Digital Policy

Approved on: October 28, 2024
Approved by: Bertrand Ferret
Implementation date: October 28, 2024
Revision date: NA

Purpose

- Set out ADEK's requirement that LFITM develop and implement a digital strategy regarding their use of technology, goals related to digital competencies and infrastructure, digital security measures, and required resources.
- Ensure that LFITM invests in the development of students' digital skills and competencies to empower them to maximize learning opportunities presented by the use of technology.
- Ensure that LFITM educates students on the responsible and safe access and usage of the online environment and protects students from digital content and interactions that are inappropriate or harmful.
- Ensure that LFITM puts in place systems, mechanisms, and procedures that are safe, balanced, and appropriate to safeguard their digital security.
- Ensure that LFITM 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.

Policy

Required Documentation
LFITM develops and implements the following documents, and make them available on their website in both Arabic and English or their language of instruction, in line with the requirements of this Policy:

1. Digital strategy (see Section 2.1 Digital Strategy).
2. Responsible usage policies (see Section 4.1 Responsible Usage Policies).
3. Framework for the selection of external providers and products (see Section 5.4 External Providers and Products).
4. Data and Cybersecurity Infrastructure (see Section 6.1 Secure Digital IT Architecture).
5. Response plan in relation to cybersecurity incidents (see Section 6.6 Cybersecurity Incidents).
6. School data protection plan and policy (see Section 7. Data Protection).
7. Digital media policy and social media policy (see Section 8. Digital Communications).
8. Digital Strategy and Oversight

Digital Strategy: LFITM shall develop and implement a digital strategy that outlines and provides rationale for their digital goals over a 5-year time frame. The strategy shall include:

1. 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 administration).
2. Assessment of how LFITM can use and provide assistive technology to enable inclusion.
3. Goals related to student digital skills and competencies that enable learning.
4. Development, procurement, and implementation plans for digital infrastructure, software, and hardware.
5. Mechanisms for ensuring the security of LFITM's digital systems.
6. Plan for future-proofing LFITM's digital infrastructure, where applicable.
7. Resources and investment required to deliver the digital strategy.
8. Staff training requirements.
9. Increase awareness related to emerging technologies (e.g., artificial intelligence).

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

1. Develop and implement LFITM's digital strategy.
2. Conduct an annual review of the digital strategy and its implementation:
   a. Monitor progress against student learning goals and development and procurement plans.
   b. Evaluate technology, software, and online platforms to ensure they meet the objectives of the strategy.
   c. Test and conduct risk assessments of LFITM's digital systems and infrastructure (e.g., backup recovery) to ensure they are secure and fit for purpose.
   d. Review the effectiveness of LFITM's data and cybersecurity provisions.
   e. Re-evaluate the technological needs of LFITM based on feedback from staff, parents, and students, and plan procurement and digital development accordingly.
   f. Re-evaluate staff digital development needs and identify additional training required.
3. Develop, implement, and review other LFITM policies required in line with this policy.
4. Engage with relevant stakeholders (e.g., the Digital Officer, Head of IT) to inform its decisions.

LFITM appoints a staff member to liaise with ADEK for matters related to digital competency, safety, and security.

Digital Competencies

Student Outcomes: LFITM defines digital competencies and expected outcomes for students by grade/year and integrates these into LFITM's curriculum. LFITM ensures 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 School Inclusion Policy.

Staff Training: LFITM provides 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 LFITM's digital infrastructure and policies, student digital learning outcomes, data protection, cybersecurity, and the digital safety measures implemented by LFITM.

Responsible Usage and Digital Safeguarding

Responsible Usage Policies: LFITM develops and communicates responsible digital usage policies for students, parents, staff, and visitors. These policies shall set out what these groups are permitted/prohibited to do on LFITM's premises, network, and systems, and shall include:

1. The definition of responsible usage of LFITM's software, network, services, and digital devices issued by LFITM, including shared devices.
2. Rules on the permitted and restricted use of personal devices on the LFITM network and premises, and during extracurricular activities that take place outside LFITM (e.g., field trips). LFITM restricts the use of Virtual Private Networks (VPNs) by students on LFITM's premises or through LFITM networks unless explicitly authorized for specific educational or administrative purposes.
3. Standards in relation to the use of personal social media accounts by staff (see Section 8.3. Personal Social Media Accounts for Staff).
4. LFITM's rules in relation to the setting and sharing of passwords for LFITM accounts.
5. Standards in relation to the sharing of data related to LFITM or the LFITM 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.
6. 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 Related Rights and the ADEK terms and conditions, copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.
7. LFITM communicates the relevant responsible usage policies to students, parents, staff, and visitors via appropriate channels. LFITM publishes responsible usage policies applicable to students and parents on the LFITM website and in the Parent Handbook, as per the ADEK School Parent Engagement Policy. For all younger students up to Grade 6/Year 7, LFITM provides age-appropriate versions of the policy to students, and a full version of the policy to parents.

Safeguarding Students: LFITM puts in place education programs and effective systems to protect students from the online risks stated below.

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

LFITM puts in place the following programs, systems, mechanisms, and procedures to safeguard students against online risks and promote their wellbeing:
a. An age-appropriate awareness program 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).
b. Appropriate filtering and monitoring systems to monitor student internet use on LFITM devices and systems.
c. Regular analysis of students' internet usage and web filter violations to identify potential adverse trends or problems.
d. 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 School Student Mental Health Policy and the ADEK School Student Behavior Policy.
e. Mechanisms to enable safeguarding during activities conducted virtually (e.g., disabling private chat for students).

LFITM ensures there is a developmental purpose before allowing students to use the Internet during school hours.

Digital Incidents:

1. A digital incident occurs when a member of the LFITM 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 LFITM regulations in an online setting.
2. Where a digital incident occurs during LFITM hours or in settings covered in LFITM's digital policies, LFITM shall make interventions and provide support to students and/or staff in line with the relevant policy (e.g., ADEK School Employment Policy, ADEK School Staff Wellbeing Policy, ADEK School Student Administrative Affairs Policy, ADEK School Parent Engagement Policy, ADEK School Student Behavior Policy, and the ADEK School Student Protection Policy). Where required, LFITM reports digital incidents to ADEK and cooperates with the Abu Dhabi Police for investigations.
3. LFITM ensures that every digital incident is recorded, documented, and signed by the Principal and stored for auditing purposes, in line with the ADEK School Records Policy.

LFITM requires parents to monitor students' usage of digital devices outside of LFITM premises and hours to ensure safe and appropriate digital behavior.

Digital Infrastructure

Digital Devices: LFITM ensures that digital devices issued to members of the school community have appropriate security features. Where LFITM 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, LFITM shall define and implement digital safety precautions (e.g., minimum device specifications, and antivirus requirements).

Digital Systems for Staff:LFITM ensures that relevant staff members have access to digital systems provided by ADEK, including the Learning Management System.

Distance Learning Readiness: LFITM adopts 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).

Lycée Français International Théodore Monod
Al Dhiba Street | PO Box 6572 | Saadiyat Island
Abu Dhabi, UAE | +971 2 443 4447
accueil.ltm@aflec-fr.org
ltmonod.aflec-fr.org
aflec-fr.org

Assistive Technology: LFITM provides assistive technology to students with additional learning needs as indicated in their Documented Learning Plan, in line with the ADEK School Inclusion Policy.

External Providers and Products: LFITM develops 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:
a. Compatibility with existing school systems.
b. Secure management of data.
c. Compliance with cybersecurity standards and frameworks.
d. Security against cyber threats.
e. Service delivery and backup/recovery provisions.
f. Reputation and financial stability of the provider.
g. 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.
h. Where relevant (e.g., learning application providers), educational quality, and age-appropriateness of content.

LFITM communicates 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.

Data and Cybersecurity

Secure Digital IT Architecture: LFITM establishes a robust secure digital infrastructure and ensure the relevant cybersecurity controls are implemented as follows:

1. Access Control
   a. Implement multi-factor authentication mechanisms across critical services.
   b. Define and enforce role-based access control to ensure users have appropriate permissions.
2. Data Encryption
   a. Employ encryption for data in transit and at rest to safeguard sensitive information.
3. Network Security
   a. Deploy next-generation firewalls and intrusion detection/prevention systems to protect against unauthorized access.
   b. Ensure web filtering policies are enforced.
   c. Ensure the ability to block inappropriate content.
   d. Ability to detect infected machines across the school network.
   e. Ensure identity-based firewalls are implemented to provide granular visibility on user browsing activity.
   f. Establish a unified security edge architecture for all internet browsing.
   g. Regularly monitor and audit network traffic for unusual patterns.
4. Endpoint Protection
   a. Install and update anti-virus/anti-malware software on all LFITM-managed devices.
   b. Implement hard disk device encryption and ensure regular security patching.
5. Data Backup and Recovery
   a. Establish automated regular backup procedures for critical data.
   b. Ensure backups are vaulted and stored offline.
   c. Develop a robust disaster recovery plan to minimize downtime in case of a security incident.
6. Data Security
   a. Establish data classification controls across school and student data.
   b. Implement Data Loss Prevention Tools to ensure data leaks or exfiltration is prevented.
7. Security Awareness Training
   a. Conduct regular training sessions for staff and students to raise awareness about cybersecurity threats and best practices.
8. Incident Response Plan
   a. Develop and regularly update an incident response plan to address security breaches promptly and effectively.
   b. Perform a tabletop cyber-attack simulation and exercise with school management involvement.

Lycée Français International Théodore Monod
Al Dhiba Street | PO Box 6572 | Saadiyat Island
Abu Dhabi, UAE | +971 2 443 4447
accueil.ltm@aflec-fr.org
ltmonod.aflec-fr.org
aflec-fr.org

9. Physical Security
   a. Ensure secure access to physical servers, networking equipment, and other critical infrastructure.
10. Regulatory Compliance
    a. Ensure compliance with local and international data protection regulations and standards.
11. Monitoring and Logging
    a. Implement comprehensive monitoring systems to detect and respond to security incidents in real-time.
    b. Maintain detailed logs for auditing and analysis purposes.
12. Secure Software Development
    a. Follow secure coding practices when developing or procuring educational software.
    b. Regularly update and patch software to address vulnerabilities.
13. Cloud Security
    a. If using cloud services, ensure the selected providers adhere to stringent security standards.
    b. Implement proper configuration and access controls for cloud resources.
    c. Integrate Cloud Services – Software as a Service (SaaS) with school identity services where possible.
    d. Establish Cloud SaaS Security Posture Management capabilities.
14. Collaboration Security
    a. Secure communication and collaboration platforms to protect sensitive educational information shared among students and staff.
15. Third-Party Security
    a. Vet and monitor third-party vendors providing educational technology solutions to ensure they meet security standards.

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

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

Safe Virtual Interaction with Invited Visitors: LFITM seeks 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 School Extracurricular Activities and Events Policy and the ADEK School Student Protection Policy.

Backup and Storage: LFITM has onsite data storage systems to ensure that backups of important information, software, and configuration settings are performed in line with the ADEK School Records Policy with regard to frequency and appropriate period of time.

1. LFITM ensures that such backups are stored securely and separately from the school network.
2. LFITM that use external cloud systems for storage shall ensure that their data is synced to the cloud.
   6.6 Cybersecurity Incidents: LFITM develops response and business continuity plans to guide staff in the event of a cybersecurity incident, including the protocols for reporting the incident to the school leadership team and to ADEK, and the process for maintaining operational continuity.
3. LFITM shall not communicate any cybersecurity incident to external parties except for the service provider involved and ADEK.
4. LFITM adheres to all applicable laws and policies set out by the Department of Government Enablement and any other relevant authorities in the UAE, including the Federal Decree Law No. (34) of 2021 on Combating Rumors and Cyber Crimes.

Data Protection

Data Protection Policy: LFITM develops a Data Protection Policy, setting out how LFITM ensures 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:

1. The specification of the types of personal information that may be collected.
2. The requirement and procedures for individual consent in the collection, processing, and storage of **personal**

Lycée Français International Théodore Monod
Al Dhiba Street | PO Box 6572 | Saadiyat Island
Abu Dhabi, UAE | +971 2 443 4447
accueil.ltm@aflec-fr.org
ltmonod.aflec-fr.org
aflec-fr.org

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

3. The conditions under which personal information may be shared by LFITM with other individuals or entities (e.g., with ADEK).
   a. LFITM 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.
   7.2 Sharing Data with ADEK: LFITM 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 its amendments 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.
4. LFITM shall inform parents of their obligations to share data with ADEK accordingly.

Data Protection Plan: LFITM develops and annually reviews a data protection plan, in compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data and the amendments and the ADEK School Records Policy.

Digital Communications

Digital Media Policy: LFITM develops, implements, and monitors a Digital Media Policy governing the creation and publication of digital media. The policy includes, at a minimum:

1. The requirement to obtain consent before recording and publishing digital media:
   a. LFITM only takes photographs and/or video recordings of students after obtaining written consent from parents. In obtaining consent, LFITM informs parents about the purposes for which the photographs and/or video recordings are being taken.
   b. LFITM obtains written consent from parents before publishing digital content involving students. LFITM shall clearly specify if the student will be identified by name in the publication when obtaining consent.
2. The procedures for the provision and withdrawal of consent.
3. Conditions related to the storage and security of digital media.
4. Conditions related to the use of personal devices and accounts for recording or publishing LFITM content.

Social Media Policy: LFITM develops and implements a Social Media Policy in relation to the use of social media by the school.

1. The policy includes, at a minimum:
   a. Social media platforms and accounts to be used by LFITM.
   b. Access, security, and password protection procedures for LFITM's social media accounts.
   c. Conditions related to content, language use, and engagement with other accounts.
   d. Conditions related to the use of names, photos, and videos of students, in accordance with Section 8.1. Digital Media Policy.
   e. Guidelines for moderators (see Section 8.2.3 Moderators) in relation to content posted by third parties on LFITM's social media pages, including procedures to manage disrespectful content and trolling.
   f. Procedures for addressing other adverse social media behaviors, such as impersonation of LFITM's accounts.
2. Monitoring LFITM Communications: LFITM shall regularly monitor all official and unofficial LFITM-related communication channels (newsletters, social media, parent communication groups, etc.) to ensure their compliance with this policy.
3. Moderators: LFITM shall appoint moderator(s) to pre-approve or remove content posted by other users on the LFITM's social media pages, where possible, in line with the LFITM's guidelines. Moderator(s) shall reject or remove, where possible, content that is inappropriate, not in line with UAE cultural values, or amounts to bullying, harassment, discrimination, or intimidation, in line with the ADEK School Values and Ethics Policy and the ADEK School Cultural Consideration Policy.

Lycée Français International Théodore Monod
Al Dhiba Street | PO Box 6572 | Saadiyat Island
Abu Dhabi, UAE | +971 2 443 4447
accueil.ltm@aflec-fr.org
ltmonod.aflec-fr.org
aflec-fr.org

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

1. Not use email addresses issued by LFITM to create such accounts.
2. Use the tightest possible privacy settings.
3. Not identify themselves as being associated with LFITM, except on professional social media platforms (e.g., LinkedIn).
4. 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.
5. Not accept invitations from parents of current students to friend, connect with, or follow them.
6. 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).
7. 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.
8. Ensure that content shared through such accounts is appropriate, in line with the ADEK School Cultural Consideration Policy, and does not amount to bullying, harassment, discrimination, or intimidation, in line with the ADEK School Values and Ethics Policy.
9. Ensure that content shared through such accounts does not give the impression of being endorsed by LFITM.
10. Ensure that they do not share any confidential information related to LFITM through such accounts.

Communications via Email: LFITM informs staff members that they are not authorized to use personal email addresses to communicate with students or parents.

LFITM Website: LFITM creates a dedicated website and keeps it up to date to serve as a reference for members of the LFITM community.

1. LFITM publishes the following content on their website, at a minimum:
   a. Contact information.
   b. Services provided by LFITM.
   c. Fees, including transportation fees and fees for optional activities.
   d. Inspection reports.
   e. Aggregate student achievement data or individual achievements (e.g., awards), with consent.
   f. Public versions of the annual report, in line with the ADEK School Reporting Policy.
   g. LFITM policies that are relevant to parents and/or students.
   h. Any other required content, as defined by ADEK policies.
2. LFITM ensures that the content published on their website is accurate and appropriate, in line with the ADEK School Values and Ethics Policy.
3. LFITM ensures that content published on their website is in line with the requirements for digital media (see Section 9.1. Digital Media Policy).

Reference

2024 (September) ADEK_School_Digital Policy_v.1.1 Department of Knowledge and Education (ADEK)

Lycée Français International Théodore Monod
Al Dhiba Street | PO Box 6572 | Saadiyat Island
Abu Dhabi, UAE | +971 2 443 4447
accueil.ltm@aflec-fr.org
ltmonod.aflec-fr.org
aflec-fr.org