DIGITAL POLICY

Introduction

Grace Valley Indian School (GVIS) has established this formal Digital Policy to codify the standards, guidelines, and procedures for the safe, responsible, and effective use of digital technology and information systems. This policy represents an ongoing process of aligning our operational practices with the core requirements of the Abu Dhabi Department of Education and Knowledge (ADEK) Digital Policy and relevant UAE Federal Laws. This policy outlines the standards, responsibilities, and mechanisms that govern digital use within the school environment.

1. Purpose

This Digital Policy aims to:

1. Ensure Compliance: Meet ADEK's requirements for digital strategy, responsible digital usage, cybersecurity, and data protection.
2. Enhance Teaching & Learning: Integrate digital competencies into the curriculum and provide safe, developmentally meaningful access to technology.
3. Protect Students: Safeguard students from online risks, inappropriate content, cyberbullying, and harmful digital interactions.
4. Strengthen Digital Security: Establish secure IT systems, data protection practices, and cybersecurity measures.
5. Guide School Community Behavior: Clearly define appropriate digital conduct for students,staff, parents, and visitors.

2. Objectives

The school is actively working to achieve the following core objectives:

1. Strategic Implementation: We are executing our comprehensive, 5-year Digital Strategy that covers digital competencies, infrastructure, security, and resource allocation.
2. Digital Competency: We are embedding the development of students' digital skills and competencies across the curriculum to maximize learning opportunities presented by technology.
3. Safety and Wellbeing: We are providing ongoing education on responsible usage and maintaining effective systems to protect students from inappropriate content, harmful interactions, and cyber risks (digital safeguarding).

4. Data Protection: We are continuously implementing secure procedures for the collection, processing, and storage of all personal data, ensuring demonstrable compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data.

5. Cybersecurity: We are maintaining and continuously hardening our Secure Digital IT Architecture and cybersecurity controls to protect the school's network, devices, and data from internal and external threats.

3. Scope

The policies and procedures described herein are currently operational and apply to all active members of the GVIS community, including:

- All Students (across all grades/years).
- All Staff (teaching, administrative, and support staff).
- Parents/Guardians who utilize school communication platforms or digital resources.
- External Stakeholders (e.g., visitors, contractors, third-party service providers) while accessing or using school-owned digital systems or the school premises network.

This policy covers all devices (school-owned and personal/BYOD), networks, systems, software, digital learning platforms, and official/personal social media accounts used for school-related communication or while on school premises.

4. Definitions

Digital Device	Any device used for communication, learning, or content access (phones, tablets, laptops, smartwatches).
Cyberbullying	Online behavior intended to harm, threaten, or harass.
Digital Incident	Any inappropriate use of technology, access to harmful content, cyberbullying, or violation of school digital rules.
Data Protection	Safeguarding personal information from unauthorized access or misuse.
Responsible Usage	Safe, ethical, and appropriate use of school or personal devices.
Assistive Technology	Tools or software support students with additional learning needs.

5. Policy Statement

Grace Valley Indian School is committed to maintaining a safe, secure, and respectful digital environment that effectively promotes student learning and development while strictly adhering to the legislative and cultural requirements of the UAE. To this end, GVIS has already:

- Implemented a mandatory and auditable suite of Responsible Usage Policies (RUPs) that are actively communicated to all stakeholders.
- Deployed and manages filtering and monitoring systems to safeguard students from inappropriate content online.
- Upholds the strictest standards for Data Protection and Cybersecurity to protect student, staff, and organizational data.
- Enforces the prohibition of using Virtual Private Networks (VPNs) by students on school premises or through school networks, unless explicitly authorized for educational or administrative purposes.

6. Procedures / Implementation Steps (Current Operations)

GVIS is implementing this policy through the following operational areas:

6.1. Digital Strategy and Oversight

- The Digital Wellbeing Committee is currently executing the 5-year Digital Strategy and conducts regular progress checks against defined milestones for infrastructure and student competencies.
- We are continually evaluating and deploying assistive technology solutions to support the inclusion of all learners.

6.2. Responsible Usage and Digital Safeguarding

* Specific, age-appropriate RUPs for students, staff, parents, and visitors are actively enforced.

* We are running mandatory, regular, and age-appropriate digital safety awareness programs for all students, covering online risks, cyberbullying, and digital wellbeing.

* We actively monitor internet usage and filter violations to identify potential adverse trends.

* We have established and are using clear procedures for recording, documenting, and managing all Digital Incidents, ensuring every record is signed by the principal and archived for auditing purposes.

6.3. Data Protection and Cybersecurity

* GVIS maintains a Secure Digital IT Architecture, which includes Multi-Factor Authentication (MFA) on critical services, data encryption for information in transit and at rest, and next-generation firewall protection.

* We have implemented a formal Third-Party Risk Assessment Framework to vet all external IT providers, ensuring their compliance with UAE data and security standards before integration.

* We have developed and regularly test our comprehensive Response Plan for all Cybersecurity Incidents, with clear protocols for immediate internal reporting and external notification to ADEK.

6.4. Digital Communications

- The Digital Media Policy is operational, ensuring that written parental consent is secured before taking and publishing any photographs/video recordings of students, specifying identification details.
- We strictly enforce rules on staff personal social media, including the prohibition of friending/following current students or parents, in line with the ADEK and GVIS Cultural Consideration Policy.
- Staff are required to only use school-issued email addresses for all professional communication with students and parents.

7. Roles and Responsibilities

All key roles are currently executing the following responsibilities in relation to this policy:

Role	Operational Responsibilities
Principal	Supervises and ensures the effective implementation and enforcement of all aspects of this policy; signs off on all major Digital Incidents.
Digital Wellbeing Committee/Lead	Manages the ongoing implementation of the Digital Strategy; chairs the annual policy review; oversees the cybersecurity incident response process.
Staff (Teachers & Admin)	Adheres to all RUPs; actively integrates digital competency outcomes into the curriculum; monitors student digital behavior in class; maintains required security standards (e.g., strong passwords, MFA compliance).
IT Department Technician	Maintains and continuously hardens the Secure Digital IT Architecture (Section 6.1); manages filtering and monitoring

	systems; executes automated, regular data backup and recovery procedures. Adheres to the Student Responsible Usage Policy;
Students	participates in digital safety education; is trained to immediately report any policy breach or incident to a staff member. Adheres to the Parent Responsible Usage Policy; actively monitors the
Parents/Guardians	child's use of digital devices and the internet outside of school hours; provides necessary consents for data and media use.

8. Compliance

8.1. Compliance Requirement

GVIS confirms that all stakeholders are required to strictly comply with all aspects of this Digital Policy, its subsidiary Responsible Usage Policies, and the relevant UAE Federal Laws listed in the References section. **8.2. Management of Non-Compliance**

- Students: Non-compliance (e.g., cyberbullying, accessing prohibited content, academic dishonesty) is managed in accordance with the ADEK Student Behavior Policy and GVIS Disciplinary Procedures. Staff: Non-compliance (e.g., data breach, inappropriate
- communication, security violation)
  is subject to disciplinary action, up to and including termination, in line with the MoE Code of Conduct for Professionals in General Education.
- Legal Violations: Any use of digital technology that violates UAE Federal Law (e.g., Federal Decree Law No. (34) of 2021 on Combatting Rumors and Cybercrimes) is immediately reported to the Abu Dhabi Police and ADEK.

9. Monitoring and Review

This policy is subject to a formal annual review, which is currently scheduled for April 2026. The review is conducted by the Digital Wellbeing Committee and is used to drive continuous improvement and ensure ongoing compliance.

The review process includes:

- Effectiveness Evaluation: Assessing the success of the Digital Strategy against set goals and student outcomes.

- Incident Analysis: Reviewing trends in Digital and Cybersecurity Incidents to identify systemic weaknesses and areas for policy refinement.
- Audit: Verifying that all mandatory systems (e.g., MFA, filtering, backups) are operational and meet the requirements of the Secure Digital IT Architecture.
- Stakeholder Feedback: Gathering feedback from staff, students, and parents on the clarity and effectiveness of the RUPs to provide necessary updates.

10.Approval and Effective Date

Thispolicy has been approved on April 9 2024 and effective on April 10 2024 and fully compliant in theschool by the same date.

Effective Date	**April 10 2024**
Compliance Date	**April 10 2025**
Next Review Date	**April 10 2026**

Principal