Policy:	**Digital Policy**
Date Published:	August 2025
Evaluation & Review:	Academic Year 2025-2026
Rationale:	This policy sets out the basic requirements for schools in their development and implementation of a digital strategy, their provision of teaching and learning on digital safety, and their secure use of digital technology.
Roles of Responsibility:	School Administration, SLT, Parents, Student Counsellor, Student Welfare Officer, Safeguarding committee. IT Coordinator, OSH Officer.

EGS shall:

- Develop and implement a digital strategy regarding their use of technology, goals related to digital competencies and infrastructure, digital security measures, and required resources, as per ADEK requirement.

- Ensure to invest in the development of students' digital skills and competencies to empower them to maximize learning opportunities presented by the use of technology.

- Ensure to educate students on the responsible and safe access and usage of the online environment and protect students from digital content and interactions that are inappropriate or harmful.

- Ensure to put in place systems, mechanisms, and procedures that are safe, balanced, and appropriate to safeguard their digital security.

- Ensure to comply with the requirements of the Monitoring and Control Center and the *Federal Decree Law No. (45) of 2021* on the Protection of Personal Data in the collection, processing, and storage of personal data.

www.egschooluae.com info@egschooluae.com +971 50 485 5511 Al Dhannah City, Abu Dhabi

1. Policy

1.1. Required Documentations

A. EGS shall develop and implement the following documents, and make them available on their school website in both Arabic and English or their language of instruction, in line with the requirements of this Policy:

a. Digital strategy (see Section 2.1 Digital Strategy).
b. Responsible usage policies (see Section 4.1 Responsible Usage Policies).
c. Framework for the selection of external providers and products (see Section 5.4 External Providers and Products).
d. Data and Cyber security (see Section 6.1 Secure Digital IT Architecture).
e. Response plan in relation to cyber security incidents (see Section 6.6 Cyber security Incidents).
f. School data protection plan and policy (see Section 7. Data Protection).
g. Digital media policy and social media policy (see Section 8. Digital Communications).

1.2. Digital Strategy and Oversight

A. **Digital Strategy:** EGS has implanted a digital strategy that outlines and provides rationale for their digital goals over a 5-year time frame. The strategy includes:

a. Overall strategic direction on how technology shall be deployed to deliver better student achievement and outcomes (e.g., to enhance teaching and learning and to support the efficient and effective running of the school administration).

b. Assessment of how the school can use and provide assistive technology to enable inclusion.

www.egschooluae.com info@egschooluae.com +971 50 485 5511 Al Dhannah City, Abu Dhabi

c. Goals related to student digital skills and competencies that enable learning.

d. Development, procurement, and implementation plans for digital infrastructure, software, and hardware.

e. Mechanisms for ensuring the security of the school's digital systems.

f. Plan for future-proofing the school's digital infrastructure, where applicable.

g. Resources and investment required to deliver the digital strategy.

h. Staff training requirements.

i. Increase awareness related to emerging technologies (e.g., Artificial Intelligence).

B. **Oversight:** A Digital Wellbeing Committee or Lead of EGS shall have the following responsibilities in relation to oversight of the school's digital strategy and associated policies:

a. Develop and implement the school's digital strategy.

b. Conduct an annual review of the digital strategy and its implementation:
   - Monitor progress against student learning goals and school development and procurement plans.
   - Evaluate technology, software, and online platforms to ensure that they meet the objectives of the strategy.
   - Test and conduct risk assessments of the school's digital systems and infrastructure (e.g., backup recovery) to ensure that they are secure and fit for purpose.
   - Review the effectiveness of the school's data and cyber security provisions.

www.egschooluae.com info@egschooluae.com +971 50 485 5511 Al Dhannah City, Abu Dhabi

- Re-evaluate the technological needs of the school based on feedback from staff, parents, and students, and plan procurement and digital development accordingly.
- Re-evaluate staff digital development needs and identify additional training required.

c. Develop and implement and review other school policies required to be created in line with this policy.

d. Engage with relevant stakeholders (e.g., the Digital Officer, Head of IT) to inform its decisions.

C. EGS shall appoint a staff member to liaise with ADEK for matters related to digital competency, safety, and security.

1.3. Digital Competencies

A. **Student Outcomes:** EGS shall define digital competencies and expected outcomes for students by grade/year and integrate these into the school's curriculum. Schools shall ensure that they have the appropriate digital infrastructure and resources in place to support students in achieving these outcomes, including students with additional learning needs, in line with the ADEK Inclusion Policy.

B. **Staff Training:** EGS shall provide relevant training to staff in line with their designation to enable them to promote the objectives of this policy. The training shall cover topics such as the school's digital infrastructure and policies, student digital learning outcomes, data protection, cyber security, and the digital safety measures implemented by the school.

1.4. Responsible Usage and Digital Safeguarding

A. **Responsible Usage Policies:** EGS shall develop and communicate responsible digital usage policies for students, parents, staff, and visitors. These policies shall set out what these groups are permitted/ prohibited to do on the school's premises, network, and systems, and shall include:

a. The definition of responsible usage of school software, network, services, and digital devices issued by the school, including shared devices.

b. Rules on the permitted and restricted use of personal devices on the school network and school premises, and during extracurricular activities that take place outside school (e.g., field trips).
    - EGS shall restrict the use of Virtual Private Networks (VPNs) by students on school premises or through school networks unless explicitly authorized for specific educational or administrative purposes.

c. Standards in relation to the use of personal social media accounts by staff (see Section 8.3. Personal Social Media Accounts for Staff).

d. The school's rules in relation to the setting and sharing of passwords for school accounts.

e. Standards in relation to the sharing of data related to the school or school community, and the channels via which such data can be shared when permitted. This includes standards related to the uploading of student data on external applications and learning tools, where applicable.

f. Standards in relation to academic honesty, plagiarism, and the responsible use of copyrighted material and digital tools (e.g., artificial intelligence), in line with the Federal Decree-Law No. (38) of 2021 on Copyrights and Neighboring Rights and the ADEK terms and conditions, copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.

g. EGS shall communicate the relevant responsible usage policies to students, parents, staff, and visitors via appropriate channels.
    - EGS shall publish responsible usage policies applicable to students and parents on the school website and in the Parent Handbook, as per the *ADEK Parent Engagement Policy.*

- For all younger students up to Grade 6 /Year 7, EGS shall provide age- appropriate versions of the policy to students, and a full version of the policy to parents.

B. **Safeguarding Students:** EGS shall put in place education programmes and effective systems to protect students from the online risks stated below.

a. Online risks posed to students are as follows:
   - Exposure to content that is inappropriate, illegal, or may harm their wellbeing.
   - Exposure to unsafe online interaction (e.g., interaction with users with fake profiles).
   - Personal online behavior that can lead to harm for self or others (e.g., engaging in cyber bullying).
   - Scams and finance-related risks such as gambling and phishing.

b. EGS shall put in place the following programmes, systems, mechanisms, and procedures to safeguard students against online risks and promote their wellbeing:
   - An age-appropriate awareness programme for all students, covering the benefits of technology, awareness of online risks, self-assessment of online risks when using technology, online safety measures, and the impact of digital habits on wellbeing (e.g., the impact of duration of usage of digital devices).
   - Appropriate filtering and monitoring systems to monitor student internet use on school devices and systems (physical firewalls).
   - Regular analysis of students' internet usage and web filter violations to identify potential adverse trends or problems.
   - Procedures to identify and support students who appear to be developing risky, excessive, or illegal digital habits, such as digital addiction or gambling, in line with the *ADEK Student Mental Health Policy* and the *ADEK Student Behavior Policy.*
   - Mechanisms to enable safeguarding during activities conducted virtually (e.g., disabling private chat for students).

www.egschooluae.com info@egschooluae.com +971 50 485 5511 Al Dhannah City, Abu Dhabi

c. EGS shall ensure there is a developmental purpose before allowing students to use the Internet during school hours.

C. Digital Incidents:

a. A digital incident occurs when a member of the school community engages in inappropriate use of digital technology. This includes a breach of reasonable usage policies, the accessing of inappropriate content, inappropriate behaviors or communications, cyberbullying, or any other breach of school regulations in an online setting.

b. Where a digital incident occurs during school hours or in settings covered in schools' digital policies, EGS shall make interventions and provide support to students and/or staff in line with the relevant policy (e.g., *ADEK Employment Policy, ADEK Staff Wellbeing Policy, ADEK Student Administrative Affairs Policy, ADEK Parent Engagement Policy, ADEK Student Behavior Policy,* and the *ADEK Student Protection Policy*). Where required, EGS shall report digital incidents to ADEK and cooperate with the Abu Dhabi Police for investigations.

c. EGS shall ensure that every digital incident is recorded, documented, and signed by the Principal and stored for auditing purposes, in line with the *ADEK Records Policy.*

D. EGS shall require parents to monitor students' usage of digital devices outside of school premises and school hours to ensure safe and appropriate digital behavior.

1.5. Digital Infrastructure

A. **Digital Devices:** EGS shall ensure that digital devices issued to members of the school community have appropriate security features. Where a school allows staff to access school-related data or systems on other devices or has a Bring Your Own Device (BYOD) policy for staff or students, the school

shall define and implement digital safety precautions (e.g., minimum device specification, and antivirus requirements).

B. **Digital Systems for Staff:** EGS shall ensure that relevant staff members have access to digital systems provided by ADEK, including the Learning Management System.

C. **Distance Learning Readiness:** EGS shall adopt measures for distance learning for emergency situations such as temporary school closures or for individual students in exceptional circumstances (e.g., prolonged hospital stay, or emergency travel with parents for extensive periods).

D. **Assistive Technology:** EGS shall provide assistive technology to students with additional learning needs-as indicated in their Documented Learning Plan, in line with the *ADEK Inclusion Policy.*

E. **External Providers and Products:**

a. EGS shall develop a third-party risk assessment framework for selecting external IT service providers and products related to the school network, system, and infrastructure, including learning application providers and open-source applications. This framework shall include the following, at a minimum:

- Compatibility with existing school systems.
- Secure management of data.
- Compliance with cyber security standards and frameworks.
- Security against cyber threats.
- Service delivery and backup/ recovery provisions.
- Reputation and financial stability of the provider.
- Adherence of the vendor to the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and the ADEK terms and conditions, copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.

- Where relevant (e.g., learning application providers), educational quality, and age-appropriateness of content.

b. EGS shall communicate to external vendors that the vendor is subject to the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and the ADEK terms and conditions, copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.

1.6. Data and Cyber Security

A. **Secure Digital IT Architecture:** EGS shall establish a robust secure digital infrastructure and ensure the relevant cybersecurity controls are implemented as follows:

a. Access Control

- Implement multi-factor authentication mechanisms across critical services.
- Define and enforce role-based access control to ensure users have appropriate permissions.

b. Data Encryption

- Employ encryption for data in transit and at rest to safeguard sensitive information.

d. Network Security

- Deploy next-generation firewalls and intrusion detection/prevention systems to protect against unauthorized access.
- Ensure web filtering policies are enforced.
- Ensure the ability to block inappropriate content.
- Ability to detect infected machines across the school network.
- Ensure identity-based firewalls are implemented to provide granular visibility on user browsing activity.
- Established a unified security edge architecture for all internet browsing.

- Regularly monitor and audit network traffic for unusual patterns.

c. Endpoint Protection

- Install and update anti-virus/ anti-malware software on all school- managed devices.
- Implement hard disk device encryption and ensure regular security patching.

d. Data Backup and Recovery

- Establish automated regular backup procedures for critical data.
- Ensure backups are vaulted and stored offline.
- Develop a robust disaster recovery plan to minimize downtime in case of a security incident.

e. Data Security

- Establish data classification controls across school and student data.
- Implement Data Loss Prevention Tools to ensure data leaks or ex-filtration is prevented.

f. Security Awareness Training

- Conduct regular training sessions for staff and students to raise awareness about cyber security threats and best practices.

g. Incident Response Plan

- Develop and regularly update an incident response plan to address security breaches promptly and effectively.
- Perform a tabletop cyber-attack simulation and exercise with school management involvement.

h. Physical Security

- Ensure secure access to physical servers, networking equipment, and other critical infrastructure.

i. **Regulatory Compliance**
   - Ensure compliance with local and international data protection regulations and standards.

j. **Monitoring and Logging**
   - Implement comprehensive monitoring systems to detect and respond to security incidents in real time.
   - Maintain detailed logs for auditing and analysis purposes.

k. **Secure Software Development**
   - Follow secure coding practices when developing or procuring educational software.
   - Regularly update and patch software to address vulnerabilities.

l. **Cloud Security**
   - If using cloud services, ensure the selected providers adhere to stringent security standards.
   - Implement proper configuration and access controls for cloud resources.
   - Integrate Cloud Services – Software as a Service (SaaS) with school identity services where possible.
   - Establish Cloud SaaS Security Posture Management capabilities.

m. **Collaboration Security**
   - Secure communication and collaboration platforms to protect sensitive educational information shared among students and staff.

n. **Third-Party Security**
   - Vet and monitor third-party vendors providing educational technology solutions to ensure they meet security standards.

B. **System Maintenance:** EGS shall maintain and regularly update digital infrastructure, operating systems, security systems, and software, including antivirus protection software. Schools shall regularly test their digital infrastructure and systems to ensure they are in good working condition.

C. **Safe Use of External Learning Applications:** EGS shall have safeguarding mechanisms in place (e.g., single sign-on systems) to protect student and system security in the use of external learning applications.

D. **Safe Virtual Interaction with Invited Visitors:** EGS shall seek parents' consent for any live virtual interactions with invited visitors, inside or outside of class. All such interactions shall also be approved by ADEK, in line with the ADEK Extracurricular Activities and Events Policy and the ADEK Student Protection Policy.

E. **Backup and Storage:** EGS shall ensure that backups of important information, software, and configuration settings are performed at an appropriate frequency and retained for an appropriate period of time to allow for business continuity.

    a. EGS shall ensure that such backups are stored securely and separately from the school network.

    b. EGS shall ensure that their data is synced to the cloud.

F. **Cyber security Incidents:** EGS shall develop response and business continuity plans to guide staff in the event of a cyber security incident, including the protocols for reporting the incident to the school leadership team and to ADEK, and the process for maintaining operational continuity.

    a. EGS shall not communicate any cyber security incident to external parties except for the service provider involved and ADEK.

    b. EGS shall adhere to all applicable laws and policies set out by the Abu Dhabi Digital Authority and any other relevant authorities in the UAE, including the Federal Decree Law No. (34) of 2021 on Combating Rumors and Cybercrimes.

www.egschooluae.com info@egschooluae.com +971 50 485 5511 Al Dhannah City, Abu Dhabi

1.7. Data Protection

A. **Data Protection Policy:** EGS shall develop a Data Protection Policy, setting out how the school shall ensure that personal information is dealt with correctly and securely, and in compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data, which shall include, at a minimum:

   a. The specification of the types of personal information that may be collected.

   b. The requirement and procedures for individual consent in the collection, processing, and storage of personal information.

      - Consent must be freely given, specific, informed, and unambiguous.
      - Consent may be withdrawn by the individual at any time.

   c. The conditions under which personal information may be shared by the school with other individuals or entities (e.g., with ADEK).
      - EGS shall have a non-disclosure agreement built into any agreements with contractors in which personal data cannot be shared within or outside the country for any purposes, without the explicit consent of ADEK.

B. **Sharing Data with ADEK:** EGS shall provide accurate and up-to-date data to authorized ADEK personnel on request, in line with the Federal Decree Law No. (18) of 2020 on Private Education and Law No. (9) of 2018 Concerning the Establishment of the Department of Education and Knowledge and in line with the ADEK terms and conditions, and data privacy policy with regard to the collection, use, and disclosure of information.

   a. EGS shall inform parents of their obligations to share data with ADEK accordingly.

C. **Data Protection Plan:** EGS shall develop and annually review a data protection plan, in compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data and the ADEK Records Policy. The data protection plan shall set out the steps taken by the school to safeguard its organizational data, including data classification methods, authorization levels, protections against cyber security and other threats, and procedures for restoring backed-up information in case of breaches.

1.8. Digital Communications

A. **Digital Media Policy:** EGS shall develop, implement, and monitor a Digital Media Policy governing the creation and publication of digital media. The policy shall include, at a minimum:

a. The requirement to obtain consent before recording and publishing digital media:

- EGS shall only take photographs and/or video recordings of students after obtaining written consent from parents. In obtaining consent, schools shall inform parents about the purposes for which the photographs and/or video recordings are being taken.
- EGS shall obtain written consent from parents before publishing digital content involving students. EGS shall clearly specify if the student will be identified by name in the publication when obtaining consent.

b. The procedures for the provision and withdrawal of consent.

c. Conditions related to the storage and security of digital media.

d. Conditions related to the use of personal devices and accounts for recording or publishing school content.

B. **Social Media Policy:** EGS has developed and implemented a Social Media Policy in relation to the use of social media by the school.

a. The policy includes:

- Social media platforms and accounts to be used by the school.
- Access, security, and password protection procedures for the school's social media accounts.
- Conditions related to content, language use, and engagement with other accounts.
- Conditions related to the use of names, photos, and videos of students, in accordance with *Section 8.1. Digital Media Policy.*
- Guidelines for moderators (see *Section 8.2.2. Moderators*) in relation to content posted by third parties on the school's social media pages, including procedures to manage disrespectful content and trolling.
- Procedures for addressing other adverse social media behaviors, such as impersonation of the school's accounts.

b. **Monitoring School Communications:** GES shall regularly monitor all official and unofficial school-related communication channels (newsletters, social media, parent communication groups, etc.) to ensure their compliance with this policy.

c. **Moderators:** GES shall appoint moderator(s) to pre-approve or remove content posted by other users on the schools' social media pages, where possible, in line with the school's guidelines. Moderator(s) shall reject or remove, where possible, content that is inappropriate, not in line with the UAE cultural values, or amounts to bullying, harassment, discrimination, or intimidation, in line with the *ADEK Values and Ethics Policy* and the *ADEK Cultural Consideration Policy.*

C. **Personal Social Media Accounts for Staff:** GES shall authorize members of staff to create and maintain existing personal social media accounts. In relation to these, staff members shall:

a. Not use email addresses issued by the school to create such accounts.

b. Use the tightest possible privacy settings.

c. Not identify themselves as being associated with the school, except on professional social media platforms (e.g., LinkedIn).

d. Not accept invitations to friend, connect with, or follow from current students or former students under the age of 18, or send such requests to current students or former students under the age of 18.

e. Not accept invitations from parents of current students to friend, connect with, or follow them.

f. Not use such accounts to communicate with current students, their parents, or former students under the age of 18. This applies to messaging applications (e.g., WhatsApp, Telegram, Signal).

g. Assume that content posted through such accounts (including online reviews and comments) is publicly visible and searchable, regardless of the privacy settings, and exercise appropriate discretion.

h. Ensure that content shared through such accounts is appropriate, in line with the *ADEK Cultural Consideration Policy*, and does not amount to bullying, harassment, discrimination, or intimidation, in line with the *ADEK Values and Ethics Policy.*

i. Ensure that content shared through such accounts does not give the impression of being endorsed by the school.

j. Ensure that they do not share any confidential information related to the school through such accounts.

D. **Communications via Email:** GES shall inform staff members that they are not authorized to use personal email addresses to communicate with students or parents.

E. **School Website:** GES has a dedicated website and it is kept up to date to serve as a reference for members of the school community.

a. GES shall publish the following content on their website, at a minimum:
   - Contact information.
   - Services provided by the school.
   - Fees, including transportation fees and fees for optional activities.
   - Inspection reports.
   - Aggregate student achievement data or individual achievements (e.g., awards), with consent.
   - Public versions of the annual report, in line with the *ADEK Reporting Policy.*
   - School policies that are relevant to parents and/or students.
   - Any other required content, as defined by ADEK policies.

b. GES shall ensure that the content published on their website is accurate and appropriate, in line with the *ADEK Values and Ethics Policy.*

c. GES shall ensure that content published on their website is in line with the requirements for digital media (see *Section 9.1. Digital Media Policy*).

******

www.egschooluae.com info@egschooluae.com +971 50 485 5511 Al Dhannah City, Abu Dhabi