Digital Policy

Created	**September 2025**
Created by	IT Department
Reviewed by	**Principal – Ms. Suheir Salah** **Vice Principal – Ms. Nadine Chamssudeen**

Disclaimer: This policy has been developed in accordance with the school's national identity policy.

School Vision:

To be a leading private school in Al Ain that provides an exemplary learning environment in line with the vision of ADEK.

School Mission:

To provide an exemplary learning environment which

- Develops student abilities.
- Augment self-confidence.
- Prepares world-class learners.
- Enables students to meet the challenges of the 21st century.
- Increases productivity and self-esteem.
- Inculcates values required to become responsible members of society.

Table of Contents

Introduction

Purpose of this Handbook

Future International Academy (FIA) recognizes that the ability to function in the digital space is no longer optional but essential for education, work, and life. The widespread integration of digital technologies into teaching, learning, and administration requires schools to take deliberate steps to ensure their safe, secure, and effective use.

This handbook sets out FIA's official **Digital Policy**, which is fully aligned with the requirements of the **Abu Dhabi Department of Education and Knowledge (ADEK) School Digital Policy Version 1.1 (September 2024)**. It consolidates all mandatory documentation required by ADEK into a single authoritative reference for staff, students, parents, visitors, and inspectors.

The handbook:

- Defines FIA's **Digital Strategy (2025–2030)** and its roadmap for educational technology.
- Establishes **Responsible Usage Policies (RUPs)** for students, staff, parents, and visitors.
- Introduces a **framework for vendor and product selection** to ensure security and compliance.
- Details FIA's **Data and Cybersecurity Infrastructure**, including firewalls, MDM, encryption, and backups.
- Provides a **Cybersecurity Incident Response Plan** to guide the school in the event of breaches.
- Outlines FIA's **Data Protection Policy**, ensuring compliance with UAE law.
- Governs FIA's **Digital Media and Social Media usage** through detailed policies.
- Assigns oversight responsibilities to the **Digital Wellbeing Committee**.
- Presents a **Five-Year Roadmap** and **Annexes** with practical tools, forms, and templates.

Scope

This handbook applies to:

- **Students** using school-issued iPads, accessing the internet, or engaging with digital platforms.
- **Teachers and staff** using school computers, networks, systems, and emails.
- **Parents and guardians** engaging with FIA's digital communications and platforms.
- **Visitors and contractors** who access FIA's digital environment.

The policy covers **on-campus digital activities**, **school-issued devices taken home**, and **official digital communication channels**. It also provides guidance for parents on monitoring students' digital use outside of school hours.

Legal and Regulatory Framework

This handbook ensures compliance with all relevant **UAE federal laws and ADEK policies**, including:

- **Federal Decree Law No. 31 of 2021** – Crimes and Penalties (criminal liability for misuse of digital systems).
- **Federal Decree Law No. 34 of 2021** – Combatting Rumors and Cybercrimes (penalties for spreading misinformation, hacking, or unauthorized access).
- **Federal Decree Law No. 38 of 2021** – Copyrights and Related Rights (protection of intellectual property and prohibition of plagiarism).
- **Federal Decree Law No. 45 of 2021** – Protection of Personal Data (regulation of personal data collection, storage, and transfer).
- **ADEK Inclusion Policy** – requiring equal access to digital resources for students of determination.
- **ADEK Parent Engagement Policy** – requiring policies to be published in the Parent Handbook and online.
- **ADEK Student Behavior Policy** – establishing disciplinary responses to digital incidents.
- **ADEK Records Policy** – regulating record-keeping, backups, and data retention.

Accountability

- The **Principal** has overall accountability for compliance with this policy.
- The **IT Manager** is responsible for technical implementation.
- The **Social Worker** is responsible for monitoring and documenting student-related incidents.
- The **Digital Wellbeing Committee** is responsible for annual review, risk assessment, and oversight.

Review and Publication

- This handbook will be reviewed annually by the Digital Wellbeing Committee.
- Updated versions will be published on FIA's **school website** and included in the **Parent Handbook**.
- An age-appropriate version of the Responsible Usage Policy will be distributed to students in **Grades 1–5 (Annex 6)**.

1. Digital Strategy (2025–2030)

Future International Academy (FIA) has developed a comprehensive **five-year Digital Strategy** that aligns with the requirements of the **ADEK School Digital Policy (September 2024)**. This strategy is designed to ensure that technology is deployed responsibly and effectively to enhance **student learning outcomes, staff efficiency, and the overall safety and wellbeing of the school community**.

The FIA Digital Strategy is built on nine key pillars:

1.1 Teaching and Learning

The core of FIA's digital strategy is to **embed technology in teaching and learning**. Students are issued **iPads** that are centrally managed through **Mosyle Mobile Device Management (MDM)** and **Apple Classroom**. These systems allow teachers to:

- Whitelist applications and block unauthorized ones.
- Monitor student screens in real time.
- Share lesson content efficiently.
- Prevent distractions by locking or restricting devices.

ICT Labs are equipped with **NetSupport School** software, enabling teachers to supervise computer usage, demonstrate lessons directly on screens, and restrict internet access during assessments.

This infrastructure ensures compliance with **ADEK's requirement for appropriate filtering and monitoring systems** to protect students from exposure to harmful content (Section 4.2 of the ADEK Digital Policy).

Technology use in the classroom is not only about access but also about **learning outcomes**. FIA integrates digital literacy into lesson planning across all subjects. Students learn:

- How to evaluate online information critically.
- How to use productivity tools (e.g., Office 365, Google Workspace).
- How to collaborate responsibly using digital platforms.
- How to use digital resources without violating copyright law (**Federal Decree Law No. 38 of 2021**).

1.2 Inclusion and Assistive Technology

FIA is fully committed to the **ADEK School Inclusion Policy**. The Digital Strategy recognizes that students of determination and those with additional learning needs must have equal access to digital learning.

Assistive technologies deployed include:

- Text-to-speech and screen reader software for students with visual impairments.
- Speech-to-text tools for students with writing difficulties.
- Magnification tools and adjustable display settings for accessibility.
- Adapted keyboards or external devices where required.

Each case is documented in the student's **Individualized Learning Plan (ILP)** or **Individual Education Plan (IEP)**. IT staff collaborate with the Inclusion Department to procure, configure, and maintain assistive technology.

By embedding assistive technology into mainstream learning, FIA ensures compliance with **Federal Law No. 29 of 2006 on the Rights of People of Determination** and ADEK's specific guidance on inclusive education.

1.3 Digital Competencies

FIA defines **grade-specific digital competencies** for all students. These competencies are aligned with ADEK's expectations for student outcomes in the digital domain.

- **KG & Cycle 1 (Grades 1–5):** Students learn safe use of devices, responsible browsing, and simple creative applications (drawing, typing, presentations).
- **Cycle 2 (Grades 6–8):** Students are introduced to coding, responsible online collaboration, and research skills. Awareness sessions on cyberbullying and digital wellbeing are emphasized.
- **Cycle 3 (Grades 9–12):** Students engage in advanced ICT, digital design, programming, and responsible use of AI tools. They are taught about **digital ethics, privacy, and compliance with UAE cybercrime laws (Federal Decree Law No. 34 of 2021)**.

Teachers integrate these competencies into their lesson plans, and student progress is assessed through assignments, digital projects, and online testing.

1.4 Infrastructure and Security

FIA recognizes that a secure digital infrastructure is essential for safe and effective digital learning. Key elements include:

- **Huawei USG6000 Next-Generation Firewall (NGFW):** Provides identity-based filtering, intrusion prevention, and the ability to block VPNs.
- **Active Directory (ADDS) and Group Policy:** Secures staff PCs by enforcing password policies, enabling disk encryption, and controlling access permissions.
- **Endpoint Security:** All school PCs run **Windows Defender Antivirus**, which is kept updated through automated patching. iPads are fully controlled via Mosyle MDM.
- **Encryption:** All sensitive data is encrypted in transit (via SSL/TLS) and at rest (via BitLocker for PCs and encrypted Google Workspace storage).
- **Backups:** Critical data is backed up daily to **Google Workspace (cloud)**, **local school servers**, and **offline IT-managed backup PCs**. Annual **restoration drills** are conducted to ensure reliability.

This infrastructure design ensures compliance with **Section 6.1 of the ADEK Digital Policy**, requiring robust IT architecture and controls against unauthorized access.

1.5 Staff Development

Staff training is a key component of FIA's Digital Strategy. Each year, the school conducts mandatory sessions for all staff covering:

- FIA's Digital Policy requirements.
- Data protection obligations under **Federal Decree Law No. 45 of 2021**.
- Cybersecurity risks, including phishing and ransomware.
- Classroom management tools (Apple Classroom, NetSupport).
- Ethical use of AI and digital resources.

Staff are also required to complete additional training if they assume new responsibilities (e.g., system administrators, data managers). Training sessions are documented in the **Training Log (Annex 4)** for ADEK inspection.

1.6 Awareness Programs

FIA promotes digital safety across the school community. Awareness is delivered in three layers:

- **Teachers:** Annual IT training sessions delivered by the IT Manager and external experts.
- **Students:** Teachers cascade awareness into ICT lessons, covering topics like online safety, cyberbullying, plagiarism, scams, and digital wellbeing.
- **Parents:** FIA organizes parent awareness workshops and distributes guides on monitoring children's device use.

This ensures compliance with **Section 4.2 of ADEK's Digital Policy**, requiring age-appropriate awareness programs for students and engagement of parents.

1.7 Future-Proofing and Emerging Technologies

FIA's strategy is designed to be **future-ready**. The school commits to:

- Evaluating AI-powered learning platforms.
- Exploring VR/AR for science and history simulations.
- Investing in scalable cloud solutions.
- Regularly reviewing firewall and MDM licenses to maintain compliance.

By future-proofing its digital infrastructure, FIA ensures long-term resilience and adaptability.

1.8 Oversight

Oversight of the strategy rests with the **Digital Wellbeing Committee**, which:

- Reviews the Digital Strategy annually.
- Monitors progress against goals.
- Conducts risk assessments.
- Evaluates feedback from staff, students, and parents.
- Reports annually to ADEK as required.

This governance structure ensures that FIA not only complies with ADEK's Digital Policy but also continuously improves its digital practices.

2. Responsible Usage Policy (RUP)

The **Responsible Usage Policy (RUP)** of Future International Academy (FIA) defines the standards for acceptable, safe, and ethical use of school digital systems. It applies to **students, staff, parents, and visitors**, ensuring that everyone who interacts with FIA's digital environment does so responsibly.

This policy is a requirement under **Section 4.1 of the ADEK Digital Policy (September 2024)** and supports other ADEK frameworks, including the **Parent Engagement Policy**, the **Student Behavior Policy**, and the **Student Protection Policy**.

The RUP is published in the **Parent Handbook**, displayed on the **FIA website**, and communicated in age-appropriate formats to students in Grades 1–6.

2.1 Responsible Usage for Students

Students are at the heart of FIA's digital ecosystem. To protect their wellbeing and ensure learning outcomes, strict guidelines apply to all student use of digital devices and platforms.

- **Use of School-Issued iPads**

  Students may only use iPads issued by the school. These devices are managed through **Mosyle MDM** and monitored using **Apple Classroom**. Unauthorized modifications, such as tampering with restrictions, jailbreaking, or installing unapproved apps, are prohibited. This ensures a safe learning environment in line with ADEK's requirement for filtering and monitoring.

- **Prohibition of VPNs and Bypassing Controls**

  Students must not use Virtual Private Networks (VPNs), proxies, or similar tools to bypass FIA's filtering systems. VPN use not only undermines classroom control but also exposes students to harmful content. ADEK explicitly prohibits student VPN use (Section 4.1 of the Digital Policy).

- **Academic Integrity and AI Usage**

  Students must respect principles of academic honesty. Copying work, plagiarism, or using **AI tools** (e.g., ChatGPT, essay generators) to produce assignments without teacher approval is a violation of FIA's rules and **Federal Decree Law No. 38 of 2021 on Copyrights**. Students are taught how to use AI responsibly as a learning aid, not as a tool for misconduct.

- **Online Behavior and Cyberbullying**

  Students are expected to behave respectfully online. Acts of cyberbullying, harassment, or use of offensive language are treated seriously under the **ADEK Student Behavior Policy** and may involve escalation to ADEK or the Abu Dhabi Police under **Federal Decree Law No. 34 of 2021 (Cybercrimes)**.

- **Data Privacy**

  Students must never attempt to access or share personal data about peers or staff without authorization. Student accounts and passwords are personal and must not be shared.

Compliance Note: These controls ensure FIA protects students in line with ADEK's safeguarding requirements and UAE law.

2.2 Responsible Usage for Staff

Staff members have a duty not only to use technology responsibly themselves but also to **model correct behavior** for students.

- **Professional Use of School Systems**

  Staff must use FIA's digital resources strictly for professional and educational purposes. All communication with students and parents must occur through **school-issued email accounts**. Personal email addresses may not be used for school matters, as mandated by **Section 8.4 of the ADEK Digital Policy**.

- **Password Security and MFA**

  Staff must maintain secure, unique passwords and must not share credentials. With the rollout of **Multi-Factor Authentication (MFA)** for Google Workspace, staff are required to complete a second authentication step when logging in. This significantly reduces the risk of unauthorized account access.

- **Social Media Conduct**

  Staff may not post FIA-related content on personal social media platforms and must not use personal accounts to communicate with students or parents. They may, however, maintain professional profiles (e.g., on LinkedIn) as long as they avoid disclosing confidential FIA information. These rules align with **Section 8.3 of the ADEK Digital Policy** on personal social media use.

- **Data Protection Responsibilities**

  Staff are directly responsible for safeguarding student data. Uploading sensitive data to unapproved apps or sharing it outside authorized channels is a breach of FIA's **Data Protection Policy** and **Federal Decree Law No. 45 of 2021**.

- **Supervision of Students**

  Teachers must monitor students' digital use during lessons, intervening where misuse occurs. This reinforces FIA's responsibility to maintain a safe learning environment.

Compliance Note: These obligations ensure FIA meets ADEK's staff conduct standards and UAE's data protection requirements.

2.3 Responsible Usage for Parents

Parents play a vital role in supporting FIA's digital safeguarding framework, particularly outside school hours.

- **Monitoring and Guidance**

  Parents are expected to monitor their child's use of FIA-issued devices at home. They should report concerns about inappropriate content or behavior to the school's Social Worker or ICT staff.

- **Consent and Data Sharing**

  Parents must provide explicit consent for the use of student data, photos, or videos through the **Parent Consent Form (Annex 3)**. FIA shares student data with ADEK only where required by law, under **Federal Decree Law No. 18 of 2020 on Private Education** and **Law No. 9 of 2018 (Establishment of ADEK)**.

- **Awareness Participation**

  Parents are encouraged to attend FIA's digital awareness workshops. These sessions explain topics such as cyber safety, device monitoring, and screen time management. Parental participation reinforces consistency between home and school.

Compliance Note: These expectations satisfy ADEK's requirement for parent engagement in digital safety.

2.4 Responsible Usage for Visitors

All visitors, contractors, and invited speakers accessing FIA's premises are bound by usage restrictions.

- **Limited Digital Access**

  Visitors may use only the **guest Wi-Fi network**, which is segregated from school systems. Unauthorized access to FIA servers, devices, or student accounts is prohibited.

- **Restrictions on Media and Content**

  Visitors are not permitted to photograph, film, or publish content involving FIA students without prior written approval from the Principal and explicit parental consent.

- **Legal Consequences for Misuse**

  Any misuse of FIA's network or devices by visitors will result in immediate termination of access and, where necessary, escalation to ADEK or Abu Dhabi Police. Misuse may constitute an offense under **Federal Decree Law No. 31 of 2021**.

2.5 Communication and Enforcement

The RUP is not a static document; it is actively communicated and enforced.

- It is introduced during **student orientation** and reinforced in ICT lessons.
- Staff review it annually during **training sessions**.
- Parents receive it as part of the **Parent Handbook** and are updated through newsletters.
- Violations by students are recorded by the **Social Worker** using the **Digital Incident Report Form (Annex 1)** and addressed under the **ADEK Student Behavior Policy**.
- Violations by staff are addressed under the **ADEK Employment Policy**.
- Serious incidents are escalated to **ADEK** and, if criminal, to the **Abu Dhabi Police**.

3. Framework for External Providers and Products

Future International Academy (FIA) relies on external providers and third-party products for services such as IT support, software, cloud hosting, and educational applications. While these providers enable innovation and efficiency, they also present risks to **data security, student safety, and compliance with UAE law**.

To address these risks, FIA has developed a **Vendor Risk Assessment Framework** that ensures all external products and services meet high standards before being adopted. This framework is mandated by **Section 5.5 of the ADEK Digital Policy (September 2024)** and aligns with **Federal Decree Law No. 45 of 2021 on the Protection of Personal Data**.

3.1 Rationale

Engaging vendors without due diligence could expose FIA to breaches, inappropriate content, or unreliable services. The framework ensures that:

- Vendors comply with UAE laws on cybersecurity and data protection.
- Applications and platforms are safe for student use.
- Contracts include accountability measures for service delivery.

This structured process demonstrates FIA's responsibility in protecting its community and digital infrastructure.

3.2 Evaluation Criteria

Each external provider must undergo a **risk assessment** using FIA's official tool (see Annex 2). The criteria include:

- **System Compatibility**

  The provider's product must integrate seamlessly with FIA's existing environment, including Google Workspace, Mosyle MDM, and Huawei USG6000 NGFW. Incompatibility could create vulnerabilities or service disruptions.

- **Data Security and Privacy**

Vendors must demonstrate strong data protection measures, including encryption and access controls. They must comply with **Federal Decree Law No. 45 of 2021**, ensuring student and staff data is collected, stored, and processed lawfully. Data cannot be transferred outside the UAE without ADEK approval.

- **Cybersecurity Standards**

  Providers must follow recognized security frameworks, such as **ISO 27001** or **NIST Cybersecurity Framework**. For cloud-based services, FIA requires compliance with **Cloud SaaS Security Posture Management (SSPM)** to prevent misconfiguration and data leakage.

- **Threat Protection**

  Vendors must have robust measures for detecting and responding to cyber threats. This includes firewalls, monitoring tools, and an incident response process. Providers must disclose any history of breaches.

- **Backup and Recovery**

  Service providers must demonstrate business continuity through reliable backup and recovery plans. FIA requires assurances that in case of failure, services and data can be restored quickly.

- **Financial Stability and Reputation**

  FIA only partners with vendors who can demonstrate financial stability and a good reputation. References may be sought from other schools or institutions. Vendors with a history of non-compliance are excluded.

- **Educational Quality and Age Appropriateness**

  Educational applications must be aligned with FIA's American curriculum and tailored to the relevant age group. Content that conflicts with UAE values or exposes students to harmful material is not permitted.

Compliance Note: These evaluation criteria satisfy **ADEK's requirement** for schools to assess vendor compliance before adoption and ensure student safety.

3.3 Procurement Process

FIA follows a structured, transparent procurement process to select vendors:

1. **Request Submission** – Department heads submit a formal request for a new product or service.
2. **Preliminary IT Review** – The IT Manager evaluates the request against FIA's existing systems.
3. **Risk Assessment** – The **Vendor Risk Assessment Tool (Annex 2)** is completed.
4. **Committee Review** – The **Digital Wellbeing Committee** reviews findings and approves or rejects the vendor.
5. **Contracting** – Contracts must include:
    - **Non-Disclosure Agreements (NDAs)** restricting unauthorized data sharing.
    - **Service Level Agreements (SLAs)** defining uptime, support, and recovery terms.
    - Clauses requiring compliance with UAE law and ADEK policies.
6. **Implementation** – The IT department supervises setup and integration.
7. **Monitoring** – Vendor performance is monitored throughout the year.

This process ensures FIA maintains oversight and accountability over all external providers.

3.4 Vendor Obligations

All vendors engaged with FIA are contractually obligated to:

- Protect FIA's data in compliance with **Federal Decree Law No. 45 of 2021**.
- Notify FIA immediately in the event of a **data breach or cyber incident**.
- Limit data access only to authorized staff members.
- Cooperate with audits requested by ADEK or UAE regulators.

3.5 Monitoring and Review

- Vendors are reviewed annually by the Digital Wellbeing Committee.
- Non-compliant vendors are given a remediation deadline; failure to comply results in termination of the contract.
- The IT department maintains a **Vendor Risk Register** that documents all vendor assessments, reviews, and outcomes for ADEK inspection.

3.6 Legal Accountability

If a vendor violates FIA's standards or UAE law:

- Contracts are terminated immediately.
- ADEK is notified.
- Vendors may face legal consequences under **Federal Decree Law No. 34 of 2021 (Cybercrimes)** and **Federal Decree Law No. 45 of 2021 (Data Protection)**.

The Vendor Risk Assessment Framework ensures that FIA only engages with external providers who meet rigorous standards of security, compliance, and educational quality. By applying structured evaluation, transparent procurement, and annual monitoring, FIA demonstrates its commitment to safeguarding its digital environment and meeting ADEK's policy requirements.

4. Data and Cybersecurity Infrastructure

Future International Academy (FIA) recognizes that a secure digital infrastructure is essential for safeguarding students, staff, and sensitive data. In line with **Section 6.1 of the ADEK Digital Policy (September 2024)**, FIA has developed a multi-layered cybersecurity framework that combines technical controls, staff awareness, and compliance with UAE federal laws.

The school's cybersecurity strategy follows a "**defense-in-depth**" model, ensuring that if one control fails, others remain in place to protect FIA's systems and community.

4.1 Access Control

Access is restricted to authorized users only, based on **role and necessity**.

- **Multi-Factor Authentication (MFA):**

  FIA is rolling out MFA across its Google Workspace accounts. MFA requires both a password and a secondary verification (such as a mobile code), significantly reducing risks of account compromise. This step is aligned with **NIST best practices** and supports ADEK's requirement for secure login mechanisms.

- **Role-Based Access Control (RBAC):**

  Permissions are allocated strictly according to job roles. Teachers, for example, may access student academic data but cannot view HR or financial systems. This principle of least privilege prevents accidental or malicious misuse of access rights and ensures compliance with **Federal Decree Law No. 45 of 2021**.

- **Active Directory (ADDS) and Group Policy:**

  All staff accounts are centrally managed via ADDS, which enforces password complexity rules, account lockouts after repeated failed attempts, and automatic session timeouts. These measures prevent unauthorized access if a workstation is left unattended.

- **Quarterly Account Reviews:**

  The IT Manager conducts quarterly audits of user accounts, ensuring that inactive, graduated, or terminated users are promptly removed. Reports of these audits are kept for ADEK inspection, demonstrating ongoing compliance.

4.2 Data Encryption

Data is encrypted to prevent interception or unauthorized access.

- **Encryption in Transit:**

  All internet traffic, including emails and portal access, uses SSL/TLS encryption. This ensures communications between staff, students, and parents remain private and tamper-proof.

- **Encryption at Rest:**

  All staff PCs and laptops use BitLocker full-disk encryption. Google Workspace applies encryption to all stored files by default. Even if a device is lost, the data remains inaccessible without proper credentials.

- **Removable Media Controls:**

  USB drives and external storage must be encrypted before use with FIA systems. The IT Manager monitors compliance to reduce the risk of data leaks.

Compliance Note: These practices align with **Federal Decree Law No. 45 of 2021**, which requires adequate safeguards for personal data storage and transfer.

4.3 Network Security

FIA operates a secure, segmented network protected by a **Huawei USG6000 Next-Generation Firewall (NGFW)**.

- **Intrusion Prevention and VPN Blocking:**

  The firewall actively scans for malicious traffic, including intrusion attempts, malware, and denial-of-service attacks. It also blocks unauthorized VPNs that students might use to bypass controls, in line with **ADEK's prohibition of student VPN usage**.

- **Web Filtering:**

FIA enforces web filtering policies that block harmful categories such as adult content, gambling, or violence. The IT Manager reviews web filter violation reports monthly, and repeat issues are referred to the Social Worker for intervention.

- **VLAN Segmentation:**

  The network is segmented into VLANs for Admin, Teachers, Students, and Guests. This reduces the risk of data exposure — for example, even if a student device is compromised, it cannot access finance or HR networks.

- **Traffic Logging and Monitoring:**

  All network traffic is logged and stored for 12 months. Logs are reviewed monthly to identify unusual patterns (e.g., large outbound data transfers, repeated failed logins). ADEK can request these logs for compliance verification.

4.4 Endpoint Protection

All devices connected to FIA's systems are protected with multiple layers of endpoint security.

- **Windows Defender Antivirus:**

  All PCs and laptops are secured with Defender, which updates automatically against malware and ransomware. The IT department monitors update compliance.

- **Patch Management:**

  FIA enforces monthly patch cycles for all operating systems and applications. This ensures that vulnerabilities are closed before they can be exploited.

- **Device Encryption and Locking:**

  All FIA laptops and PCs are encrypted with BitLocker. Devices lock automatically after periods of inactivity, preventing misuse if left unattended.

- **MDM for iPads:**

Student iPads are managed through Mosyle MDM, which enforces app whitelisting, blocks unauthorized content, and allows teachers to monitor device use. Students cannot install or remove apps independently.

4.5 Backup and Recovery

A robust backup system protects FIA against data loss.

- **Daily Automated Backups:**

  Critical data (academic, HR, financial) is backed up daily across multiple platforms.

- **Multiple Storage Layers:**

  Data is stored in Google Workspace (cloud), on-site servers, and offline IT backup PCs. This three-tiered system provides redundancy.

- **Offline Vaulting:**

  Offline copies are stored securely in locked IT facilities, ensuring resilience against ransomware attacks.

- **Annual Restoration Drills:**

  FIA conducts annual restoration exercises, simulating data recovery after incidents. Results are documented and reviewed by the Digital Wellbeing Committee.

- **Disaster Recovery Plan (DRP):**

  FIA has a DRP defining procedures to restore critical systems after major disruptions such as fire, hardware failure, or cyberattack.

4.6 Awareness and Training

FIA embeds cybersecurity awareness across its community.

- **Staff Training:**

  All staff undergo annual sessions on phishing awareness, password hygiene, and secure handling of student data. Specialized staff (IT, HR, Finance) receive additional training on data protection and UAE law compliance.

- **Student Awareness:**

  ICT lessons include modules on cyberbullying, responsible social media use, identifying scams, and managing screen time. These are tailored by age group.

- **Parent Workshops:**

  FIA organizes sessions for parents to help them monitor student device usage at home and recognize online risks.

All sessions are recorded in the **Training Log (Annex 4)** as evidence for ADEK inspections.

4.7 Monitoring and Compliance

- Network and user logs are maintained for a minimum of 12 months.
- Logs from the NGFW, ADDS, and Google Admin are reviewed monthly.
- The Digital Wellbeing Committee evaluates compliance annually, including audits of account management, filtering, and backups.
- ADEK inspectors may request documentation, which FIA can provide on demand.

By combining access controls, encryption, network security, endpoint protections, backups, and awareness training, FIA ensures that its digital infrastructure is **resilient, secure, and compliant**. These measures fulfill ADEK's requirements under the Digital Policy and UAE laws, demonstrating FIA's commitment to protecting its students, staff, and digital environment.

5. Cybersecurity Incident Response Plan

Future International Academy (FIA) recognizes that no security system is foolproof and that **cybersecurity incidents** may occur despite preventive measures. To minimize disruption, protect sensitive information, and comply with regulatory requirements, FIA has established a **Cybersecurity Incident Response Plan (CIRP)**.

This plan ensures that FIA can **detect, contain, investigate, and recover** from incidents efficiently, while also meeting its obligations under the **ADEK Digital Policy (Section 6.4)** and UAE federal laws, including **Federal Decree Law No. 34 of 2021 (Combatting Rumors and Cybercrimes)**.

The CIRP applies to all staff, students, contractors, and vendors who access FIA systems or data.

5.1 Definition of an Incident

A **cybersecurity incident** at FIA includes, but is not limited to:

- Unauthorized access to FIA systems or accounts.
- Data breaches involving student or staff information.
- Malware or ransomware infections.
- Cyberbullying, online harassment, or distribution of harmful content.
- Attempted bypassing of FIA's controls (e.g., VPN misuse).
- Disruption of services such as email, Google Workspace, or school networks.

Compliance Note: This definition aligns with ADEK's requirement to classify both technical breaches and inappropriate digital behavior as incidents.

5.2 Detection and Reporting

Incidents may be detected through technical monitoring or reported by community members.

- **Technical Monitoring**

  FIA's Huawei NGFW, ADDS, and Google Admin consoles continuously monitor for unusual login activity, malware traffic, and suspicious data transfers. Alerts are sent to the IT Manager for investigation.

- **Staff and Student Reporting**

  Teachers and students are encouraged to report suspicious emails, cyberbullying, or inappropriate digital behavior to the IT Manager or Social Worker.

- **Incident Logging**

  Every report is documented in the **Digital Incident Report Form (Annex 1)**, ensuring accountability and traceability.

Compliance Note: Early detection and proper documentation fulfill **ADEK's requirement for safeguarding logs**.

5.3 Containment and Mitigation

When an incident is confirmed, FIA takes immediate steps to contain the impact.

- **Isolation of Affected Systems**

  Infected or compromised devices are disconnected from the network to prevent further spread.

- **Temporary Access Restrictions**

  User accounts involved in suspicious activity are suspended until the investigation is complete.

- **Blocking Harmful Content**

  If harmful websites or media are involved, the firewall and MDM policies are updated to prevent recurrence.

Compliance Note: These actions ensure adherence to **Federal Decree Law No. 31 of 2021 (Crimes and Penalties)** by preventing further misuse of digital systems.

5.4 Escalation and Communication

Not all incidents are equal in severity. FIA follows a tiered escalation model.

- **Internal Notification**

  The IT Manager immediately informs the Principal of any confirmed incident. For student-related incidents, the Social Worker is also notified.

- **External Notification**

  If the incident involves sensitive data or criminal behavior, FIA escalates the case to **ADEK** and, where necessary, to the **Abu Dhabi Police** in line with **Federal Decree Law No. 34 of 2021**.

- **Controlled Communication**

  Only the Principal or a designated spokesperson communicates externally (e.g., to parents or authorities). This prevents misinformation and complies with the UAE's laws on false reporting.

5.5 Investigation and Documentation

Each incident undergoes a structured investigation to determine root cause and impact.

- The IT Manager collects forensic evidence from logs, systems, and user reports.
- The Social Worker documents student-related incidents, including interviews and screenshots if necessary.
- Findings are recorded in the **Digital Incident Report Form (Annex 1)**, which is signed by the Principal.
- Evidence is stored securely for ADEK inspection and potential legal proceedings.

Compliance Note: This process satisfies **Section 6.4 of the ADEK Digital Policy**, which requires schools to investigate and document all incidents.

5.6 Recovery and Lessons Learned

FIA prioritizes restoring services while learning from incidents to strengthen defenses.

- **System Restoration**

  Data is recovered from backups as per FIA's Disaster Recovery Plan (see Section 4.5). Systems are reconfigured to prevent reinfection.

- **Policy Adjustments**

  If an incident reveals gaps in FIA's controls, policies (e.g., firewall rules, access policies) are updated accordingly.

- **Awareness Reinforcement**

  Staff and students are briefed on the incident and reminded of best practices to prevent recurrence.

- **Committee Review**

  The **Digital Wellbeing Committee** reviews major incidents in its annual meeting and includes lessons learned in FIA's risk register.

5.7 Testing and Preparedness

To ensure readiness, FIA conducts **annual tabletop exercises** simulating different scenarios, such as phishing campaigns, ransomware attacks, or cyberbullying incidents. These exercises test staff awareness and the school's ability to execute the CIRP effectively.

Compliance Note: Annual testing demonstrates proactive compliance with ADEK's expectations for incident preparedness.

FIA's Cybersecurity Incident Response Plan provides a structured, legally compliant process for handling digital threats. By focusing on **detection, containment, escalation, investigation, and recovery**, FIA minimizes disruption to learning while protecting its community. The inclusion of annual testing and committee oversight ensures continuous improvement and full alignment with ADEK's Digital Policy and UAE law.

6. Data Protection Policy and Plan

Future International Academy (FIA) is committed to protecting the privacy and security of all personal data it collects, processes, and stores. This includes information relating to students, parents, staff, and contractors. FIA's **Data Protection Policy and Plan** is aligned with **Federal Decree Law No. 45 of 2021 on the Protection of Personal Data** and **Section 6.5 of the ADEK Digital Policy (September 2024)**.

The policy ensures that FIA processes personal data lawfully, transparently, and for defined educational purposes. It also outlines how FIA responds to requests from parents, protects student records, and maintains compliance with ADEK's requirements for data retention and safeguarding.

6.1 Data Collection and Consent

FIA collects personal data only when it is required for educational or administrative purposes.

- **Parental Consent**

  Written consent is obtained from parents or guardians before collecting student personal data beyond mandatory academic records. Consent covers photos, videos, and participation in digital platforms. The **Parent Consent Form (Annex 3)** formalizes this process.

- **Informed and Transparent**

  Consent forms clearly explain what data will be collected, how it will be used, and whether it will be shared with third parties (e.g., ADEK or assessment providers). Parents are informed of their right to withdraw consent at any time without penalty.

- **Minimal Data Collection**

  FIA adheres to the principle of **data minimization**, ensuring that only the minimum necessary personal information is collected for specific purposes.

Compliance Note: These practices align with **Articles 4–6 of Federal Decree Law No. 45 of 2021**, which mandate lawful and transparent processing of personal data.

6.2 Data Classification and Handling

All data at FIA is classified and managed according to sensitivity:

- **Confidential Data** – Student medical records, safeguarding notes, and HR files. Access restricted to designated staff only.
- **Restricted Data** – Assessment results, report cards, and staff evaluations. Accessible by relevant departments.
- **Internal Data** – Lesson plans, teaching resources, and internal communications. Shared within the school community.
- **Public Data** – Information on FIA's website, brochures, and newsletters.

Each classification carries handling rules, such as encryption requirements, access restrictions, and sharing protocols. Staff receive annual training on these classifications.

Compliance Note: Data classification ensures compliance with ADEK's **School Records Policy** and the UAE's requirement to apply safeguards proportional to risk.

6.3 Vendor and Third-Party Data Protection

Vendors handling FIA data must comply with strict contractual obligations.

- **Non-Disclosure Agreements (NDAs):**

  All vendors sign NDAs preventing unauthorized use or disclosure of FIA data.

- **Restricted Data Transfers:**

  Vendors may not transfer FIA data outside the UAE without ADEK approval, in line with **Article 22 of Federal Decree Law No. 45 of 2021**.

- **Annual Reviews:**

  Vendors are reviewed annually using the **Vendor Risk Assessment Tool (Annex 2)** to confirm ongoing compliance.

Compliance Note: These requirements demonstrate FIA's due diligence in managing third-party data risk.

6.4 Data Retention and Storage

FIA follows a structured retention schedule:

- **Student Records:** Retained for the duration of enrollment and archived for seven years after graduation or withdrawal.
- **Staff Records:** Retained for the duration of employment and archived for seven years after departure.
- **Financial Records:** Retained for ten years in line with UAE accounting regulations.
- **Digital Media:** Retained only as long as parental consent remains valid. If consent is withdrawn, media is promptly deleted.

All digital records are stored in **Google Workspace**, protected by encryption and secure access controls.

Compliance Note: This schedule fulfills **Section 6.5 of the ADEK Digital Policy** and the **ADEK Records Policy** on retention and deletion.

6.5 Backup, Restoration, and Data Recovery

FIA ensures that data is not only stored securely but can also be restored if lost.

- **Daily Backups:** Critical data is backed up daily to cloud, local, and offline systems.
- **Annual Restoration Drills:** FIA tests recovery procedures annually to confirm reliability.
- **Secure Storage:** Offline backups are stored in a locked IT facility with restricted access.
- **Disaster Recovery Integration:** Data restoration is integrated into FIA's Disaster Recovery Plan (see Section 4.5).

6.6 Rights of Data Subjects

In compliance with UAE law, FIA recognizes the rights of individuals (students, staff, parents) regarding their data:

- **Right to Access:** Individuals may request access to their personal records.

- **Right to Correction:** Errors in personal data must be corrected upon request.
- **Right to Withdraw Consent:** Parents may withdraw consent for the use of student data or media at any time.
- **Right to Deletion:** Personal data must be deleted once it is no longer needed for its stated purpose.

Requests are managed by the IT Manager in coordination with the Principal, and responses are provided within 30 working days.

The Data Protection Policy and Plan ensures that FIA manages personal data with integrity, security, and transparency. By applying **data classification**, **parental consent**, **vendor obligations**, and **rights of individuals**, FIA complies with **Federal Decree Law No. 45 of 2021** and ADEK's Digital Policy. This framework protects the privacy of students, staff, and parents while supporting the school's operational and educational needs.

7. Digital Media and Social Media Policy

Future International Academy (FIA) recognizes that digital media and social media are powerful tools for communication, learning, and community engagement. However, their use also introduces risks related to privacy, cultural sensitivity, and safeguarding.

This policy ensures that FIA manages media responsibly and that staff, students, and parents understand their roles in maintaining the school's digital reputation. It aligns with **Section 8 of the ADEK Digital Policy (September 2024)** and complies with **Federal Decree Law No. 45 of 2021 on Personal Data Protection** and **Federal Decree Law No. 34 of 2021 on Cybercrimes**.

7.1 Digital Media (Photos, Videos, Recordings)

FIA uses digital media for educational and promotional purposes, such as showcasing student achievements, documenting school events, and publishing materials online or in print.

- **Parental Consent Requirement**

  No student photo, video, or audio recording may be taken or published without **written parental consent**. Parents indicate their preferences using the **Parent Consent Form (Annex 3)**, where they may agree to internal use (e.g., yearbooks, classroom displays) or external use (e.g., school website, social media).

- **Secure Storage of Media**

  Approved media files are stored in FIA's secure Google Workspace drives, with access restricted to authorized staff. Media is never stored on personal staff devices.

- **Withdrawal of Consent**

  Parents may withdraw consent at any time. In such cases, FIA immediately removes or deletes relevant media from its platforms and records.

Compliance Note: This practice ensures alignment with **Article 12 of Federal Decree Law No. 45 of 2021**, which grants individuals the right to withdraw consent for data use.

7.2 Official Social Media Accounts

FIA maintains official accounts on approved platforms (e.g., Instagram, Facebook, YouTube, LinkedIn) to share school news, celebrate achievements, and communicate with the community.

- **Principal Authorization**

  Only the Principal or a delegated Communications Officer may authorize the creation and management of FIA social media accounts. Unauthorized accounts are prohibited.

- **Moderation of Content**

  Content must be reviewed and approved before publication. Moderators are appointed to monitor comments, remove inappropriate posts, and respond to concerns.

- **Cultural and Legal Sensitivity**

  All posts must reflect UAE cultural values and avoid any content that could be considered offensive, disrespectful, or politically sensitive. This is in line with **Federal Decree Law No. 34 of 2021**, which penalizes the publication of unlawful or defamatory content.

- **Crisis Communication**

  In case of incidents (e.g., accidents, false rumors), FIA's social media may only be used for official, approved updates issued by the Principal. Staff are prohibited from sharing unofficial information.

7.3 Personal Use of Social Media by Staff

Staff members are role models and must use personal accounts responsibly.

- **No Direct Communication with Students/Parents**

  Staff may not use personal social media accounts to communicate with students or parents. All communication must occur through official school channels (email, iCampus, etc.).

- **No Publication of School Content**

Staff may not post FIA-related content, such as classroom activities or student work, on personal accounts without Principal approval. Even positive posts may inadvertently expose student identities or breach privacy.

- **Professional Boundaries**

  Staff may maintain professional profiles (e.g., on LinkedIn) but must avoid disclosing sensitive school information or making statements that could damage FIA's reputation.

Compliance Note: These measures fulfill **Section 8.3 of the ADEK Digital Policy**, which regulates staff use of personal accounts in relation to school content.

7.4 Student and Parent Use of Social Media

- **Students**

  Students must not create social media accounts representing FIA or post school-related content without authorization. Any incidents of cyberbullying, inappropriate posts, or sharing of harmful content are investigated under the **ADEK Student Behavior Policy**.

- **Parents**

  Parents are encouraged to support FIA's reputation online by using respectful language when discussing the school on social media. Concerns should be addressed directly to school leadership, not posted publicly.

Compliance Note: These expectations align with **ADEK's safeguarding framework**, ensuring responsible engagement by the broader school community.

7.5 Website Compliance

FIA's website serves as the school's official digital presence. It must:

- Display required information, including ADEK inspection reports, school fees, policies, and contact details.
- Publish student achievements only with parental consent.
- Be regularly reviewed for accuracy and compliance.

The Digital Media and Social Media Policy ensures that FIA communicates effectively while protecting students, respecting cultural norms, and complying with UAE law. By combining **strict consent procedures, official account management, staff restrictions, and website oversight**, FIA safeguards its community and maintains a professional digital reputation.

8. Oversight and Compliance

Future International Academy (FIA) recognizes that effective digital governance requires **clear oversight, structured accountability, and continuous review**. To ensure sustained compliance with the **ADEK Digital Policy (September 2024)** and UAE laws, FIA has established a **Digital Wellbeing Committee**.

This committee provides strategic direction, monitors implementation, and ensures that all digital policies are actively applied across the school. Oversight also involves regular audits, staff and student training, and stakeholder engagement to build a culture of digital safety and responsibility.

8.1 Digital Wellbeing Committee

The **Digital Wellbeing Committee** is FIA's central oversight body for digital policy.

- **Composition:**

  The committee includes the Principal (chair), IT Manager, Social Worker, and ICT Head of Department. External advisors may be invited as needed.

- **Roles and Responsibilities:**
  - The **Principal** holds ultimate accountability and ensures ADEK requirements are met.
  - The **IT Manager** manages technical implementation and compliance reporting.
  - The **Social Worker** documents digital incidents, supports affected students, and monitors wellbeing.
  - The **ICT HOD** ensures digital literacy is embedded in teaching and learning.
- **Meeting Schedule:**

  The committee meets at least **once per term** and conducts an **annual policy review**. Meeting minutes and decisions are documented for ADEK inspection.

Compliance Note: This governance model aligns with **Section 2.1 of the ADEK Digital Policy**, requiring schools to maintain oversight structures for digital initiatives.

8.2 Policy Review and Updates

FIA's digital policies are **living documents**, subject to continuous improvement.

- **Annual Review:**

  The committee reviews all policies annually, making updates based on new technologies, ADEK directives, or UAE legal changes.

- **Stakeholder Input:**

  Feedback is collected from staff, parents, and students through surveys and meetings to ensure policies remain relevant.

- **Documentation:**

  Updated policies are re-published in the Parent Handbook, shared via email to staff, and uploaded to FIA's website.

Compliance Note: This fulfills **ADEK's requirement for periodic review and transparency** in digital safeguarding policies.

8.3 Risk Assessment and Auditing

The committee conducts structured risk assessments and internal audits.

- **Quarterly IT Risk Reviews:**

  The IT Manager identifies vulnerabilities in systems (e.g., expired licenses, misconfigured settings) and proposes mitigation steps.

- **Annual Internal Audit:**

  Using the **Internal Audit Checklist (Annex 5)**, the committee verifies compliance in areas such as firewall licensing, backups, account management, and awareness training.

- **External Penetration Testing:**

Every 1–2 years, FIA engages external cybersecurity firms to conduct penetration tests, ensuring that defenses meet industry standards.

Compliance Note: These processes demonstrate proactive compliance with **ADEK's inspection framework** and UAE cybersecurity best practices.

8.4 Training and Capacity Building

Oversight includes monitoring whether staff, students, and parents are trained to meet FIA's digital safety standards.

- **Staff Training Logs:**

  All staff training sessions are recorded and audited annually to ensure 100% participation.

- **Student Programs:**

  ICT-based awareness modules are reviewed each term to ensure age-appropriateness and consistency with ADEK safeguarding requirements.

- **Parent Engagement:**

  Attendance at parent workshops is tracked, and digital safety guides are regularly distributed.

Compliance Note: Documented training evidence supports compliance with **Section 4.2 of the ADEK Digital Policy** on awareness programs.

8.5 Incident Oversight

The Digital Wellbeing Committee monitors how incidents are managed and documented.

- **Incident Logs:**

  The Social Worker and IT Manager maintain a shared Digital Incident Log, recording all reported cases.

- **Committee Review:**

Major incidents are reviewed in committee meetings to evaluate response effectiveness and update policies if needed.

- **Escalation Monitoring:**

  The committee ensures serious incidents are escalated to ADEK or Abu Dhabi Police where legally required.

Compliance Note: This oversight ensures FIA meets **ADEK's requirement for structured incident response and documentation**.

8.6 Reporting to ADEK

- FIA submits digital policy updates, training logs, and audit findings to ADEK during inspections.
- Evidence of compliance, including forms from Annexes 1–5, is maintained for inspection.
- Non-compliance identified during ADEK inspections is addressed within 30 working days, with corrective measures reported back to ADEK.

Oversight and compliance at FIA are achieved through a structured governance framework led by the Digital Wellbeing Committee. By conducting annual reviews, audits, training monitoring, and structured incident oversight, FIA ensures continuous alignment with **ADEK Digital Policy standards** and UAE laws. This framework also creates a culture of accountability, transparency, and digital safety across the entire school community.

9. Five-Year Compliance Roadmap (2025–2030)

Future International Academy (FIA) recognizes that digital compliance is not a one-time exercise but an ongoing commitment requiring planning, investment, and continuous improvement. To meet the evolving requirements of the **ADEK Digital Policy (September 2024)** and UAE cybersecurity laws, FIA has developed a structured **five-year compliance roadmap**.

This roadmap ensures that FIA remains proactive in upgrading its infrastructure, enhancing awareness, and meeting ADEK inspection requirements. It is reviewed annually by the **Digital Wellbeing Committee** and updated in light of technological developments, ADEK directives, and emerging threats.

Year 1 (2025/26): Foundation and Activation

The first year focuses on establishing the foundations for full compliance.

- **Firewall Licensing Renewal**

  FIA will renew the Huawei USG6000 NGFW license to ensure uninterrupted access to intrusion prevention, VPN blocking, and filtering features. Without renewal, filtering logs may not be compliant with ADEK's safeguarding requirements.

- **MFA Activation for Google Workspace**

  Multi-Factor Authentication (MFA) will be rolled out across all staff and administrative accounts. This step significantly reduces risks from stolen or weak passwords, aligning with UAE cybersecurity best practices.

- **ADDS and Group Policy Enforcement**

  FIA will complete the implementation of Active Directory Domain Services (ADDS) with Group Policies for password enforcement, screen lockouts, and access controls. This establishes robust identity management across staff PCs.

- **Policy Publication**

  The Digital Policy Handbook will be finalized, approved, and published on FIA's website and in the Parent Handbook, as required by ADEK.

Year 2 (2026/27): Assessment and First Audit

The second year focuses on assessment and the first external audit.

- **Vendor Risk Assessments**

  All existing vendors and newly proposed providers will be assessed using the **Vendor Risk Assessment Tool (Annex 2)**. Non-compliant vendors will be remediated or terminated.

- **External Penetration Test**

  FIA will engage a licensed cybersecurity company to conduct its first **penetration test**, simulating real-world cyberattacks. Results will be documented and corrective actions applied.

- **Parent Survey on Digital Safety**

  FIA will conduct a survey of parents to measure awareness of digital risks and gather feedback for future improvements.

Year 3 (2027/28): Strategy Refresh and Cloud Security Audit

The third year emphasizes reviewing progress and strengthening cloud compliance.

- **Digital Strategy Review**

  The Digital Wellbeing Committee will conduct a mid-cycle review of the 2025–2030 Digital Strategy. New objectives will be set in line with emerging technologies, including AI and VR in education.

- **Cloud Security Audit**

  An independent audit of FIA's Google Workspace and other SaaS platforms will be conducted to ensure correct configuration and compliance with **Cloud SaaS Security Posture Management (SSPM)** standards.

- **Staff Training Curriculum Update**

  Training programs will be refreshed to include new topics, such as AI ethics, deepfakes, and evolving phishing tactics.

Year 4 (2028/29): Infrastructure Renewal and Advanced Testing

The fourth year focuses on infrastructure upgrades and reinforcing resilience.

- **Firewall Upgrade or Renewal**

  FIA will evaluate whether to upgrade to a newer NGFW model or renew the current licensing, based on ADEK inspection feedback and vendor recommendations.

- **Second Penetration Test**

  A second penetration test will be conducted to evaluate improvements since Year 2 and identify new vulnerabilities.

- **Awareness Program Refresh**

  FIA will update its student, staff, and parent awareness materials to reflect new online risks, including social engineering attacks and AI-based threats.

Year 5 (2029/30): Consolidation and Strategy Renewal

The final year focuses on consolidation and preparing for the next five-year cycle.

- **Full Internal Audit**

  The **Internal Audit Checklist (Annex 5)** will be used to conduct a comprehensive review of all digital practices. Results will be documented for ADEK inspection.

- **ADEK Compliance Review**

  FIA will undergo a full ADEK review of its digital policies and implementation. Evidence from annexes, training logs, and incident reports will be submitted.

- **New Five-Year Strategy (2030–2035)**

  The Digital Wellbeing Committee will develop a new strategy to guide FIA's digital transformation, ensuring continuity and resilience for the next cycle.

The **Five-Year Compliance Roadmap** provides FIA with a structured, forward-looking plan to remain compliant with ADEK requirements and UAE law. By focusing on **foundational implementation, external audits, strategy refresh, infrastructure renewal, and consolidation**, FIA demonstrates proactive digital governance and a long-term commitment to safeguarding its school community.

Annexes – Digital Policy Handbook

Annex 1: Digital Incident Report Form

This form must be completed for all digital incidents at FIA, including cyberbullying, data breaches, inappropriate access, or technical failures. The form ensures structured documentation, accountability, and escalation in line with Section 6.4 of the ADEK Digital Policy.

Instructions: Completed by staff who identify/report the incident, signed by Principal, stored securely.

Date of Incident	_____
Time of Incident	_____
Location	_____
Reported by (Name/Role)	_____
Individuals Involved	_____
Description of Incident	_____
Immediate Actions Taken	_____
Escalation Required (ADEK/Police/Vendor)	_____
Follow-Up Actions	_____
Signatures (IT, Social Worker, Principal)	_____

Annex 2: Vendor Risk Assessment Tool

This tool must be completed before approving any new external provider or application. It ensures compliance with Federal Decree Law No. 45 of 2021 and ADEK Digital Policy Section 5.5.

Assessment Category	Guiding Questions	Compliance Check	Comments/Evidence
Compatibility	Does it integrate with FIA systems?	☐ Yes ☐ No	
Data Protection	Does vendor comply with UAE law, encryption?	☐ Yes ☐ No	
Hosting Location	Is data hosted in UAE or ADEK-approved?	☐ Yes ☐ No	
Cybersecurity	Follows ISO/NIST standards?	☐ Yes ☐ No	
Backup & Recovery	Does vendor provide DRP?	☐ Yes ☐ No	
Financial Stability	Is the vendor reputable, sustainable?	☐ Yes ☐ No	
Educational Suitability	Age-appropriate, curriculum aligned?	☐ Yes ☐ No	

Annex 3: Parent Consent Form (Media Usage)

This form captures parental consent for the use of student photos, videos, and digital media. It complies with Federal Decree Law No. 45 of 2021 and ADEK Digital Policy Section 8.1.

Student Name: _____

Grade/Class: _____

Parent/Guardian Name: _____

Consent Options:

☐ Photograph for internal school use (classroom, yearbook)

☐ Video recording for internal school use (assemblies, projects)

☐ Featured in external publications (website, newsletters)

☐ Featured on official FIA social media accounts

Signature of Parent/Guardian: _____ Date: _____

Annex 4: Training and Awareness Session Log

This log provides evidence that staff, students, and parents have received cybersecurity and digital safety training, as required under ADEK Digital Policy Section 4.2.

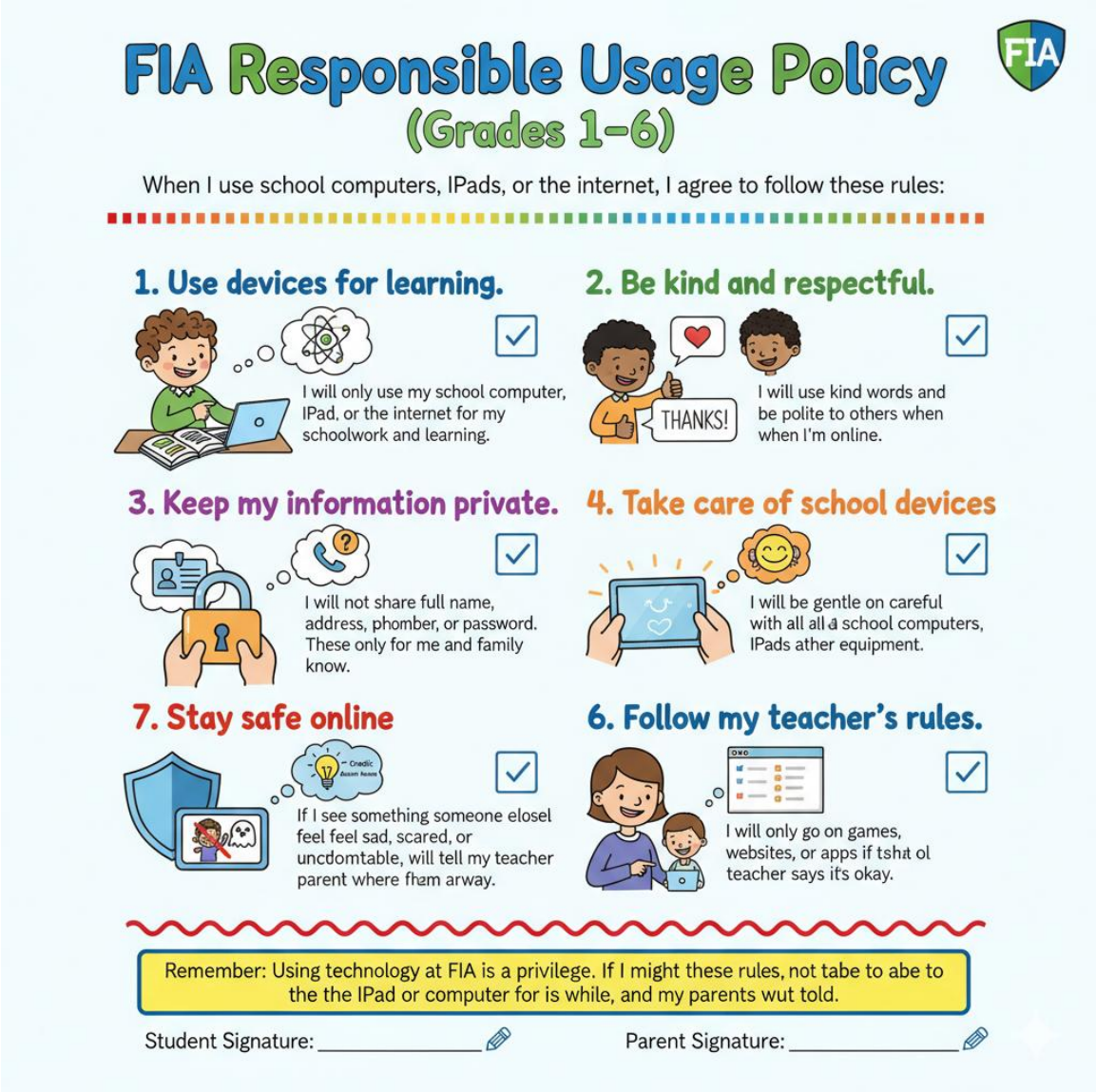
Date of Session	_____
Audience (Staff/Students/Parents)	_____
Title/Topic of Session	_____
Facilitator/Trainer	_____
Duration	_____
Key Learning Outcomes	_____
Attendance (%)	_____
Feedback/Comments	_____

Annex 5: Internal Audit Checklist

The Internal Audit Checklist ensures FIA's policies are reviewed annually and compliance is documented. This fulfills ADEK's requirement for annual reviews and audits.

Area	Requirement	Compliance Status	Evidence/Comments
Firewall	NGFW license renewed and active	☐ Yes ☐ No	
MFA	Activated for Google Workspace	☐ Yes ☐ No	
ADDS	Group Policies enforced	☐ Yes ☐ No	
Web Filtering	Monthly reports reviewed	☐ Yes ☐ No	
Endpoint Security	Defender updated, devices encrypted	☐ Yes ☐ No	
Backups	Daily backups, annual restoration drill	☐ Yes ☐ No	
Incident Reporting	Logs completed in Annex 1	☐ Yes ☐ No	
Training	Logs completed in Annex 4	☐ Yes ☐ No	
Vendor Review	Annex 2 completed	☐ Yes ☐ No	
Parent Consent	Forms collected (Annex 3)	☐ Yes ☐ No	

Annex 6: FIA Responsible Usage Policy (Grades 1-5)



Sample image. Working on the updated RUP