Digital Policy

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

Objectif

Établir une stratégie numérique: Exiger que le LFITM élabore et mette en œuvre une stratégie numérique complète couvrant l'utilisation des technologies, les infrastructures numériques, les objectifs en matière de compétences numériques, les mesures de sécurité digitale, ainsi que les ressources nécessaires.
Promouvoir les compétences numériques des élèves: Veiller à ce que le LFITM investisse dans le développement des compétences numériques des élèves, afin de leur permettre de tirer pleinement parti des opportunités d'apprentissage offertes par la technologie.
Éduquer à l'utilisation responsable et sécurisée du numérique: S'assurer que le LFITM forme les élèves à un usage responsable, sûr et éthique des environnements numériques, tout en les protégeant contre les contenus ou interactions en ligne inappropriés ou nuisibles.
Assurer la sécurité numérique: Exiger la mise en place par le LFITM de systèmes, procédures et mécanismes appropriés, équilibrés et efficaces pour garantir la sécurité numérique et la protection des données personnelles des élèves.
Garantir la conformité légale: S'assurer que le LFITM respecte les exigences du Centre de Contrôle et de Surveillance et se conforme au Décret-loi fédéral n° 45 de 2021 sur la protection des données personnelles, notamment en ce qui concerne la collecte, le traitement et le stockage des données personnelles.

Politique

Documentation Requise: Le LFITM élabore et met en œuvre les documents suivants, qui doivent être rendus disponibles sur leur site internet en arabe et en anglais (ou dans leur langue d'enseignement), conformément aux exigences de la présente politique:

- Stratégie numérique *(voir Section 2.1 – Stratégie numérique)*
- Politiques d'utilisation responsable *(voir Section 4.1 – Politiques d'utilisation responsable)*
- Cadre de sélection des prestataires externes et des produits *(voir Section 5.4 – Prestataires externes et produits)*
- Infrastructure de données et de cybersécurité *(voir Section 6.1 – Architecture numérique et informatique sécurisée)*
- Plan de réponse aux incidents de cybersécurité *(voir Section 6.6 – Incidents de cybersécurité)*
- Plan et politique de protection des données scolaires *(voir Section 7 – Protection des données)*
- Politique sur les médias numériques et les réseaux sociaux
  (voir Section 8 – Communications numériques)

Stratégie numérique: Le LFITM doit élaborer et mettre en œuvre une stratégie numérique définissant ses objectifs numériques et leur justification sur une période de cinq ans. Cette stratégie devra inclure les éléments suivants :

1. Orientation stratégique globale sur la manière dont la technologie sera utilisée pour améliorer la réussite et les résultats des élèves (par exemple : renforcer l'enseignement et l'apprentissage, soutenir une gestion administrative efficace et efficiente).
2. Évaluation de l'utilisation des technologies d'assistance pour favoriser l'inclusion et l'accessibilité au sein de l'établissement.
3. Objectifs liés aux compétences et à la culture numérique des élèves, en lien avec l'apprentissage et l'autonomie dans un environnement technologique.

4. Plans de développement, d'acquisition et de mise en œuvre des infrastructures numériques, logiciels et matériels.
5. Mécanismes de sécurité pour garantir la protection des systèmes numériques du LFITM.
6. Plan d'anticipation et d'adaptabilité pour assurer la pérennité de l'infrastructure numérique, lorsque cela est applicable.
7. Ressources et investissements nécessaires à la mise en œuvre de la stratégie numérique.
8. Besoins en formation du personnel, afin de renforcer les compétences numériques des enseignants et du personnel administratif.
9. Sensibilisation accrue aux technologies émergentes, notamment l'intelligence artificielle (IA), et leur impact potentiel sur l'éducation.

Supervision: Un Comité de Bien-être Numérique ou un responsable désigné aura les responsabilités suivantes en ce qui concerne la supervision de la stratégie numérique de LFITM et des politiques associées :

1. Élaborer et mettre en œuvre la stratégie numérique de LFITM.
2. Effectuer un examen annuel de la stratégie numérique et de sa mise en œuvre, incluant :
    - Suivre les progrès réalisés par rapport aux objectifs d'apprentissage des élèves et aux plans de développement et d'acquisition.
    - Évaluer les technologies, logiciels et plateformes en ligne pour s'assurer qu'ils répondent aux objectifs de la stratégie.
    - Tester et effectuer des évaluations des risques sur les systèmes et infrastructures numériques de LFITM (par exemple, la récupération des données de sauvegarde) pour garantir leur sécurité et leur adéquation avec les besoins de l'établissement.
    - Examiner l'efficacité des dispositifs de protection des données et de cybersécurité de LFITM.
    - Réévaluer les besoins technologiques de LFITM sur la base des retours du personnel, des parents et des élèves, et planifier l'acquisition et le développement numérique en conséquence.
    - Réévaluer les besoins en développement numérique du personnel et identifier toute formation supplémentaire nécessaire.
3. Développer, mettre en œuvre et réexaminer les autres politiques de LFITM requises conformément à cette politique.
4. Collaborer avec les parties prenantes pertinentes (par exemple, le Responsable Numérique, le Responsable IT) pour informer ses décisions.

Nommer un membre du personnel pour communiquer avec ADEK sur les questions liées à la compétence numérique, à la sécurité et à la cybersécurité.

Compétences Numériques

Résultats des élèves: Le LFITM définit les compétences numériques et les résultats attendus pour les élèves par niveau/année et les intègre dans le programme scolaire du LFITM. Le LFITM veille à disposer de l'infrastructure numérique et des ressources nécessaires pour soutenir les élèves dans l'atteinte de ces résultats, y compris les élèves ayant des besoins éducatifs supplémentaires, conformément à la politique d'inclusion scolaire d'ADEK.

Formation du Personnel: Le LFITM fournit une formation pertinente au personnel en fonction de ses fonctions, afin de leur permettre de promouvoir les objectifs de cette politique. La formation couvre des sujets tels que : l'infrastructure et les politiques numériques du LFITM, les résultats d'apprentissage numérique des élèves, la protection des données,la cybersécurité, et les mesures de sécurité numérique mises en place par le LFITM.

Utilisation Responsable et Protection Numérique

Politiques d'Utilisation Responsable: Le LFITM élabore et communique des politiques d'utilisation responsable du numérique pour les élèves, les parents, le personnel et les visiteurs. Ces politiques doivent préciser ce que ces groupes sont autorisés à faire et interdits de faire sur les locaux, le réseau et les systèmes du LFITM, et inclure les éléments suivants :

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

1. La définition de l'utilisation responsable des logiciels, réseaux, services et appareils numériques fournis par le LFITM, y compris les appareils partagés.
2. Les règles concernant l'utilisation autorisée et restreinte des appareils personnels sur le réseau et les locaux du LFITM, ainsi que lors d'activités parascolaires organisées en dehors du LFITM (par exemple, les sorties scolaires). Le LFITM limite l'utilisation des réseaux privés virtuels (VPN) par les élèves sur les locaux du LFITM ou via ses réseaux, sauf autorisation explicite à des fins éducatives ou administratives spécifiques.
3. Les normes concernant l'utilisation des comptes personnels de réseaux sociaux par le personnel (voir la Section 8.3 – Comptes de réseaux sociaux personnels pour le personnel).
4. Les règles du LFITM concernant la définition et le partage des mots de passe des comptes LFITM.
5. Les normes relatives au partage de données liées au LFITM ou à la communauté LFITM, ainsi que les canaux par lesquels ces données peuvent être partagées lorsqu'elles sont autorisées. Cela inclut les normes relatives au téléchargement des données des élèves sur des applications externes et des outils d'apprentissage, le cas échéant.
6. Les normes en matière d'honnêteté académique, de plagiat et d'utilisation responsable des œuvres protégées par des droits d'auteur et des outils numériques (par exemple, l'intelligence artificielle), conformément au Décret-Loi Fédéral n° (38) de 2021 sur les droits d'auteur et droits connexes et aux conditions d'utilisation, à la politique de droits d'auteur et à la politique de confidentialité des données d'ADEK, concernant la collecte, l'utilisation et la divulgation des informations.
7. Le LFITM communique les politiques d'utilisation responsable pertinentes aux élèves, aux parents, au personnel et aux visiteurs via les canaux appropriés. Le LFITM publie les politiques d'utilisation responsable applicables aux élèves et aux parents sur le site web du LFITM et dans le manuel des parents, conformément à la politique d'engagement des parents d'ADEK. Pour les élèves plus jeunes jusqu'en Grade 6/Year 7, le LFITM fournit des versions adaptées à l'âge de la politique aux élèves, et une version complète de la politique aux parents.

Protection des Élèves: Le LFITM met en place des programmes éducatifs et des systèmes efficaces pour protéger les élèves contre les risques en ligne suivants :

Risques en ligne auxquels les élèves sont exposés :

a. Exposition à des contenus inappropriés, illégaux ou susceptibles de nuire à leur bien-être.
b. Exposition à des interactions en ligne non sécurisées (par exemple, interaction avec des utilisateurs ayant des profils falsifiés).
c. Comportement en ligne personnel pouvant entraîner des préjudices pour soi-même ou pour autrui (par exemple, s'engager dans le cyberharcèlement).
d. Escroqueries et risques financiers tels que le jeu en ligne et le phishing.

Le LFITM met en place les programmes, systèmes, mécanismes et procédures suivants pour protéger les élèves contre les risques en ligne et promouvoir leur bien-être :

a. Un programme de sensibilisation adapté à l'âge pour tous les élèves, abordant les bienfaits de la technologie, la prise de conscience des risques en ligne, l'auto-évaluation des risques en ligne lors de l'utilisation de la technologie, les mesures de sécurité en ligne, et l'impact des habitudes numériques sur le bien-être (par exemple, l'impact de la durée d'utilisation des appareils numériques).Systèmes de filtrage et de surveillance appropriés pour suivre l'utilisation d'Internet par les élèves sur les appareils et systèmes du LFITM.
b. Analyse régulière de l'utilisation d'Internet des élèves et des violations des filtres web afin d'identifier d'éventuelles tendances ou problèmes négatifs.
c. Procédures pour identifier et soutenir les élèves qui semblent développer des habitudes numériques risquées, excessives ou illégales, telles que l'addiction numérique ou le jeu en ligne, conformément à la politique ADEK sur la santé mentale des élèves et à la politique ADEK sur le comportement des élèves.
d. Mécanismes de protection lors des activités menées virtuellement (par exemple, désactivation du chat privé pour les élèves).

Le LFITM s'assure qu'il existe un objectif pédagogique clair avant de permettre aux élèves d'utiliser Internet pendant les heures de classe.

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

Incidents Numériques

1. Un incident numérique se produit lorsqu'un membre de la communauté du LFITM utilise de manière inappropriée la technologie numérique. Cela inclut une violation des politiques d'utilisation raisonnables, l'accès à des contenus inappropriés, des comportements ou communications inappropriés, du cyberharcèlement, ou toute autre violation des règlements du LFITM dans un environnement en ligne.
2. Lorsqu'un incident numérique se produit pendant les heures du LFITM ou dans des contextes couverts par les politiques numériques du LFITM, ce dernier doit intervenir et fournir un soutien aux élèves et/ou au personnel conformément à la politique pertinente (par exemple, la politique d'emploi de l'école ADEK, la politique de bien-être du personnel ADEK, la politique des affaires administratives des élèves ADEK, la politique d'engagement des parents ADEK, la politique de comportement des élèves ADEK et la politique de protection des élèves ADEK). Lorsque cela est nécessaire, le LFITM signale les incidents numériques à ADEK et coopère avec la police d'Abou Dhabi pour les enquêtes.
3. Le LFITM veille à ce que chaque incident numérique soit enregistré, documenté et signé par le principal et conservé à des fins d'audit, conformément à la politique des dossiers scolaires ADEK.

Le LFITM exige que les parents surveillent l'utilisation des appareils numériques par les élèves en dehors des locaux et des heures du LFITM pour garantir un comportement numérique sûr et approprié.

Infrastructure Numérique

Appareils Numériques: Le LFITM s'assure que tous les appareils numériques fournis aux membres de la communauté scolaire sont équipés de fonctionnalités de sécurité appropriées.
Lorsque le LFITM autorise le personnel à accéder aux données ou aux systèmes scolaires depuis d'autres appareils, ou lorsqu'une politique BYOD (Bring Your Own Device) est en place pour le personnel ou les élèves, le LFITM définit et applique les mesures de sécurité numérique nécessaires (par exemple, spécifications minimales des appareils, exigences en matière d'antivirus).

Systèmes Numériques pour le Personnel: Le LFITM veille à ce que les membres du personnel concernés aient accès aux systèmes numériques fournis par ADEK, y compris le système de gestion de l'apprentissage..

Préparation à l'Enseignement à Distance: Le LFITM adopte des mesures adaptées à l'enseignement à distance en cas de situations d'urgence telles que des fermetures temporaires de l'établissement ou pour des élèves dans des circonstances exceptionnelles (par exemple, un séjour prolongé à l'hôpital ou un déplacement d'urgence à l'étranger avec les parents pour une durée prolongée).

Technologies d'Assistance: Le LFITM fournit des technologies d'assistance aux élèves ayant des besoins éducatifs particuliers, conformément à leur Plan d'Apprentissage Personnalisé, et en ligne avec la politique d'inclusion scolaire d'ADEK.

Fournisseurs et Produits Externes: Le LFITM développe un cadre d'évaluation des risques liés aux prestataires externes pour la sélection des fournisseurs de services informatiques et des produits liés au réseau, aux systèmes et à l'infrastructure de l'école. Cela inclut les fournisseurs d'applications d'apprentissage ainsi que les applications open source. Ce cadre doit inclure, au minimum, les éléments suivants :

a. Compatibilité avec les systèmes existants de l'école.
b. Gestion sécurisée des données.
c. Conformité aux normes et cadres en matière de cybersécurité.
d. Protection contre les menaces cybernétiques.
e. Conditions de prestation de service ainsi que les dispositifs de sauvegarde et de récupération.
f. Réputation et stabilité financière du fournisseur.
g. Respect par le fournisseur du Décret-loi fédéral n° (45) de 2021 sur la protection des données personnelles, ainsi que des conditions générales d'ADEK, de la politique de droits d'auteur et de la politique de confidentialité des données, concernant la collecte, l'utilisation et la divulgation des informations.
h. Lorsque cela est pertinent (par exemple pour les fournisseurs d'applications éducatives), la qualité éducative du contenu ainsi que son adéquation à l'âge des élèves.

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

Le LFITM informe clairement les fournisseurs externes qu'ils sont soumis au Décret-loi fédéral n° (45) de 2021 sur la protection des données personnelles ainsi qu'aux conditions générales, à la politique de droits d'auteur et à la politique de confidentialité des données d'ADEK, en ce qui concerne la collecte, l'utilisation et la divulgation des informations.

Données et Cybersécurité

Architecture Numérique Sécurisée de l'IT: Le LFITM établit une infrastructure numérique sécurisée robuste et s'assure que les contrôles en matière de cybersécurité sont mis en œuvre comme suit :

1. **Contrôle d'Accès**

a. Mise en œuvre de mécanismes d'authentification multi-facteurs pour les services critiques.
b. Définir et appliquer un contrôle d'accès basé sur les rôles pour garantir que les utilisateurs disposent des autorisations appropriées.

2. **Cryptage des Données**

a. Utilisation du cryptage des données pendant le transit et au repos pour protéger les informations sensibles.

3. **Sécurité du Réseau**

a. Déploiement de pare-feu de nouvelle génération et de systèmes de détection/prévention d'intrusions pour se protéger contre l'accès non autorisé.
b. Veiller à l'application des politiques de filtrage web.
c. Assurer la capacité de bloquer les contenus inappropriés.
d. Capacité à détecter les machines infectées sur le réseau de l'école.
e. S'assurer que des pare-feu basés sur l'identité sont mis en œuvre afin d'avoir une visibilité granulaire de l'activité de navigation des utilisateurs.
f. Établir une architecture de sécurité unifiée pour toute la navigation internet.
g. Surveiller et auditer régulièrement le trafic réseau pour repérer des modèles inhabituels.

4. **Protection des Points de Terminaison (Endpoint Protection)**

a. Installer et mettre à jour les logiciels antivirus/antimalware sur tous les appareils gérés par le LFITM.
b. Mettre en œuvre le chiffrement des disques durs et assurer l'application régulière des correctifs de sécurité.

5. **Sauvegarde et Reprise des Données**

a. Établir des procédures de sauvegarde automatisées et régulières pour les données critiques.
b. Garantir que les sauvegardes sont externalisées et stockées hors ligne.
c. Développer un plan robuste de reprise après sinistre pour minimiser les interruptions en cas d'incident de sécurité.

6. **Sécurité des Données**

a. Mettre en place un système de classification des données scolaires et des données élèves.
b. Implémenter des outils de prévention des pertes de données (Data Loss Prevention) pour éviter toute fuite ou extraction non autorisée.

7. **Formation à la Sensibilisation à la Sécurité**

a. Organiser des sessions de formation régulières pour le personnel et les élèves afin de sensibiliser aux menaces cyber et aux bonnes pratiques.

8. **Plan de Réponse aux Incidents**

a. Élaborer et mettre à jour régulièrement un plan de réponse aux incidents afin de traiter rapidement et efficacement

toute violation de sécurité.
b. Réaliser une simulation de cyberattaque (tabletop exercise) impliquant la direction de l'établissement.

9. **Sécurité Physique**

a. Assurer un accès sécurisé aux serveurs physiques, équipements réseau et autres infrastructures critiques.

10. **Conformité Réglementaire**

a. Veiller à la conformité avec les réglementations locales et internationales en matière de protection des données.

11. **Surveillance et Journalisation**

a. Mettre en œuvre des systèmes de surveillance complets permettant de détecter et de répondre en temps réel aux incidents de sécurité.
b. Maintenir des journaux détaillés pour les besoins d'audit et d'analyse.

12. **Développement Logiciel Sécurisé**

a. Adopter des pratiques de codage sécurisé lors du développement ou de l'acquisition de logiciels éducatifs.
b. Mettre à jour régulièrement les logiciels pour corriger les vulnérabilités.

13. **Sécurité Cloud**

a. En cas d'utilisation de services cloud, veiller à ce que les fournisseurs choisis respectent des normes de sécurité strictes.
b. Mettre en place une configuration correcte et des contrôles d'accès adaptés aux ressources cloud.
c. Intégrer les services Cloud (SaaS) aux systèmes d'identité de l'école dans la mesure du possible.
d. Mettre en place des capacités de gestion de la posture de sécurité Cloud (Cloud SaaS Security Posture Management).

14. **Sécurité des Plateformes Collaboratives**

a. Sécuriser les plateformes de communication et de collaboration afin de protéger les informations éducatives sensibles partagées entre élèves et personnel.

15. **Sécurité des Fournisseurs Tiers**

a. Évaluer et surveiller les fournisseurs tiers de solutions technologiques éducatives afin de garantir qu'ils respectent les normes de sécurité.

Maintenance du Système : LFITM doit maintenir et mettre à jour régulièrement l'infrastructure numérique, les systèmes d'exploitation, les systèmes de sécurité et les logiciels, y compris les logiciels de protection antivirus. LFITM doit régulièrement tester leur infrastructure et leurs systèmes numériques afin de s'assurer qu'ils sont en bon état de fonctionnement.

Utilisation Sécurisée des Applications d'Apprentissage Externes: LFITM dispose de mécanismes de protection (par exemple, des systèmes d'authentification unique) pour garantir la sécurité des élèves et des systèmes lors de l'utilisation d'applications d'apprentissage externes.

Interactions Virtuelles Sécurisées avec des Invités : LFITM cherche le consentement des parents pour toute interaction virtuelle en direct avec des invités, à l'intérieur ou à l'extérieur de la classe. Toutes ces interactions doivent également être approuvées par ADEK, conformément à la Politique des Activités et Événements Extracurriculaires de l'École ADEK et à la Politique de Protection des Élèves de l'École ADEK.

Sauvegarde et Stockage : LFITM dispose de systèmes de stockage de données sur site afin de garantir que les

sauvegardes des informations importantes, des logiciels et des paramètres de configuration sont effectuées conformément à la Politique des Archives Scolaires de l'ADEK, en ce qui concerne la fréquence et la durée appropriée de conservation. LFITM veille à ce que ces sauvegardes soient stockées de manière sécurisée et séparément du réseau scolaire. LFITM utilisant des systèmes cloud externes pour le stockage s'assure que leurs données sont synchronisées avec le cloud.

Incidents de Cybersécurité : LFITM développe des plans de réponse et de continuité des activités pour guider le personnel en cas d'incident de cybersécurité, y compris les protocoles pour signaler l'incident à l'équipe de direction de l'école et à ADEK, ainsi que le processus pour maintenir la continuité des opérations.
LFITM ne doit communiquer aucun incident de cybersécurité à des parties externes, à l'exception du fournisseur de services impliqué et d'ADEK. LFITM respecte toutes les lois et politiques applicables établies par le Département de la Gouvernment Enablement et toutes les autres autorités compétentes aux Émirats Arabes Unis, y compris le Décret-Loi Fédéral No. (34) de 2021 sur la Lutte contre les Rumeurs et les Cybercrimes.

Protection des Données

Politique de Protection des Données : LFITM développe une Politique de Protection des Données, définissant comment LFITM garantit que les informations personnelles sont traitées correctement et en toute sécurité, conformément au Décret-Loi Fédéral No. (45) de 2021 sur la Protection des Données Personnelles, qui doit inclure, au minimum :

1. La spécification des types d'informations personnelles qui peuvent être collectées.

2. Les exigences et procédures pour obtenir le consentement individuel lors de la collecte, du traitement et du stockage des informations personnelles :

- Le consentement doit être donné librement, spécifique, éclairé et sans ambiguïté.

- Le consentement peut être retiré par l'individu à tout moment.

3. Les conditions dans lesquelles les informations personnelles peuvent être partagées par LFITM avec d'autres individus ou entités (par exemple, avec ADEK) :

- LFITM doit inclure un accord de confidentialité dans tous les contrats avec des prestataires, stipulant que les données personnelles ne peuvent être partagées à l'intérieur ou à l'extérieur du pays, sauf si cela est explicitement autorisé par ADEK.

Partage des Données avec ADEK : LFITM doit fournir des données précises et à jour aux personnels autorisés d'ADEK sur demande, conformément au Décret-Loi Fédéral No. (18) de 2020 sur l'Éducation Privée et ses amendements, ainsi qu'à la Loi No. (9) de 2018 concernant la création du Département de l'Éducation et de la Connaissance, et en accord avec les termes et conditions d'ADEK et la politique de confidentialité des données concernant la collecte, l'utilisation et la divulgation des informations.

LFITM doit informer les parents de leurs obligations de partager des données avec ADEK en conséquence.

Communications numériques

Politique relative aux médias numériques : Le LFITM élabore, met en œuvre et supervise une politique relative aux médias numériques régissant la création et la publication de contenus numériques. Cette politique comprend, au minimum :

1.L'obligation d'obtenir un consentement avant d'enregistrer et de publier des contenus numériques :

a. Le LFITM ne prend des photographies et/ou des enregistrements vidéo des élèves qu'après avoir obtenu un

consentement écrit des parents. Lors de l'obtention du consentement, le LFITM informe les parents des finalités pour lesquelles les photographies et/ou vidéos sont prises.
b. Le LFITM obtient également un consentement écrit avant de publier tout contenu numérique impliquant des élèves, en précisant clairement si l'élève sera identifié par son nom dans la publication.

2.Les procédures de fourniture et de retrait du consentement.
3.Les conditions relatives au stockage et à la sécurité des médias numériques.
4.Les conditions d'utilisation d'appareils personnels et de comptes personnels pour l'enregistrement ou la publication de contenus du LFITM.

Politique relative aux réseaux sociaux : Le LFITM élabore et met en œuvre une politique relative à l'utilisation des réseaux sociaux par l'établissement. Cette politique comprend, au minimum :

a. Les plateformes de réseaux sociaux et les comptes qui seront utilisés par le LFITM.
b. Les procédures de sécurité, de gestion des accès et de protection des mots de passe pour les comptes du LFITM.
c. Les règles concernant le contenu, le langage et les interactions avec d'autres comptes.
d. Les conditions liées à l'utilisation des noms, photos et vidéos des élèves, conformément à la section 8.1 sur les médias numériques.
e. Les lignes directrices pour les modérateurs (voir section 8.2.3) sur les contenus publiés par des tiers sur les pages du LFITM, y compris la gestion des contenus inappropriés et des commentaires agressifs (trolling).
f. Les procédures à suivre en cas de comportements nuisibles liés aux réseaux sociaux, tels que l'usurpation d'identité des comptes du LFITM.

Surveillance des communications du LFITM : Le LFITM surveille régulièrement tous les canaux de communication officiels et non officiels liés à l'établissement (bulletins d'information, réseaux sociaux, groupes de communication parents, etc.) afin de garantir leur conformité à cette politique.

Modérateurs : Le LFITM désigne un ou plusieurs modérateurs pour approuver ou supprimer les contenus publiés par d'autres utilisateurs sur ses pages de réseaux sociaux, lorsque cela est possible, conformément aux directives du LFITM. Les modérateurs doivent rejeter ou supprimer, si possible, tout contenu qui est :

- Inapproprié
- Contraire aux valeurs culturelles des Émirats arabes unis
- Constitue un cas de harcèlement, intimidation, discrimination ou intimidation en ligne
  Conformément à la politique des valeurs et de l'éthique d'ADEK et à la politique des considérations culturelles d'ADEK.

Comptes personnels sur les réseaux sociaux (personnel) : Le LFITM autorise les membres du personnel à créer et maintenir leurs comptes personnels sur les réseaux sociaux. Concernant ces comptes, les membres du personnel doivent :

- Ne pas utiliser les adresses e-mail du LFITM pour créer ces comptes.

- Utiliser les paramètres de confidentialité les plus stricts.

- Ne pas s'identifier comme étant affiliés au LFITM, sauf sur des plateformes professionnelles (ex. : LinkedIn).
- Ne pas accepter ni envoyer d'invitations de connexion à des élèves actuels ou anciens de moins de 18 ans.
- Ne pas accepter d'invitations provenant des parents d'élèves actuels.
- Ne pas utiliser ces comptes pour communiquer avec des élèves actuels, leurs parents ou d'anciens élèves de moins de 18 ans, y compris via des applications de messagerie (WhatsApp, Telegram, Signal).
- Considérer tout contenu publié comme public, même avec des paramètres de confidentialité élevés, et agir avec discrétion.
- Veiller à ce que le contenu publié soit approprié, respectueux des valeurs culturelles des Émirats arabes unis, et conforme aux politiques ADEK sur les valeurs et l'éthique.
- Ne pas laisser penser que le contenu publié est approuvé ou soutenu par le LFITM.

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

- Ne jamais partager de données confidentielles liées au LFITM via ces comptes.

Communication par e-mail : Le LFITM informe les membres du personnel qu'ils ne sont pas autorisés à utiliser des adresses e-mail personnelles pour communiquer avec les élèves ou leurs parent**s.**

Site Web du LFITM : Le LFITM crée un site Web dédié et le maintient à jour pour servir de référence aux membres de la communauté du LFITM.

Le LFITM publie, au minimum, les contenus suivants sur son site Web :

a. Informations de contact.
b. Services fournis par le LFITM.
c. Tarifs, y compris les frais de transport et les frais pour les activités optionnelles.
d. Rapports d'inspection.
e. Données agrégées de la réussite des élèves ou de leurs réalisations individuelles (par exemple, récompenses), avec consentement.
f. Versions publiques du rapport annuel, conformément à la politique de rapport des écoles d'ADEK.
g. Politiques du LFITM qui sont pertinentes pour les parents et/ou les élèves.
h. Tout autre contenu requis, tel que défini par les politiques d'ADEK.

Le LFITM s'assure que le contenu publié sur son site Web est exact et approprié, conformément à la politique des valeurs et de l'éthique des écoles d'ADEK.
Le LFITM garantit également que le contenu publié sur son site Web respecte les exigences en matière de médias numériques (voir la section 9.1 sur la Politique relative aux médias numériques).

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