.

6.11.6 A prohibition on entering personal data or sensitive information into public or unapproved systems.

6.11.7 The prevention of the use of artificial intelligence tools for the purposes of cheating, academic dishonesty, or identity impersonation.

6.12 Reporting, Documentation, and Incident Management

Private educational institutions shall document digital incidents and the actions taken in response thereto in a secure register, while ensuring data confidentiality and the protection of the identities of all parties involved, particularly students. Sensitive digital incidents shall not be addressed without proper documentation or outside official channels.

6.13 Review and Improvement

Private educational institutions shall maintain compliance records comprising a register of approved platforms, a register of digital incidents, acceptable-use agreements, and cybersecurity controls review register, and shall provide such records to the Sharjah Private Education Authority upon request.

7 Non-Compliance Procedures

7.1 The first year following the issuance of this Policy shall serve as an implementation phase intended to enhance students' health and foundational skills, and to utilize the outcomes of implementation in the development of the next version of the Policy.





8 Roles and Responsibilities

8.1 Sharjah Private Education Authority

- 8.1.1 Monitoring educational institutions' compliance with the provisions of this Policy.
- 8.1.2 Conducting periodic audits and inspections to verify compliance.
- 8.1.3 Issuing and updating supplementary regulatory guides as required.
- 8.1.4 Taking administrative measures and imposing sanctions where a violation is established.

8.2 Private Educational Institutions

- 8.2.1 Implementing the provisions of this Policy and monitoring compliance therewith.
- 8.2.2 Approving the digital platforms and applications used.
- 8.2.3 Providing a safe and protected digital environment.
- 8.2.4 Documenting and reporting digital incidents.
- 8.2.5 Training staff and students in digital safety.

8.3 Teachers

- 8.3.1 Direct supervision of digital use within classrooms.
- 8.3.2 Ensuring the purposeful, educational use of digital technologies.
- 8.3.3 Monitoring students' compliance with the provisions of this Policy.

8.4 Students

- 8.4.1 Complying with acceptable-use controls.
- 8.4.2 Refraining from the misuse of digital devices or platforms.
- 8.4.3 Reporting any unsafe digital content or conduct.

8.5 Parents

- 8.5.1 Supporting adherence to responsible digital conduct beyond the educational institution.
- 8.5.2 Cooperating with the educational institution in addressing digital risks.
- 8.5.3 Monitoring their children's use of digital technologies.





8.6 Service Providers and Contractors

8.6.1 Service providers and contractors shall comply with data protection, security, and confidentiality controls, and shall not process or share the data of the private educational institution or its students except in accordance with the contract and the specified purpose. They shall also notify the private educational institution of any security incident or change affecting the service.

9 References

First: Federal Legislation

1. Federal Law No. (3) of 2016 on Child Rights Law ("Wadeema").
2. Federal Decree-Law No. (30) of 2025 on the Governance of the National Educational Curriculum.
3. Federal Decree-Law No. (18) of 2020 Regarding Private Education.
4. Federal Decree-Law No. (34) of 2021 Regarding the Combating of Rumours and Cybercrimes.
5. Federal Decree-Law No. (34) of 2023 Regarding the Combating of Discrimination, Hatred, and Extremism.
6. Federal Decree-Law No. (45) of 2021 Regarding the Protection of Personal Data.

Second: Local Legislation — Emirate of Sharjah

7. Administrative Resolution No. (19) of 2019 Regarding the Regulation of Private Education in the Emirate of Sharjah.

Third: Official Guides and Documents

8. Safe and Responsible Use Guide of Generative AI in Classrooms, Ministry of Education 2026, United Arab Emirates.

