EVEREST SCHOOL

EV-S.1824
Online Safety and Acceptable Use

Policy

December 2024

EVEREST
SCHOOL

Table contents

1. Introduction et Objectifs
2. Principes fondamentaux de la politique
3. Responsabilités des élèves et des parents
4. Education and Curriculum
5. Comportement attendu et gestion des incidents
6. Mesures de suivi et de sanction
7. Communication et implication des parents
8. Réseaux sociaux et surveillance
9. Equipements et contenu numérique

1. Introduction et Objectifs

L'Online Safety and Acceptable Use Policy (Politique de sécurité en ligne et d'utilisation acceptable) est un cadre essentiel pour garantir un environnement numérique sûr et responsable au sein de notre école. Cette politique vise à encadrer l'utilisation des technologies numériques par tous les membres de la communauté scolaire, incluant les élèves, le personnel, les parents, et les visiteurs, afin de protéger la sécurité et le bien-être de chacun. Elle définit les attentes en matière de comportement en ligne, s'assurant que les technologies soient utilisées de manière appropriée pour des fins éducatives tout en réduisant les risques associés aux abus en ligne tels que le cyberharcèlement, l'exploitation en ligne, et l'accès à des contenus inappropriés. Cette politique s'inscrit dans un engagement global à créer un environnement d'apprentissage où la sécurité numérique est prioritaire, en sensibilisant la communauté scolaire à l'importance de naviguer de manière responsable et respectueuse sur Internet. Elle inclut également des mesures disciplinaires pour toute violation des règles, garantissant ainsi une gestion proactive des risques liés à la sécurité en ligne.

Raisons d'être : La politique vise à définir des principes de sécurité numérique pour la communauté scolaire, protéger les enfants et le personnel, assurer une utilisation sûre et responsable d'internet, et mettre en place des structures pour traiter les abus en ligne.

Risques identifiés : Exposition à des contenus inappropriés, comportements dangereux en ligne, harcèlement, vol d'identité, problèmes de confidentialité, comportements agressifs, et risques liés à l'apprentissage à distance

a. Objectifs de la politique

- Sécuriser l'environnement numérique : Protéger les élèves des risques associés à Internet, notamment l'exposition à des contenus inappropriés, le cyberharcèlement, la fraude en ligne et les contacts dangereux.
- Favoriser un usage éducatif : Encourager les élèves à utiliser Internet et les technologies de manière constructive, en soutenant leur apprentissage, la recherche scolaire, et la collaboration.
- Responsabiliser les élèves : Enseigner aux enfants les bonnes pratiques en ligne et l'importance du respect de la vie privée et des autres utilisateurs.
- Informer et impliquer les parents : Assurer que les parents comprennent les risques numériques et qu'ils participent activement à la gestion de l'utilisation d'Internet à la maison.

b. Portée de la Politique

Cette politique s'applique à tous les membres de la communauté scolaire, incluant le personnel, les élèves, les parents, et les groupes externes, tant à l'intérieur qu'à l'extérieur de l'école, y compris durant le télétravail ou l'enseignement à distance.

c. Rôles et Responsabilités

- Chef d'établissement : Responsable de la sécurité en ligne, du filtrage Internet, et de la formation du personnel.
- Responsable de la sécurité en ligne (DSL) : Supervise la sécurité en ligne au quotidien, assure l'intégration de la sécurité dans le programme scolaire, et collabore avec le personnel technique.

- Gouverneurs et autres responsables : Assurent la conformité des pratiques de sécurité et approuvent la politique.
- Enseignants : Intègrent la sécurité en ligne dans l'enseignement et supervisent l'utilisation des technologies par les élèves.
- Tous les membres du personnel : Doivent signer et respecter l'Accord d'Utilisation Acceptable (AUP), être formés, et signaler tout abus.

d. Gestion des plaintes et incidents

- Plainte : Tout abus en ligne ou mauvais usage doit être signalé au coordinateur de la sécurité en ligne. Des mesures disciplinaires ou légales peuvent être prises.
- Sexting : Une procédure est établie pour gérer les incidents de partage d'images inappropriées, avec des critères spécifiques pour impliquer la police ou les services sociaux.

e. Communication et Sensibilisation

- La politique est communiquée via le site de l'école, des réunions, et des formations régulières.
- Des accords d'utilisation sont signés par le personnel, les élèves, et les parents.

f. Révision et Suivi

- La politique doit être révisée en relation avec les politiques de comportement et de protection de l'enfance pour assurer une approche cohérente de la sécurité en ligne.

2. Principes fondamentaux

L'usage des technologies numériques dans les écoles présente des avantages considérables pour l'apprentissage des élèves, mais il comporte également des risques qui nécessitent une gestion rigoureuse. La politique de sécurité en ligne et d'utilisation acceptable vise à établir des principes clairs pour garantir que l'utilisation d'Internet et des appareils numériques soit sécurisée, responsable et respectueuse. Ce texte présente les principes fondamentaux de cette politique, notamment l'accès sécurisé aux technologies, la protection de la vie privée, le comportement en ligne respectueux, ainsi que les responsabilités des élèves et des parents pour assurer un environnement numérique sûr et éducatif.

1. **Accès sécurisé et contrôlé**

   Les élèves doivent utiliser les appareils numériques uniquement pour des activités scolaires. L'accès à des sites non autorisés est interdit, et l'Internet à l'école est filtré pour bloquer les contenus inappropriés. Les activités en ligne sont surveillées par les enseignants pour garantir la conformité.

2. **Confidentialité et sécurité des données**

   Les élèves doivent éviter de partager des informations personnelles en ligne. Ils doivent créer des mots de passe sécurisés, avec l'aide des enseignants si nécessaire, pour protéger leurs comptes en ligne.

3. **Comportement en ligne responsable et respectueux**

Les élèves doivent traiter les autres avec respect en ligne et éviter tout comportement nuisible comme la cyberintimidation. Le partage de contenu inapproprié est interdit, et l'utilisation des technologies doit être bienveillante.

4. **Éducation à la sécurité en ligne**

Des leçons sur la sécurité numérique seront organisées, abordant des sujets comme la protection des données et les risques des réseaux sociaux. Les élèves doivent être informés des dangers en ligne, tels que les arnaques et la cyberintimidation.

5. **Utilisation de l'Internet à des fins éducatives**

L'Internet doit être utilisé pour des activités scolaires, comme la recherche et la communication avec les enseignants. L'école met à disposition des applications éducatives pour soutenir l'apprentissage des élèves.

3. Responsabilités des élèves et des parents

a. Responsabilités des élèves

Les élèves ont un rôle essentiel dans le respect des règles d'utilisation des technologies établies par l'école. Cela implique qu'ils doivent utiliser les dispositifs numériques uniquement à des fins éducatives et dans le cadre des activités scolaires, en respectant les consignes définies par leurs enseignants. Il est également important que les élèves soient vigilants en ligne et signalent immédiatement toute activité suspecte ou inappropriée à un adulte de confiance. En ce qui concerne l'utilisation d'Internet, les élèves doivent suivre scrupuleusement les instructions des enseignants, que ce soit pour les recherches, l'utilisation d'applications éducatives ou la gestion de leur comportement en ligne. L'objectif est de garantir un environnement numérique sécurisé et propice à l'apprentissage.

b. Responsabilités des parents

Les parents jouent un rôle crucial dans la gestion de l'utilisation des technologies à la maison. Ils doivent surveiller activement l'accès de leurs enfants à Internet pour s'assurer qu'ils n'entrent pas en contact avec des contenus inappropriés. Cette supervision nécessite une vigilance constante et la mise en place de règles claires concernant l'utilisation des appareils numériques à la maison. De plus, les parents doivent entretenir des conversations régulières avec leurs enfants pour les sensibiliser aux dangers d'Internet. Ils sont encouragés à discuter des risques associés à la cyberintimidation, aux interactions avec des inconnus en ligne et à la divulgation d'informations personnelles. Par ailleurs, les parents doivent utiliser des outils de contrôle parental pour restreindre l'accès à certains contenus et gérer les applications utilisées par leurs enfants. Cela permet de renforcer la sécurité numérique et d'assurer un cadre de confiance pour l'utilisation d'Internet.

4. Éducation et Curriculum

a. Éducation et sensibilisation des élèves :

Everest School (EV-S) intègrent des programmes éducatifs progressifs dans le curriculum, couvrant les compétences et comportements adaptés à chaque tranche d'âge. Les élèves apprennent à :

- Naviguer prudemment en ligne, en évaluant les informations et en reconnaissant les biais des contenus.

- Adopter des comportements respectueux en ligne, protéger leurs données personnelles et activer les paramètres de confidentialité.
- Comprendre les risques associés aux relations en ligne et l'importance de ne pas partager de détails personnels ou de publier sans autorisation.
- Gérer les contenus inappropriés, signaler les abus, et demander de l'aide en cas de cyberharcèlement ou d'autres formes de harcèlement en ligne.
- Respecter les droits d'auteur et éviter le plagiat en utilisant uniquement des plateformes approuvées par l'école dans des environnements sécurisés.

b. Formation du personnel et des gouverneurs :

Le personnel reçoit des formations régulières pour comprendre et appliquer les principes de sécurité en ligne, incluant :

- La gestion sécurisée des données sensibles grâce au chiffrement.
- La modélisation de comportements responsables dans l'usage des technologies en classe.
- La sensibilisation aux enjeux de la propriété intellectuelle et de l'utilisation commerciale d'Internet.
  Des informations sur les politiques de sécurité numérique sont également fournies aux nouveaux membres du personnel lors de leur intégration.

c. Sensibilisation des parents :

Les parents bénéficient d'un accompagnement régulier pour renforcer la sécurité numérique à la maison grâce à :

- Des sessions d'intégration présentant les principes de comportement en ligne sûr.
- Des brochures, newsletters, et informations sur les sites de soutien nationaux.
- Un programme continu d'ateliers et de conseils sur la sécurité en ligne pour les aider à superviser et guider l'usage des technologies par leurs enfants.

Ce programme vise à créer un environnement numérique sûr et responsable, impliquant élèves, personnel, et parents dans une approche collaborative et éducative.

5. Comportement attendu et gestion des incidents

Comportement attendu

A Everest School, tous les utilisateurs :

- Responsabilité et conformité : Doivent utiliser les systèmes informatiques et de communication de l'école en respectant la politique en vigueur ainsi que le programme et le calendrier établis par l'établissement.
- Conscience des conséquences : Doivent comprendre les risques liés à l'utilisation abusive ou l'accès à des contenus inappropriés, ainsi que les conséquences qui en découlent.
- Signalement : Ont la responsabilité de signaler tout abus, utilisation abusive ou accès à des contenus inappropriés, et de savoir comment le faire.

- Pratiques en ligne sûres : Devraient adopter des pratiques sûres en ligne, que ce soit dans ou hors de l'école, et comprendre que la politique s'étend aux activités liées à leur appartenance à l'école.
- Conformité aux politiques : Doivent se familiariser avec les politiques de l'école sur l'utilisation des téléphones, appareils numériques, et la gestion des images, ainsi que sur le cyberharcèlement.

Rôles spécifiques :

- Personnel : Lit et applique la politique de sécurité en ligne, y compris les règles d'utilisation des appareils mobiles et portables, et veille à une supervision adéquate des élèves.
- Élèves : Développent des compétences en recherche, évitent le plagiat, et respectent les droits d'auteur.
- Parents/tuteurs : Donnent leur consentement pour l'utilisation des technologies par les élèves et s'assurent de comprendre les règles et sanctions liées à leur usage inapproprié.

Gestion des incidents

Dans Everest School :

- Surveillance stricte : La politique de sécurité en ligne est appliquée rigoureusement, avec des sanctions différenciées et adaptées. Les comportements positifs des utilisateurs minimisent cependant le recours aux sanctions.
- Signalement : Tous les membres de la communauté sont encouragés à signaler tout problème en ligne, en ayant l'assurance que les incidents seront traités rapidement et avec sensibilité.
- Suivi des incidents : Les incidents sont surveillés, documentés et analysés pour contribuer à l'amélioration des politiques et pratiques. Les rapports sont partagés avec les responsables de l'école, les gouverneurs et les autorités locales.
- Information des parties concernées : Les parents sont informés des incidents impliquant leurs enfants.

6. Mesures de suivi et de sanction

Afin d'assurer un usage responsable et sécurisé des technologies numériques au sein de l'école, des mesures de suivi et des mécanismes disciplinaires ont été établis. Ces dispositions visent à prévenir les comportements inappropriés, à détecter rapidement toute infraction et à appliquer des sanctions proportionnées, tout en impliquant les parents dans le processus éducatif. L'objectif est de promouvoir un environnement numérique où les élèves peuvent évoluer de manière sécurisée, tout en étant responsabilisés face à leurs actions en ligne. Les sections suivantes décrivent en détail les modalités de suivi des activités numériques et les mesures à prendre en cas de non-respect des règles.

6.1 Suivi des activités en ligne

- Surveillance proactive : L'école utilise des outils et des systèmes appropriés pour surveiller l'utilisation des appareils numériques par les élèves, tout en veillant à respecter les droits à la vie privée. Ces mesures permettent d'identifier rapidement tout usage inapproprié ou non conforme.

- Identification et alerte : En cas de détection d'un comportement problématique, comme le cyberharcèlement, la consultation de contenu inapproprié ou la violation des règles, une alerte est émise. Les enseignants et le personnel concerné sont tenus de mener une enquête approfondie pour évaluer la situation et déterminer les mesures correctives nécessaires.
- Documentation des incidents : Les activités en ligne problématiques sont enregistrées dans un rapport détaillé pour assurer un suivi rigoureux et permettre des ajustements futurs des politiques ou des outils de surveillance si nécessaire.

6.2 Sanctions en cas de non-respect de la politique

- Avertissements progressifs : Lorsqu'un élève enfreint les règles pour la première fois ou pour des infractions mineures, un avertissement verbal ou écrit est émis, accompagné d'une explication des conséquences potentielles en cas de récidive.
- Suspension temporaire des privilèges : En cas de récidive ou de comportement plus grave, l'accès aux ressources numériques peut être temporairement restreint, empêchant l'élève d'utiliser certains outils ou plateformes.
- Sanctions disciplinaires : Pour les infractions sérieuses, telles que la diffusion intentionnelle de contenu nuisible ou la mise en danger d'autres élèves, des mesures disciplinaires plus strictes, allant de la retenue à l'exclusion temporaire, peuvent être appliquées conformément au règlement intérieur.

6.3 Rôle des parents dans le processus disciplinaire

- Notification des parents : Les parents sont informés rapidement de tout incident grave impliquant leur enfant. Une communication claire est établie pour expliquer les faits, les conséquences et les mesures prises par l'école.
- Réunions de concertation : Si nécessaire, une réunion est organisée avec les parents, les enseignants et éventuellement l'élève pour discuter des causes de l'incident et convenir d'un plan d'action visant à corriger le comportement et éviter toute récidive.
- Implication dans les solutions : Les parents sont encouragés à jouer un rôle actif en renforçant les règles d'utilisation des technologies à domicile et en participant à l'élaboration de solutions éducatives ou comportementales pour leur enfant.

7. Communication et implication des parents

Dans un monde où les technologies numériques occupent une place centrale dans l'éducation et la vie quotidienne, il est essentiel d'assurer une collaboration étroite entre l'école et les parents pour promouvoir une utilisation sûre et responsable des outils numériques. Les parents jouent un rôle crucial dans l'accompagnement de leurs enfants, tant à l'école qu'à la maison, en veillant à ce que les pratiques numériques respectent les règles de sécurité et d'éthique.

Pour renforcer ce partenariat, l'école a mis en place des mécanismes de communication efficaces et des initiatives spécifiques visant à informer, responsabiliser et engager activement les parents dans cette démarche éducative. Ces mesures contribuent à construire un environnement numérique harmonieux et sécurisé, propice à l'apprentissage et au développement des élèves.

L'école considère les parents comme des partenaires essentiels dans la promotion d'un usage sûr et responsable des technologies numériques par les élèves. Pour garantir une approche collaborative et cohérente, plusieurs initiatives et mécanismes de communication sont mis en place :

7.1 Contrat d'utilisation acceptable

- Engagement formel : Un contrat d'utilisation acceptable est remis aux parents et aux élèves au début de l'année scolaire. Ce document détaille les règles d'utilisation des technologies numériques à l'école, ainsi que les comportements attendus.
- Signature conjointe : La signature de ce contrat par les parents et les élèves représente un engagement mutuel à respecter les politiques en vigueur. Ce processus permet également de sensibiliser les parents aux responsabilités numériques de leurs enfants.
- Suivi et renouvellement : Ce contrat est révisé périodiquement pour inclure les évolutions technologiques et réglementaires. Les parents sont informés de ces mises à jour et invités à renouveler leur engagement.

7.2 Ateliers et réunions d'information

- Ateliers pratiques : L'école propose régulièrement des ateliers interactifs pour les parents, animés par des experts en cybersécurité et des enseignants. Ces ateliers couvrent des sujets tels que :
  - ✓ Les risques associés aux réseaux sociaux.
  - ✓ L'installation et l'utilisation d'outils de contrôle parental.
  - ✓ La gestion du temps d'écran et des habitudes numériques à la maison.
- Réunions d'information : Des sessions sont organisées pour informer les parents des politiques de l'école, des tendances actuelles en matière de sécurité numérique et des mesures mises en place pour protéger les élèves en ligne.
- Guides et ressources : Des guides pratiques, fiches conseils et liens vers des plateformes éducatives fiables sont régulièrement distribués via des newsletters ou le site Internet de l'école. Ces documents permettent aux parents de rester informés et équipés pour accompagner leurs enfants dans leur usage numérique.

7.3 Dialogue continu avec les parents

- Échanges réguliers : L'école maintient une communication ouverte avec les parents, par le biais de réunions individuelles, de plateformes numériques ou d'événements communautaires, pour discuter des préoccupations ou des incidents liés à la sécurité en ligne.
- Retour d'expérience : Les parents sont invités à partager leurs expériences ou suggestions pour améliorer les pratiques de l'école en matière de sécurité numérique, renforçant ainsi leur implication active.

Grâce à ces initiatives, l'école vise à établir une collaboration solide avec les parents pour garantir un environnement numérique sûr et enrichissant pour les élèves, tant à l'école qu'à la maison.

8. Réseaux sociaux et surveillance

a. Personnel, bénévoles et contractuels

- Séparation des communications : Le personnel est tenu de maintenir une distinction stricte entre les communications professionnelles et personnelles pour garantir un cadre professionnel, préserver la confidentialité et protéger la réputation de l'école.
- Utilisation des réseaux sociaux : Les enseignants ne doivent pas créer ni utiliser d'espaces personnels pour interagir avec les élèves ou leurs parents. *Les communications se font via les* plateformes *Kinderpedia*, conformément à la politique de communication.
- Bonnes pratiques :
  - ✓ Aucune mention d'élèves, parents ou collègues sur des réseaux sociaux privés.
  - ✓ Pas de connexion amicale en ligne avec les élèves ou leurs parents sans approbation de la direction.
  - ✓ Pas de participation à des discussions en ligne concernant des membres de la communauté scolaire.
  - ✓ Opinions personnelles et comportement en ligne ne doivent pas compromettre la réputation ou les valeurs de l'école.
  - ✓ Les paramètres de confidentialité des profils personnels doivent être régulièrement vérifiés.

b. Élèves

- Formation et accords : Les élèves reçoivent une éducation sur l'utilisation responsable des réseaux sociaux.

c. Parents

- Sensibilisation : Les parents sont sensibilisés aux risques liés aux réseaux sociaux à travers Kinderpedia et lors des réunions. Ils doivent obtenir l'autorisation préalable de la direction de l'école avant de publier tout contenu impliquant l'établissement ou son personnel.

9. Équipement et contenu numérique

L'école applique des règles strictes pour l'utilisation des téléphones mobiles et appareils numériques personnels afin de protéger la vie privée, garantir un environnement éducatif sûr et respecter les protocoles de sécurité.

Téléphones et appareils mobiles personnels

- Responsabilité : Les téléphones mobiles apportés à l'école sont sous la responsabilité de leur propriétaire ; et sont interdits pour les élèves de primaire et maternelle. L'école décline toute responsabilité en cas de perte, vol ou dommage.
- Utilisation des appareils par les élèves :
  - ✓ Appareils remis à l'administration à l'arrivée et récupérés à la fin de la journée.
- Utilisation des appareils par le personnel :

- ✓ Interdiction d'utiliser des téléphones personnels pour contacter des élèves ou leurs familles.
- ✓ Téléphones éteints ou en mode silencieux pendant les cours, sauf autorisation exceptionnelle ou activités scolaires.

Images et vidéos numériques

- Photographies et vidéos des élèves :
  - ✓ Autorisation parentale obligatoire pour l'utilisation d'images ou vidéos d'élèves.
  - ✓ Aucune identification d'élèves dans les publications en ligne ou supports de l'école sans consentement explicite.
- Éducation des élèves :
  - ✓ Formation sur les risques liés à la publication d'images en ligne et l'importance des paramètres de confidentialité.
  - ✓ Enseignement sur les dangers de la diffusion d'informations personnelles avec des images et sur les démarches à suivre en cas d'abus.

Ces mesures visent à maintenir un environnement numérique sûr et respectueux, tout en protégeant les informations personnelles et la confidentialité des élèves, du personnel et des familles.