GUIDE - CONSEILS ET OUTILS

UN MODÈLE À L'ÈRE DU NUMÉRIQUE

POUR LE PERSONNEL ENSEIGNANT

BEE SECURE

TABLE DES MATIÈRES

INTRODUCTION 3

1. LES LIGNES DE CONDUITE DANS LE CONTEXTE SCOLAIRE **4**
1.1 Le droit à l'image : partage des images des élèves 4
1.2 RGPD : sauvegarde et partage de données ou de photos 6
1.3 Utilisation d'œuvres de tierces personnes : droits d'auteur (Copyright ©) 8
1.4 Règles pour l'utilisation des écrans par les enfants : apprendre en sécurité 10

2. CONFIGURATION ET PROTECTION DES OUTILS **12**
2.1 Sécuriser les appareils électroniques 12
2.2 Confidentialité et protection de la vie privée 16

3. UTILISATION DES RÉSEAUX SOCIAUX **19**
3.1 Représentation de soi en ligne 19
3.2 La classe sur les réseaux sociaux 21
3.3 Risque : piratage et usurpation d'identité 22

4. PRÉVENTION ET INTERVENTION EN CAS D'INCIDENT **24**
4.1 Prévention 24
4.2 Intervention en cas de situation d'incident 26
4.3 Les limites de votre responsabilité 31

BIBLIOGRAPHIE 34

Afin d'alléger la lecture de la présente publication, la forme masculine a été employée comme genre neutre pour désigner toute la population.

INTRODUCTION

À l'ère du numérique, les technologies connectées occupent une place centrale dans la vie quotidienne des élèves et du personnel enseignant. Ces outils offrent d'immenses possibilités pédagogiques, mais soulèvent aussi de nouveaux défis éthiques, légaux et éducatifs. Dans un environnement où les frontières entre vie privée et vie professionnelle s'estompent, il est essentiel pour le personnel enseignant de connaître les bonnes pratiques afin de garantir la sécurité, la protection et le bien-être de tous les acteurs de la communauté scolaire.

Ce guide a été conçu comme un outil pratique et concret pour accompagner le personnel enseignant dans son rôle de modèle à l'ère du numérique. Il propose des conseils, des repères légaux et des recommandations issues des ressources officielles, afin de faciliter la mise en place de comportements responsables et sécurisés, tant dans l'usage personnel que professionnel des outils numériques. Son objectif est d'aider chaque enseignant à adopter des réflexes de prévention et à savoir comment réagir face aux situations problématiques.

L'organisation de cette publication débute par les lignes de conduite à adopter dans le contexte scolaire, puis aborde la configuration et la sécurisation des outils numériques, avant de traiter de l'utilisation des réseaux sociaux. La quatrième partie est consacrée à la prévention et à la gestion des incidents, afin de fournir des repères concrets d'intervention et des ressources utiles. Le guide est complété par des petits mémos pour le personnel enseignant (post-its), une checklist pour l'utilisation des réseaux sociaux et des annexes, par exemple un modèle d'une charte de bonne conduite.

Ensemble, ce guide et les outils qui l'accompagnent visent à soutenir le personnel enseignant dans sa mission éducative et à promouvoir un usage réfléchi, sûr et responsable du numérique à l'école.

1. LES LIGNES DE CONDUITE DANS LE CONTEXTE SCOLAIRE

Les appareils numériques font partie de la vie quotidienne, pour les enseignants comme pour les élèves. Pour assurer l'intégrité et le bien-être de toutes et tous, il est important de connaître et de respecter certaines lignes de conduite.

1.1 Le droit à l'image : partage des images des élèves

Dans le contexte scolaire

La prise de photos ou de vidéos a bien sa place dans la vie scolaire, par exemple pour créer des souvenirs de visites ou documenter des projets. En même temps, toute personne a le droit de s'opposer à la prise et à la publication de son image, y inclus les enfants. Pour le personnel enseignant, il s'agit donc de trouver un juste équilibre entre la documentation et le respect du droit à l'image et de la vie privée des élèves.

D'un point de vue légal

Le droit à l'image repose sur différentes lois relatives à la **protection de la vie privée**[1] (p.35), au niveau européen et national : il est interdit de « *fixer par un appareil quelconque les images d'une personne se trouvant dans un lieu non accessible au public, sans le consentement de celle-ci* » (loi du 11 août 1982 concernant la protection de la vie privée). Ce consentement peut être retiré à tout moment. La violation de ces dispositions peut faire l'objet de poursuites pénales et civiles sérieuses.

IMPORTANT

Accepter d'être photographié ne veut pas dire autoriser la diffusion de la photographie !

Le **consentement des mineurs** en matière de droit à l'image implique plusieurs considérations légales et éthiques. Les enfants ne peuvent conclure de contrat juridiquement contraignant (article 1124 du Code civil) avant l'âge de 18 ans. Ce sont donc leurs représentants légaux qui doivent donner le consentement à leur place. À partir de 13 ans, il est toutefois conseillé de prendre en compte l'avis des enfants. On assume que les enfants ont alors atteint l'âge de discernement, c'est-à-dire qu'ils sont capables de comprendre la nature et les conséquences de leurs actions, comme le consentement à l'utilisation de leur image.

DROITS DES ENFANTS

Le « **droit aux droits** » des enfants est inscrit dans la constitution luxembourgeoise en vigueur depuis juillet 2023. La participation des enfants fait donc partie des principes fondamentaux de la société luxembourgeoise.

La Convention internationale des droits de l'enfants (CIDE ou Convention relative aux droits de l'enfant) énonce les droits fondamentaux des enfants. En tant que signataire, le Luxembourg s'est engagé à respecter ces droits. L'article 16 de la CIDE garantit le respect de la vie privée des enfants et l'article 17 leur droit à l'information et à la participation.

Recommandations

Afin de respecter les consignes relatives au droit à l'image et d'apprendre les bons réflexes aux enfants autour de la prise de photo ou de vidéos :

- **demandez l'accord écrit explicite** des représentants légaux avant de prendre ou publier des images des élèves. BEE SECURE met à disposition un modèle pour une autorisation parentale en annexe qui peut être utilisé et adapté selon vos besoins ;
- **thématisez le droit à l'image** et le consentement avec les enfants et les parents ;
- **expliquez aux enfants pourquoi vous prenez des photos** et demandez leur accord avant de prendre des clichés pour leur apprendre le réflexe. Veillez au fait qu'une autorisation à la prise de photo n'est pas automatiquement une autorisation à sa publication ;
- s'il n'y pas d'accord, **une solution est de rendre floues les images** pour que les enfants ne soient pas identifiables.

EN BREF

- Demandez un consentement par écrit aux représentants légaux.
- Demandez toujours l'accord pour prendre des photos afin d'apprendre ce réflexe aux élèves.
- Expliquez aux enfants pourquoi vous désirez les prendre en photo et ce que vous ferez des photos.

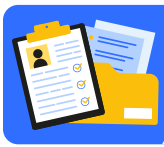
1.2 RGPD : sauvegarde et partage de données ou de photos dans le contexte scolaire

Dans le contexte scolaire

En tant qu'enseignant, vous avez accès à de nombreuses informations personnelles sur les élèves et leurs parents, comme des informations sur des allergies des enfants, les données de contact des parents ou les noms et adresses des élèves. Pour garantir la protection de ces données, il est important d'adopter des gestes responsables pour leur sauvegarde et leur partage.

D'un point de vue légal

La sauvegarde et le partage de données ou de photos sont régis par le règlement général sur la protection des données (RGPD) qui s'applique à tous les acteurs sur le territoire européen depuis 2018. Tout traitement de données à caractère personnel doit répondre à **6 grands principes** :



1. Ne collecter **que les données vraiment nécessaires** pour atteindre un objectif précis.

2. Définir **les objectifs de manière précise** avant le traitement de données.

3. **Être transparent** sur la façon dont les données ou les images sont traitées.

4. Mettre en place des procédures pour permettre aux concernés **d'accéder, de rectifier ou de supprimer leurs données.**

5. **Fixer des limites** de conservation pour les données ou images.

6. **Sécuriser les données** et les **protéger** contre le traitement non autorisé.

Recommandations

En intégrant les principes du RGPD dans votre pratique quotidienne, vous pouvez contribuer à protéger les données personnelles des élèves et de leurs représentants légaux et à créer un environnement scolaire respectueux de la vie privée. Pour une gestion sécurisée de données, il s'agit surtout de savoir où elles sont stockées et de ne les transférer que par des canaux sécurisés.

Des données stockées dans certains services cloud comme Dropbox ou des services de messagerie comme *WhatsApp* pourraient atterrir sur des serveurs externes ne fournissant aucune garantie de sécurité et de transparence.

Voilà pourquoi il est recommandé :

- **d'utiliser des supports de stockage physiques** et des serveurs locaux pour sauvegarder les données ou photos ;
- d'éviter **d'envoyer des données ou photos par e-mail** ou de les partager dans des clouds ou des groupes de chat ;
- d'informer les représentants légaux sur **la sauvegarde et le traitement de données et d'images** de leur enfant ;
- de développer **une démarche pour revoir et supprimer systématiquement les données qui ne sont plus nécessaires**, par exemple à la fin du trimestre ou de l'année scolaire.

EN BREF

- Soyez précis et transparent sur la sauvegarde et le partage de photos et de documents.
- Supprimez les photos ou données dès que vous n'en avez plus besoin.
- Sauvegardez les données sur des supports dont vous contrôlez l'accès.
- Utilisez des canaux de transfert sécurisés (rubrique 2.1 Sécuriser les appareils électroniques).

1.3 Utilisation d'œuvres de tierces personnes : droits d'auteur (Copyright ©)

Dans le contexte scolaire

En tant qu'enseignant, il se peut que vous ayez besoin de matériel pédagogique en plus des supports prévus par le Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse (MENJE). Les images, vidéos et textes utilisés pour illustrer ou approfondir un sujet constituent des outils essentiels pour concevoir des cours actuels et adaptés pour les élèves. Il est toutefois important de savoir comment se procurer du matériel de manière licite et en respectant les droits d'auteur.

D'un point de vue légal : exception pour utilisation pédagogique et licences

Les **droits d'auteur**, en anglais « *copyright* », appartiennent à la famille des droits de la propriété intellectuelle. Ils protègent les œuvres littéraires et artistiques dès leur création, sans nécessiter de formalités d'enregistrement. Ils confèrent à l'auteur le droit exclusif d'exploiter son œuvre et d'en tirer un profit financier et protègent donc une œuvre du partage, de la reproduction et de la vente non autorisée par des tiers.

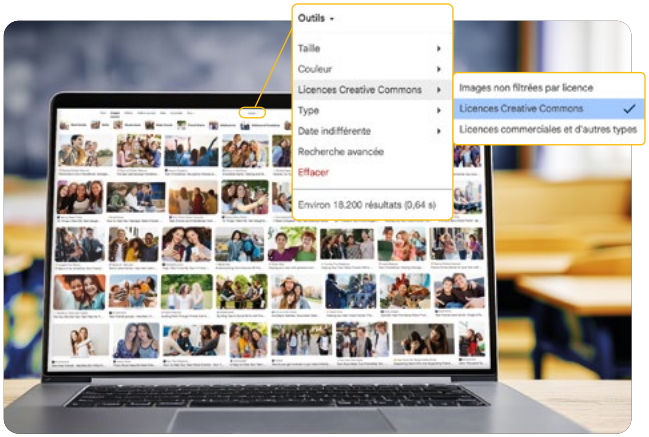
Exception pour utilisation pédagogique : au Luxembourg, l'article 10 de la loi sur les droits d'auteur prévoit une exception pour l'utilisation pédagogique des œuvres. Selon cette exception, il est autorisé de copier des extraits d'œuvres protégées par le droit d'auteur sans demander une autorisation tant que la source est citée.

Domaine public : une œuvre fait partie du domaine public lorsqu'elle n'est pas protégée par un droit de protection intellectuelle ou lorsque cette protection a expiré. Ces œuvres peuvent être librement utilisées sans aucune autorisation.

Creative Commons : les œuvres sous licence « Creative Commons » peuvent être utilisées gratuitement. L'auteur de l'œuvre peut toutefois choisir les conditions sous lesquelles il la met à disposition. Par conséquent, il y a différentes variantes de ce type de licence : faut-il mentionner l'auteur ? A-t-on le droit de modifier ou d'adapter l'œuvre ?

Recommandations

- Il est conseillé de toujours indiquer les sources que vous avez utilisées comme support ou inspiration pour des raisons déontologiques et de transparence (par exemple en bas des copies ou des diapositives *Powerpoint*).
- Favorisez les ressources du domaine public et « *Creative Commons* » : ajoutez « *free to use* » à votre terme de recherche ou utilisez des filtres pour afficher seulement les images sous une licence « *Creative Commons* ».



LES DROITS D'AUTEUR ET L'INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA) bouscule les règles précédentes de la création et par extension celles des droits d'auteur : l'IA peut générer des œuvres de façon autonome, mais sont-elles à traiter comme des œuvres de créateurs humains ? Dans un sens restreint : non, il faut un créateur humain pour avoir un droit d'auteur. La question se complique quand l'IA est utilisée comme assistante à la création. Un autre point critique en matière de conciliation entre droit d'auteur et IA sont les données utilisées pour entraîner les modèles d'IA. Certaines de ces données peuvent effectivement, selon l'outil IA, inclure des oeuvres protégées par le droit d'auteur, qui sont cependant utilisées sans l'accord de l'auteur.

Jusqu'à nouvel ordre, BEE SECURE souligne que la transparence est indispensable. En plus d'apprendre les bons gestes aux élèves, vous évitez ainsi des revendications abusives de droits d'auteurs et contribuez en même temps à protéger la rémunération des artistes face aux créations générées par l'ordinateur. Servez-vous des outils d'IA recommandés sur le site du KI Kompass.

Montrez le bon exemple : indiquez si vous utilisez IA.

EN BREF

- Assurez-vous que vous avez le droit d'utiliser l'image ou autre œuvre et que vous citez adéquatement l'auteur.
- Thématisez les droits d'auteurs avec les élèves et expliquez comment éviter le plagiat.
- Indiquez si une intelligence artificielle a été utilisée pour créer un contenu.

1.4 Règles pour l'utilisation des écrans par les enfants : apprendre en sécurité

Dans le contexte scolaire

Les médias numériques présentent de nouvelles possibilités d'apprentissage, mais aussi de nouveaux défis. Une utilisation excessive des écrans comporte divers risques comme, entre autres, une influence sur le sommeil, une contribution au surpoids. Il s'agit d'apprendre aux enfants un usage responsable et éclairé des médias numériques tout en les protégeant de leurs effets néfastes.

D'un point de vue légal : interdiction des smartphones à l'école

L'utilisation de smartphones et autres appareils connectés est interdit dans toute l'enceinte des écoles fondamentales et des maisons relais depuis 2025. Cette décision du Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse avait été prise dans le but de réduire le temps passé devant les écrans et d'encourager l'exploration d'activités analogiques.

Les appareils connectés peuvent toujours être utilisés à des fins pédagogiques, sous la surveillance des enseignants. Des exceptions sont faites pour répondre à des besoins médicaux des enfants sur présentation d'un certificat médical.

Recommandations

Les compétences et les capacités pour utiliser des appareils connectés et absorber des contenus numériques ne sont pas innées. Les enfants les apprennent au cours de leur développement. La **règle 3-6-9-12** proposée par Serge Tisseron, psychiatre et psychanalyste, donne une ligne de conduite quant à l'utilisation des écrans en fonction de l'âge de l'enfant.

ACCOMPAGNER L'USAGE DES OUTILS NUMÉRIQUES

À l'entrée au cycle 2 de l'école fondamentale, les enfants ont besoin d'accompagnement lors de l'utilisation d'appareils numériques. Avec le temps, ils gagnent en indépendance et maîtrisent mieux leur environnement immédiat.

9 à 12 ans

APPRENEZ-LEUR LES RISQUES SUR INTERNET

À cet âge, les élèves sont plus aptes à agir de façon autonome et à choisir leurs activités, mais ils n'ont pas encore la maturité nécessaire pour évaluer seuls les dangers du web. C'est le moment opportun de leur expliquer que tout ce qui est mis en ligne peut être vu par tout le monde et que, même effacée, une information ou une photo peut continuer à circuler. Sensibilisez aussi les enfants aux fausses informations : **ce n'est pas parce que c'est écrit que c'est vrai !**

EN BREF

- Interdiction de smartphones à l'école depuis avril 2025.
- Adaptez l'usage des outils numériques à l'âge des enfants (règle 3-6-9-12).
- Planifiez et préparez des activités numériques encadrées afin d'en maximiser les avantages didactiques.
- Planifiez des activités analogiques (erliewen.snj.lu).

2. CONFIGURATION ET PROTECTION DES OUTILS

Afin de guider et d'inspirer les élèves, les enseignants sont censés incarner les valeurs et les comportements qu'ils cherchent à inculquer aux élèves. Conscients de l'impact profond de leur influence, les enseignants doivent, eux aussi, savoir comment configurer et utiliser leurs appareils électroniques de manière sécurisée en classe.

2.1 Sécuriser les appareils électroniques

Séparer les appareils électroniques privés et professionnels

L'utilisation d'appareils privés et de services comme *WhatsApp* peut sembler pratique pour organiser le quotidien à l'école. Cette utilisation présente cependant des risques quant à la protection des données du personnel enseignant et des élèves. Il est donc fortement recommandé de ne pas utiliser des appareils privés connectés, comme des smartphones, tablettes ou ordinateurs, dans le contexte scolaire et de n'utiliser que les services recommandés par le Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse (voir point suivant).

Utiliser les services recommandés par les instances compétentes

Les établissements scolaires mettent souvent en place des systèmes et des logiciels spécifiques pour gérer les ressources pédagogiques, communiquer avec les élèves et les parents et suivre les progrès des élèves. Les outils professionnels viennent avec des paramètres déjà configurés pour assurer un maximum de sécurité. Ces systèmes ont aussi l'avantage de réduire le risque de distraction (pas d'accès à des réseaux sociaux ou jeux).

Des exemples de services et logiciels actuellement recommandés et mis à disposition par le Ministère de l'Éducation nationale, de la Jeunesse et de l'Enfance :

Microsoft Teams/OneDrive pour l'échange de documents

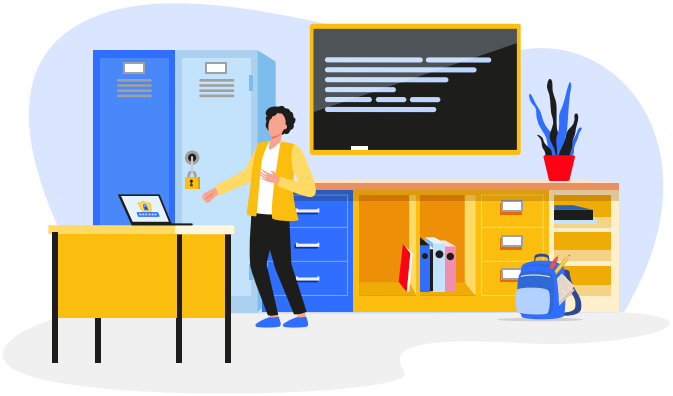
KI Kompass regroupe toutes les informations sur l'IA ainsi que les outils recommandés

LuxChat ou **Signal** pour la communication avec les élèves

Luxchat4Gov « éducation » pour la communication avec les parents d'élèves.

En salle de classe

Windows+L ou Cmd+Q: verrouillez l'écran en utilisant le raccourci clavier Windows + « L » ou Cmd + « Q » pour Mac lorsque vous sortez de la classe ou si vous quittez le bureau.



Rangement sécurisé dans des espaces désignés: utilisez des options de stockage sécurisées tels des armoires ou des tiroirs verrouillables pour ranger vos appareils personnels pendant les heures de cours, afin d'éviter qu'ils ne soient facilement accessibles ou endommagés.

Protections d'écran et étuis : utilisez des protections d'écran et des étuis durables pour protéger les appareils contre les chutes ou les chocs accidentels lors de déplacements dans la classe.

Mesures pour sécuriser vos appareils privés

Assurer la meilleure protection possible de vos outils et données n'est jamais une mauvaise idée. Et d'autant plus si une situation se présente où vous êtes amené à utiliser votre ordinateur, smartphone ou autre appareil connecté privé dans le contexte scolaire.

Verrouillage par code pin ou mot de passe

Activer un code ou un mot de passe fort protège votre appareil contre les accès non autorisés et réduit le risque de vol de données.

Gestionnaire de mots de passe

Utiliser un tel logiciel permet de concevoir des mots de passe forts et uniques et de les stocker en toute sécurité. De cette manière, il n'est plus nécessaire de retenir une multitude de mots de passe différents, vous ne devez retenir que le mot de passe principal de votre gestionnaire.

Mise à jour des logiciels

S'assurer que tous les logiciels et applications utilisés sont régulièrement mis à jour pour bénéficier des dernières protections contre les menaces en ligne.

Sauvegardes régulières

Sauvegarder régulièrement (p. ex. une fois par semaine) les données et les fichiers importants sur un support externe ou un service cloud sécurisé ou configurer des sauvegardes automatiques afin d'éviter toute perte en cas de dommage ou de dysfonctionnement.

Réseaux Wi-Fi publics

Préférer l'Internet mobile aux réseaux publics pour entrer des mots de passe ou effectuer des paiements.

Désactivation de fonctionnalités inutilisées

Désactiver les services Bluetooth, NFC ou de localisation et ne les activer qu'en cas de besoin.

Mesures en cas de vol ou de perte d'un appareil

Se familiariser avec les démarches à entreprendre pour minimiser les conséquences en cas de perte ou de vol de son smartphone ou autre appareil.

LES MOTS DE PASSE AVEC LES ÉLÈVES

Le **choix du mot de passe** est un moment opportun pour sensibiliser les élèves aux notions de responsabilité et de droit à la vie privée. Il est recommandé de laisser les enfants choisir leur propre mot de passe après avoir expliqué comment créer un mot de passe fort.

Comment créer un mot de passe sécurisé ?

VARIANTE 1

Choisissez une phrase qui vous plaît, facile à mémoriser et qui ne contient pas d'informations personnelles.

EXEMPLE

Aujourd'hui je mange 1 pomme du jardin de mes parents !

OPTION AVANCÉE

Remplacez les espaces par un caractère spécial.

EXEMPLE

Aujourd'hui!je!mange!1!pomme!du!jardin!de!mes!parents!

VARIANTE 2

Vous pouvez aussi utiliser uniquement les premières lettres des mots de la phrase choisie, comme :

EXEMPLE

Ajm1pdjdmp!

Créez des mots de passe différents : personnalisez votre mot de passe en fonction de l'application ou du site que vous utilisez. Par exemple, pour *TikTok*, ajoutez « *tt* » à la fin de votre mot de passe.:

EXEMPLE

Ajm1pdjdmp!tt

Pour tester votre mot de passe, allez sur le site web de **BEE SECURE**, choisissez « *Outils interactifs* » dans le menu, puis « *Tester la résistance d'un mot de passe* ».

Conserver le mot de passe dans un endroit sûr

Une fois les mots de passe individuels choisis, les élèves les notent sur un bout de papier qui sera mis dans une enveloppe fermée à l'aide d'un morceau de scotch. Les enveloppes sont à garder dans un endroit non accessible à des tiers. Si jamais un élève ne se rappelle plus son mot de passe, il pourra toujours jeter un coup d'œil dans l'enveloppe. Il est important que les élèves apprennent que les mots de passe sont comme des brosses à dents que l'on ne partage pas avec autrui.

2.2 Confidentialité et protection de la vie privée

En tant qu'enseignant, vous communiquez avec les enfants, les parents, les collègues, les intervenants pour des besoins spécifiques et autres. Souvent cette communication porte sur des données sensibles telles que des informations sur la santé de l'enfant ou des données personnelles comme son nom et son adresse. Assurez-vous de prendre les mesures appropriées pour traiter ces données de façon responsable et garantir le droit à la vie privée des enfants.

DONNÉES PERSONNELLES OU DONNÉES SENSIBLES ?

Les **données personnelles** permettent d'identifier une personne, par une information ou un croisement d'information. Exemples : le nom, l'adresse, l'âge, le numéro de téléphone. Le traitement de ces données est régi par le RGPD.

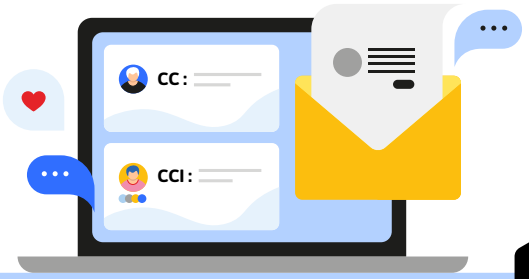
Les **données sensibles** permettent non seulement l'identification d'une personne, mais risquent d'entraîner une discrimination ou une atteinte aux droits fondamentaux de la personne. Il est interdit par le RGPD de partager ces données, sauf dans quelques cas exceptionnels très précis, comme la protection de la vie ou le consentement explicite de la personne concernée. Exemples : origine raciale ou ethnique, convictions religieuses, données médicales, données concernant l'orientation sexuelle.

Mesures pour sécuriser la communication et le transfert de données

Envoi de messages et d'e-mails: l'envoi de données personnelles par *WhatsApp* ou par e-mail est déconseillé, car il s'agit de canaux non-sécurisés. Pour protéger la vie privée des enfants et des parents, il faut privilégier les canaux sécurisés, comme Luxchat et les plateformes d'échange de données proposées par le CGIE/Restena/l'école (rubrique 2.1 Sécuriser les appareils électroniques).

LES BONS RÉFLEXES POUR EMPÊCHER QU'UN E-MAIL NE TOMBE ENTRE DE MAUVAISES MAIN

- Vérifiez le destinataire : est-ce bien le bon parent ou représentant légal à qui vous envoyez le mail ?
- Vérifiez les champs Cc et Cci (vides, à l'exception des destinataires choisis bien sûr).
- Si vous transférez un mail, y a-t-il des informations dans les e-mails envoyés auparavant qui ne regardent pas le destinataire ?
- Vérifiez si vous avez choisi «répondre» ou «répondre à tous».



CC ET CCI, C'EST QUOI, DÉJÀ ?

«Cc», abréviation pour «copie carbone». Ce champ ajoute aux destinataires «premiers», des destinataires dont on n'attend pas forcément une réponse, mais que l'on souhaite inclure dans une affaire ou informer d'un sujet. Les adresses électroniques des personnes en « Cc » sont visibles aux destinataires premiers.

«Cci/BCC», abréviation pour «copie carbone invisible/blind carbon copy». Les personnes recevant le mail ne voient pas les autres destinataires. Une option pour ne révéler aucun destinataire – et ainsi protéger leurs données de contact – est d'envoyer le mail à sa propre adresse et de mettre tous les destinataires en Cci.

Outils de traitement des données en ligne: les outils de traitement en ligne, comme les éditeurs de texte en ligne avec des fonctionnalités de coopération, peuvent présenter des risques de sécurité. Les enseignants doivent être conscients des politiques de confidentialité des outils qu'ils utilisent et s'assurer que les données sont traitées de manière éthique et sécurisée. Il est recommandé de se limiter aux programmes et outils proposés par le Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse. Cela vaut également pour les programmes d'IA.

TRAVAILLER AVEC UNE INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle a fait irruption dans nos vies et ses fonctions toujours plus performantes évoluent à un rythme hallucinant. Tandis qu'il est tout à fait légitime de se faire assister par une IA, il faut **rester vigilant et critique** vis-à-vis des réponses de l'IA :

- les réponses peuvent être très convaincantes mais incorrectes ;
- les réponses peuvent être incomplètes, donc risque de manquer des aspects ;
- les réponses sont biaisées et peuvent renforcer des stéréotypes.

Un autre point à considérer est la **protection des données** : il est difficile de savoir comment ces outils traitent les données et comment elles seront utilisées ultérieurement. Si un service (avec ou sans IA) est gratuit, il est probable qu'on paye avec ses données personnelles. **Évitez donc d'entrer des données personnelles ou autres informations qui facilitent votre identification ou celles de vos élèves (prénoms, noms, dates de naissance, adresses, nom de l'école etc.) dans le contact avec un chatbot utilisant l'IA**.

Précautions contre les risques sur Internet

Filtrage de contenus sur Internet : les logiciels de filtrage de contenus analysent le contenu de pages web en temps réel et limitent le contenu pouvant être visualisé. Ils sont personnalisables et bloquent l'accès à des sites inappropriés ou dangereux, tels que ceux contenant de la violence, de la pornographie ou des discours de haine.

Authentification à deux facteurs : activer l'authentification à deux facteurs sur les comptes en ligne ajoute une couche de sécurité supplémentaire lors de la connexion. Cette mesure réduit le risque qu'un tiers ne se connecte à un compte (p. ex. un réseau social), même s'il est arrivé à se procurer le mot de passe.

Reconnaître les signes de d'hameçonnage (*phishing*) (rubrique 3. Utilisation des réseaux sociaux) :

- Vérifiez l'authenticité des e-mails ou des sites web avant de cliquer sur des liens.
- Examinez le domaine de l'URL pour vous assurer qu'il correspond au site auquel vous vous souhaitez accéder. Les sites d'hameçonnage utilisent souvent des domaines similaires à ceux des sites légitimes, mais avec de légères variations ou des fautes de frappe.
- Vérifiez la syntaxe de l'URL, les erreurs ou caractères inhabituels pourraient indiquer une tentative de tromperie.
- Protocole de sécurité : vérifiez que l'URL commence par « *https://* » plutôt que simplement par « *http://* ». La présence de « *https://* » indique que la connexion est sécurisée et cryptée.

Rapport des tentatives d'hameçonnage : signalez toute tentative d'hameçonnage à l'administration scolaire ou au service informatique afin de prendre des mesures appropriées et d'informer les autres membres du personnel.

3. UTILISATION DES RÉSEAUX SOCIAUX

Être présent sur les réseaux sociaux fait aujourd'hui partie de la vie sociale numérique et les règles de comportement n'y sont pas si différentes que dans la vie sociale analogique. En connaissant les risques, les enseignants peuvent non seulement protéger leur image publique, mais aussi protéger les enfants de menaces en ligne.

3.1 Représentation de soi en ligne

Dans le contexte scolaire

En tant qu'enseignant et fonctionnaire, vous êtes un représentant de l'État et de l'école comme institution publique, ce qui vous oblige à faire valoir la précaution dans ce que vous publiez. Tandis que des publications sur des réussites sportives ou des engagements volontaires peuvent améliorer l'image publique, des photos de fêtes déjantées ou autres contenus douteux peuvent susciter des questions sur votre aptitude à enseigner aux enfants.

Les réseaux sociaux sont a priori des plateformes publiques : vos collègues, vos supérieurs, les élèves, leurs parents y ont accès et pourraient voir ce que vous y publiez.

- Même les contenus destinés uniquement aux amis peuvent être visibles par d'autres s'ils sont partagés ou si vos amis ou le réseau social sont victimes d'une violation de données.
- Même l'acte de « *liker* » un contenu n'est pas un acte privé, mais consiste déjà en un acte de publication qui est visible par d'autres.

D'un point de vue légal

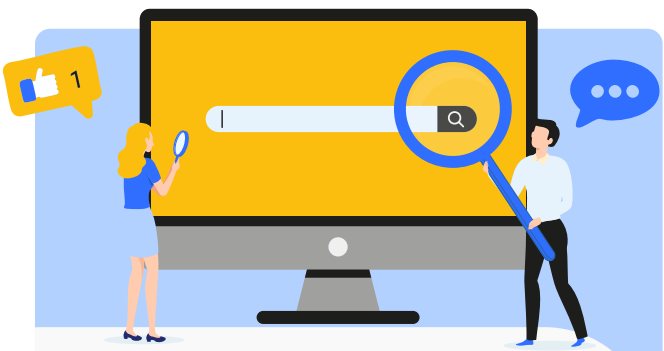
(Art. 10 § 1 Loi modifiée du 16 avril 1979)
Comportement digne de ses fonctions

Le fonctionnaire doit, ***dans l'exercice comme en dehors de l'exercice de ses fonctions****, éviter tout ce qui pourrait porter atteinte à la dignité de ces fonctions ou à sa capacité de les exercer, donner lieu à scandale ou compromettre les intérêts du service public.*

Votre réputation professionnelle sert à la préservation de la confiance dans la profession de l'enseignant et dans le système éducatif. La décrédibilisation de l'école ou de la profession peut faire l'objet d'une sanction disciplinaire ou, dans un cas extrême, d'un licenciement.

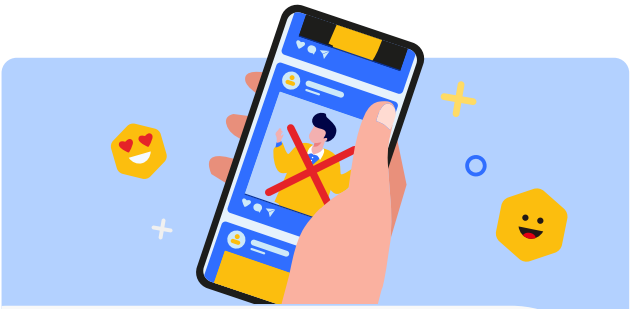
Recommandations

Il est recommandé de vérifier quelle image de vous on trouve en ligne, de choisir les paramètres de confidentialité adéquats et de soigner votre représentation sur les réseaux sociaux.



POUR VÉRIFIER VOTRE REPRÉSENTATION EN LIGNE:

- Entrez votre nom dans un moteur de recherche et analysez les résultats : quelles informations, photos et publications trouvez-vous ? Quelles conclusions pourrait-on en tirer ?
- Déconnectez-vous de vos profils sur les réseaux sociaux ou demandez à quelqu'un d'autre de voir votre profil sur son téléphone pour vérifier ce que les autres voient affiché quand ils consultent votre profil.
- Utilisez la checklist proposée par BEE SECURE en annexe.



POUR GÉRER VOTRE REPRÉSENTATION SUR LES RÉSEAUX SOCIAUX:

- Faites le ménage du passé : supprimez les publications et photos compromettantes, faites le tri dans vos listes d'amis.
- Actualisez les paramètres de confidentialité du profil pour limiter la visibilité et la portée de vos publications.
- Définissez l'objectif d'utilisation pour chaque réseau social (Avec qui je communique, sur quoi et comment ?).
- Utilisez des photos de profil et pseudonymes différents selon les plateformes – surtout entre usage privé et professionnel.

3.2 La classe sur les réseaux sociaux

Dans le contexte scolaire

Le personnel enseignant peut jouer un rôle clé en sensibilisant les élèves aux bonnes pratiques et aux risques liés à l'utilisation des réseaux sociaux. En général, peu d'enfants ont un compte utilisateur sur des réseaux sociaux avant l'âge de 12 ans ; à savoir aussi que les réseaux sociaux sont déconseillés avant 15 ans (stratégie « sécher.digital » du MENJE). Il reste néanmoins pertinent de comprendre les mécanismes et les pratiques existants, afin de mieux appréhender les enjeux auxquels les enfants peuvent être confrontés.

Vous pourriez aussi souhaiter participer avec votre classe à un projet requérant une présence sur les réseaux pour collecter des votes ou des sponsors ou être amené à publier des photos de projets sur un réseau social. Dans ce cas, vous devez mesurer l'utilité du projet, les avantages et les désavantages de s'adresser à un plus large public et les droits des enfants à la vie privée.

D'un point de vue légal

La plupart des réseaux sociaux et services de messagerie exigent que les utilisateurs aient au moins 13 ans à cause de la législation en matière de protection des enfants aux États-Unis. Au Luxembourg, comme ailleurs en Europe, le RGPD définit l'âge minimum des utilisateurs. Les jeunes et enfants entre 13 et 16 ans doivent avoir obtenu le consentement de leurs parents pour utiliser un tel service. En pratique, la vérification d'âge s'est avérée assez facile à contourner.

Il est interdit d'utiliser des photos prises en classe pour faire de la publicité pour vendre des ressources pédagogiques, puisqu'il s'agit d'un but lucratif.

Recommandations

- Évitez les «*amitiés*» avec les parents ou élèves: expliquez aux élèves que vous n'acceptez aucune demande d'«*amitié*» d'élèves pour préciser qu'il ne s'agit pas d'un rejet personnel.
- Séparez votre profil personnel de publications des projets scolaires.
- Demandez la permission explicite des parents pour le type de contenu (ex : photos des produits des enfants), le type de plateforme utilisé et la durée de la visibilité.
- Publiez les photos sans données personnelles des enfants (comme leur nom).
- Pensez aux consignes en matière de droit à l'image (rubrique 1.1).
- Configurez les paramètres de confidentialité (rubrique 3.1).

EN BREF

- Soignez votre présence dans le monde virtuel et veillez à votre réputation professionnelle.
- Demandez l'accord explicite des parents si vous publiez des photos ou autres informations de projets scolaires.

3.3 Risque : piratage et usurpation d'identité

Dans le contexte scolaire

Toute personne peut être la cible ou même la victime des cybercriminels cherchant à usurper son identité pour accéder à des informations sensibles ou manipuler des données. Du fait de leur position d'autorité et de confiance, les risques de ce type de menace sont encore plus significatifs pour les enseignants. Les précautions prises pour protéger votre identité contribuent également à protéger les élèves de contenus inappropriés ou de comportements nuisibles.

DIFFÉRENTES FORMES DE CYBERCRIMINALITÉ

L'hameçonnage est une technique utilisée par des cybercriminels pour tromper les utilisateurs dans le but de leur faire divulguer des informations sensibles, telles que des mots de passe, des numéros de carte de crédit ou d'autres données personnelles. En créant un « profil cloné » ou « faux profil », *fake profile* en anglais, les cybercriminels établissent des liens de confiance avec leurs victimes pour leur demander ensuite des informations personnelles ou sensibles.

Le **grooming** désigne le processus par lequel un adulte établit une relation de confiance avec un enfant ou un adolescent dans le but de l'exploiter sexuellement. Le personnel enseignant est particulièrement vulnérables face à cette menace si l'identité de l'un de ses membres et les conséquences pour les enfants et leur entourage sont dévastatrices.

Les **photomontages** et les vidéos *deepfake* utilisent des images existantes du visage ou du corps pour les placer dans des contextes compromettants ou pour les manipuler de façon à ce que la personne fasse ou dise des choses qu'elle n'a jamais dites ou faites, par exemple des vidéos pornographiques. Bien que les victimes ne soient absolument pas responsables de la création de telles images, la diffusion par Internet rend souvent le rétablissement de la vérité et de la réputation très difficile.

D'un point de vue légal

Le RGPD vous oblige à traiter les données des enfants de manière responsable, transparente et sûre (rubrique 1.2). Si des informations confidentielles sur les élèves sont divulguées à cause d'un comportement négligent de la part d'un enseignant, cela pourrait avoir des conséquences juridiques pour ce dernier.

Recommandations : prévention et action contre l'usurpation de l'identité

- Vérifiez régulièrement si votre nom, identité ou photos sont utilisés.
- Protégez vos profils avec des mots de passe uniques sûrs.
- Créez une adresse e-mail juste pour les réseaux sociaux.
- En cas d'abus : signalez les faux profils ou l'abus de vos données auprès de l'opérateur du réseau.
- Avertissez vos collègues afin qu'ils se méfient du faux profil.

4. PRÉVENTION ET INTERVENTION EN CAS D'INCIDENT

Que ce soit en ligne ou en présentiel, le respect envers autrui est important et doit être cultivé dans toutes les circonstances. Dans le monde numérique, l'anonymat et la distance facilitent parfois des comportements irrespectueux. Comme mesure préventive, une charte de bonne conduite établie avec les élèves au début de l'année scolaire aide à connaître les risques auxquels les enfants peuvent être exposés et permet d'intervenir de manière appropriée en cas de situation critique en classe.

4.1 Prévention

Mettre en place une charte de bonne conduite

Dès le début de l'année scolaire, il est utile de thématiser le sujet du comportement respectueux envers autrui avec les élèves. Des règles générales pour le traitement des autres en classe et en ligne peuvent être discutées, puis inscrites dans une charte de bonne conduite. Il importe de parler des conséquences et de fixer des procédures en cas de violation des règles. Signée par toutes les personnes impliquées – personnel enseignant, élèves et parents – et affichée bien visiblement en classe, elle constitue un outil de prévention contre les comportements irrespectueux.

BEE SECURE met à disposition un modèle de charte de bonne conduite en annexe.

Fixer des règles pour le chat de classe

Comme beaucoup de classes utilisent un chat pour l'échange entre tous les membres de la classe, il est conseillé de fixer aussi des règles pour le chat. Avec un grand nombre de participants dans un chat, des problèmes peuvent survenir, tels que les messages de harcèlement, le spam, les contenus non-pertinents ou des messages en chaîne. Pensez aussi aux conséquences et sanctions en cas de non-respect des règles.

Donner le bon exemple

Votre propre conduite en classe peut influencer celle de vos élèves. Profitez-en pour leur montrer le bon exemple en respectant les droits de l'enfant, le règlement général de la protection des données, le règlement d'ordre intérieur de l'école, mais aussi la charte des règles que vous avez fixée avec vos élèves !

Garder le dialogue avec les élèves

- Tenez-vous au courant des préférences en matière de communication de vos élèves : les tendances, les jeux, les plateformes utilisées et les défis évoluent en permanence et varient selon les groupes d'âge. Plongez dans leur univers et restez à l'écoute pour mieux les comprendre.
- La formation continue constitue également un excellent moyen de rester informé des nouvelles tendances. N'hésitez pas à vous renseigner sur les formations et cours disponibles – notamment les formations BEE SECURE pour les professionnels du secteur pédagogique.

Sensibiliser les élèves et la communauté scolaire

- Abordez le sujet avec la classe afin d'apprendre aux élèves les risques que ces plateformes peuvent poser pour eux, surtout lorsqu'on constate que beaucoup d'élèves en classe utilisent des plateformes non adaptées à leur âge.
- Une autre option est de réserver une formation préventive BEE SECURE pour aborder le sujet de manière ludique en classe avec un de nos formateurs (« Cyberharcèlement : en mission avec le détective Shadow », pour le cycle 3.2).
- Organisez une séance d'information pour les parents sur les risques et dangers en ligne.

Faciliter l'accès à l'aide

Assurez-vous que les enfants aient accès aux numéros et adresses où ils peuvent recevoir de l'aide de façon anonyme, confidentielle et gratuite, au cas où ils n'oseraient pas s'adresser à une personne de confiance.

BEE SECURE Helpline
8002 1234

KJT
116111

Online help : Consultation par écrit, en ligne, pour les enfants et les jeunes

Chatberodung : Consultation par discussion en direct, pour les enfants et les jeunes

4.2 Intervention en cas de situation d'incident

L'Internet fait partie de la vie quotidienne des élèves et des enseignants. Les dangers pour les élèves sont multiples : le cyberharcèlement, l'exposition à des contenus inadaptés, les atteintes à la vie privée, le partage illicite de données ou de contenu ne s'arrêtent pas devant les salles de classe. Connaître les risques auxquels peuvent-être confrontés les enfants et savoir comment réagir permet de mieux les protéger et de les accompagner vers un usage responsable et sécurisé d'Internet.

Les rubriques suivantes vous présentent des cas de figure exemplaires, les questions à se poser avant de réagir et les démarches à entamer par la suite.

CAS 01

CYBERHARCÈLEMENT

Jacky a 8 ans, elle vient vers vous pour vous informer qu'un autre élève de l'école lui a envoyé un commentaire sur TikTok lui disant que sa façon de danser était moche.

MÊME DROIT POUR TOUS

L'article 2 de la Convention relative aux droits des enfants que tout enfant à des droits, « sans distinction aucune », c'est à dire que tout enfant a droit à la non-discrimination.

Avant de réagir

Est-ce que le commentaire a été envoyé au moment de l'école ?

Attention à ne pas dépasser les limites de sa fonction professionnelle ; à côté de la responsabilité du personnel enseignant, il y a aussi la responsabilité des parents.

Est-ce que la plateforme sur laquelle le message ou commentaire a été envoyé est destinée à des enfants de l'âge de la victime ?

Il est important de se rendre compte que les médias sociaux tels que *TikTok*, *Instagram* et Co ne sont pas destinés aux enfants en-dessous de 13 ans.

Est-ce que la victime a obtenu plusieurs messages de ce genre ou est-ce qu'il s'agit d'un seul message ?

Par cyberharcèlement, on entend le fait d'insulter, de menacer, de ridiculiser ou de harceler intentionnellement d'autres personnes à l'aide des services en ligne ou téléphoniques pendant une période prolongée.

Démarches

1. Être à l'écoute de l'élève et assurer le soutien

- Déculpabilisez l'enfant. Rassurez-le sur le fait que ce n'est pas de sa faute et qu'il n'a rien à se reprocher.
- Intervenez en tant qu'adulte et assurez à l'enfant que vous allez réagir. Les enfants ne sont pas en mesure de résoudre par eux-mêmes des situations de harcèlement en ligne, l'intervention d'un adulte est indispensable.
- Conseillez à l'enfant de ne pas réagir aux messages ou publications des harceleurs.
- Notez tout ce que l'élève explique, afin d'avoir un suivi et si besoin, aidez-le à sécuriser les preuves.

2. Informer la direction

- Adressez-vous à vos collègues et si besoin à votre direction régionale et aux parents pour évaluer la situation et vous concerter sur la démarche à suivre

3. Sensibilisation de la communauté scolaire

- Rapprochez-vous du groupe « Stop Mobbing », une initiative du Ministère de l'Education nationale, de l'Enfance et de la Jeunesse qui intervient dans les classes, soutient les victimes et parle aux enseignants.
- S-Team du Service national de la jeunesse : le projet propose des activités de sensibilisation et de prévention de la violence dans l'école/ maison relais. Le but est de responsabiliser les enfants et les jeunes quant à leur rôle dans la prévention de la violence et de leur permettre de contribuer à un meilleur vivre-ensemble. La « médiation par les pairs » est partie intégrante du projet « S-Team ».
- BEE SECURE – Formation « Cyberharcèlement: en mission avec le détective Shadow » pour les élèves du cycle 3.2.
- BEE SECURE – Formations pour le personnel enseignant et éducatif sur l'utilisation d'Internet par les enfants et les jeunes et les risques y liés.

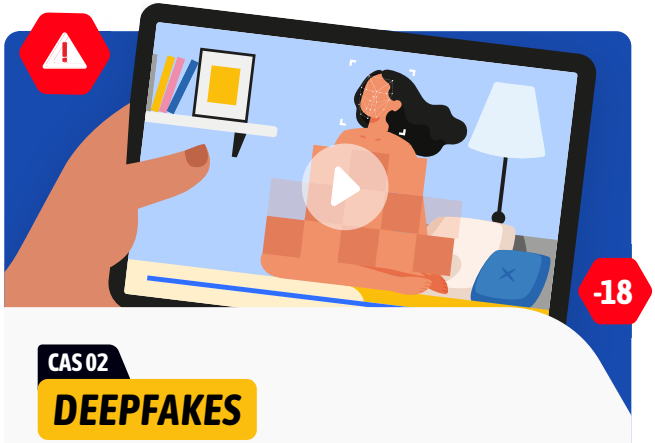
4. S'informer sur le cadre légal

- Informez-vous sur le dépôt d'une plainte et sur la manière d'agir lors de confrontations dans le BEE SECURE Guide sur le cyberharcèlement que vous trouvez sur le site sous la rubrique « Publications ».

Aides externes

BEE SECURE Helpline
8002 1234

KJT
116111



CAS 02

DEEPFAKES

On vous a informé qu'un deepfake d'un de vos élèves circule dans l'école. La vidéo truquée, qui montre l'élève dans une situation compromettante, a été partagée par plusieurs élèves.

Démarches

1. **Être à l'écoute et assurer le soutien de l'élève concerné**
   - Il est important de fournir un soutien émotionnel et psychologique à l'élève victime du *deepfake*.
   - Adressez-vous à vos collègues et si besoin à votre direction régionale et aux parents pour évaluer la situation et vous concerter sur la démarche à suivre.

2. **Informer la direction de l'école**
   - Signalez l'incident à la direction d'école pour que des mesures appropriées puissent être prises.
   - Identifiez l'origine de la diffusion : en collaboration avec la direction, il est essentiel de déterminer comment le *deepfake* a été créé et diffusé, et de repérer les élèves impliqués.

ARTICLE 16 -DROIT À LA PROTECTION DE LA VIE PRIVÉE

Aucun enfant ne peut faire l'objet d'ingérences arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance.

Chaque enfant a droit à une protection contre les atteintes à son honneur et à sa réputation.

3. **Informer et impliquer les parents**
   - Les parents de l'élève concerné doivent être informés de l'incident. Une collaboration avec les parents est cruciale pour soutenir l'élève et aborder la situation de manière cohérente.

4. **Prendre des mesures appropriées**
   - Mesures disciplinaires appropriées : si des élèves sont identifiés comme responsables de la création ou de la diffusion du *deepfake*, des mesures disciplinaires doivent être envisagées conformément aux politiques de l'établissement.

5. **Sensibiliser la communauté scolaire**
   - Organisez des sessions de sensibilisation pour informer les élèves et le personnel éducatif sur les dangers des *deepfakes* et promouvoir un environnement numérique respectueux.

6. **Considérer les aspects juridiques**
   - La loi du 21 mai 2024 au Luxembourg a adapté le droit pénal pour inclure les *deepfakes*, les qualifiant d'infractions pénales.

Aides externes

BEE SECURE Helpline
8002 1234

KJT
116111

CAS 03

DROIT À L'IMAGE ET PROTECTION DE LA VIE PRIVÉE

Pendant le cours, Alex a utilisé sa montre connectée pour enregistrer une vidéo de son enseignant, ainsi qu'un enregistrement audio des conversations de ses camarades sans leur en demander la permission. Il a été signalé par un de ses camarades.

Démarches

1. **Parler à l'élève concerné**
   - Demandez de supprimer immédiatement la vidéo et l'audio.
   - Expliquez que, sans consentement, la vidéo viole la vie privée et peut mettre les autres mal à l'aise.
2. **Si nécessaire, informer la direction et les parents**
   - Informez les parents de l'enfant concerné.
   - Informez la direction pour prendre d'éventuelles mesures disciplinaires ou de prévention.
3. **Sensibiliser la communauté scolaire**
   - Abordez le sujet du droit à l'image et des droits des enfants en classe.
   - Informez les parents pour discuter de l'importance de respecter la vie privée et de l'interdiction d'utiliser les appareils connectés en classe.
   - Mettez en place une charte de bonne conduite (rubrique 4.1 Prévention).
4. **Si la gravité du cas le nécessite, s'informer sur les éventuelles démarches légales à entreprendre.**

CAS 04

CHALLENGES (LES DÉFIS EN LIGNE)

Un élève lance un défi dangereux qui se répand rapidement dans la classe. L'enseignant prend conscience de la situation.

Avant de réagir

- Évaluez de quel type de challenge il s'agit : est-il inoffensif, risqué ou même dangereux ?
- Si les enfants vous parlent de *challenges*, écoutez-les et expliquez les risques, mais évitez de parler de challenges qui ne circulent pas encore afin de ne pas les diffuser.

Démarches

1. **Parler aux élèves concernés**
   - Cherchez à comprendre l'intérêt du challenge.
   - Expliquez les risques.
2. **Si nécessaire, informer la direction et les parents**
   - Informez les parents des enfants concernés.
   - Informez la direction pour prendre d'éventuelles mesures disciplinaires ou de prévention.
3. **Sensibiliser la communauté scolaire**
   - Soulignez les risques potentiels et aborder le sujet du respect, de la sécurité et de la manière de reconnaître et refuser les défis nuisibles en classe.
   - Informez les parents pour discuter de l'importance de respecter la vie privée et de l'interdiction d'utiliser les appareils connectés en classe.
   - Mettez en place une charte de bonne conduite (rubrique 4.1 Prévention).
4. **Si la gravité du cas le nécessite, s'informer sur les éventuelles démarches légales à entreprendre.**

4.3 Les limites de votre responsabilité

Vous n'êtes pas seuls à gérer ces incidents ! Découvrez les divers services que vous pouvez contacter en cas de besoin :

BEE SECURE Helpline

Une ligne d'assistance offrant des conseils pratiques et un soutien aux enfants, jeunes, parents, adultes et au personnel enseignant et éducatif confrontés à des problèmes liés à la sécurité en ligne. Elle aide à comprendre et à gérer les risques numériques.

→ bee-secure.lu/helpline

BEE SECURE Stopline

Une plateforme pour signaler des contenus illégaux en ligne (comme la pédopornographie ou l'exploitation). Elle reçoit les signalements et les traite en collaboration avec les autorités et partenaires compétents au niveau national et international.

→ stopline.bee-secure.lu

KJT – KannerJugendTelefon 1 1 6 1 1 1

Un service d'assistance pour enfants et jeunes, il offre également un soutien aux personnes qui s'occupent d'eux. La consultation se fait par téléphone, mail ou chat.

→ kjt.lu

CEPAS – Centre psycho-social et d'accompagnement scolaires

Le CePAS s'engage à favoriser l'épanouissement et le bien-être des jeunes à l'école en collaboration avec les acteurs de la communauté scolaire. Son Centre de ressources soutient le personnel éducatif et psycho-social des Services psycho-sociaux et d'accompagnement scolaires (SePAS), des Services socio-éducatifs (SSE) et des internats scolaires et les accompagne dans la mise en place de leurs pratiques professionnelles.

→ cepas.public.lu

CESAS – Centre national de référence pour la promotion de la santé affective

Le Cesas est un facilitateur du réseau d'acteurs poursuivant l'objectif de promouvoir la santé affective et sexuelle à travers l'information, la sensibilisation et la formation. Une attention particulière est consacrée aux professionnels de l'enfance et de la jeunesse.

→ cesas.lu

CNAPA – Centre national de prévention des addictions

Il a la mission d'informer et sensibiliser au sujet de modes de vie sains et offre également des formations pour les professionnels du domaine pédagogique.

→ cnapa.lu

CNPD – Commission nationale pour la protection des données

Garante du respect de la vie privée et du traitement légal des données personnelles ; elle conseille, contrôle et peut sanctionner les organismes en cas de non-conformité.

→ cnpd.public.lu

OKAJU – Ombudsman fir Kanner a Jugendlecher

Cette institution indépendante a pour mission de promouvoir, de sauvegarder et de protéger les droits de l'enfant tels qu'ils sont définis par la Convention internationale relative aux droits de l'enfant (CIDE).

→ okaju.lu

ONE – Office national de l'enfance

L'Office national de l'enfance (ONE) est une administration publique sous la tutelle du ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse. Il offre aide et soutien aux enfants, aux jeunes, aux jeunes adultes et aux familles qui rencontrent des difficultés.

→ officenationalenfance.lu

Police Luxembourg

Elle est chargée de la prévention, de l'enquête et de l'intervention en cas d'infraction ou de danger immédiat; elle prend en charge les signalements nécessitant une intervention policière.

→ police.public.lu

Planning Familial

Cette asbl est conventionnée par le Ministère de la Santé ; sa mission est de faciliter l'accès à l'information, l'éducation et les services de santé affective, sexuelle et reproductive. Elle opère dans des centres à Luxembourg-Ville, Esch-sur-Alzette et Ettelbruck.

→ pfl.lu

Respect.lu

Un service d'écoute et d'accompagnement des personnes qui sont confrontées, de quelque manière que ce soit, à l'extrémisme et à la radicalisation violente ; il offre ressources, conseils et outils pédagogiques.

→ respect.lu

CGIE – Centre de gestion informatique de l'éducation

Le CGIE du Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse est compétent pour l'ensemble des technologies de l'information et de la communication pour l'administration de l'Éducation nationale. Le CGIE promeut la familiarisation avec le numérique à travers un nombre de projets.

→ zesummendigital.lu

SCRIPT – Service de Coordination de la Recherche et de l'Innovation pédagogiques et technologiques

Le SCRIPT est un des moteurs principaux de développement du domaine de l'éducation au Luxembourg. Il est chargé de mettre en œuvre les priorités de la politique éducative et de contribuer ainsi au développement de la qualité scolaire.

→ script.lu

GOVCERT

Point de contact unique pour tous les types d'incidents informatiques qui pourraient constituer une menace pour les systèmes d'information du gouvernement national et d'autres opérateurs d'infrastructures critiques publiques ou privées.

→ govcert.lu

BIBLIOGRAPHIE

- **BEE SECURE.** Sexting - Unité de cours pour la vidéo « Sharen » bee-secure.lu/fr/publication/unite-de-cours-sexting-pour-la-video-sharen
- **BEE SECURE.** Le label PEGI pour les jeux vidéo bee-secure.lu/fr/publication/le-label-pegi-pour-les-jeux-video
- **BEE SECURE.** Droit à l'image. bee-secure.lu/droit-image-fiche-thematique
- **BEE SECURE.** Les écrans en famille. bee-secure.lu/les-ecrans-en-famille
- **BEE SECURE.** Sécurisez votre smartphone bee-secure.lu/wp-content/uploads/2023/11/securisez-votre-smartphone-fr.pdf
- **BEE SECURE.** Risques sur Internet bee-secure.lu/fr/publication/risques-sur-internet
- **BEE SECURE.** Guide sur le cyberharcèlement bee-secure.lu/cyberharcelement-guide
- **BEE SECURE.** Radar 2025 bee-secure.lu/bee-secure-radar
- **BEE SECURE.** Âge minimum pour utiliser *WhatsApp*, *Instagram* & Co. bee-secure.lu/fr/news/age-minimum-a-partir-de-quel-age-les-enfants-peuvent-ils-utiliser-whatsapp-instagram-co
- **CGID.** Devoirs du fonctionnaire cgid.gouvernement.lu/fr/legislation/devoirs-fonctionnaire.html
- **Childfocus.** De mots à maux : comprendre, reconnaître et agir sur le cyberharcèlement. childfocus-webshop.be/products/dossier-pedagogique-stop-au-cyber-harcelement
- **Unicef.** Texte de la Convention relative aux droits de l'enfant unicef.org/fr/convention-droits-enfant/texte-convention
- **Commission européenne.** Public domain https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/public-domain-2020-11-19_en
- **CNIL.** Grands principes du RGPD cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd cnil.fr/fr/identifier-les-donnees-personnelles cnil.fr/fr/definition/donnee-sensible
- **CNPD .** Droit à l'image. cnpd.public.lu/fr/dossiers-thematiques/droit-image.html cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/droit-image/CNPD-fiche-edusphere-milieu-scolaire.pdf
- **GDPR.eu.** What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr/

- **KI Kompass**. Orientation pratique et échange sur l'intelligence artificielle pour les écoles au Luxembourg
  ki-kompass.lu

- **Klicksafe.** Mediennutzungsvertrag.
  mediennutzungsvertrag.de

- **Klicksafe.** Klassenchat-Regeln.
  klicksafe.de/printmaterialien/unsere-regeln-fuer-den-klassenchat-unterrichtseinheit

- **Legilux.** Droits d'auteur
  legilux.public.lu/eli/etat/leg/loi/2001/04/18/n2/consolide/20220409

- **Ministère de la culture.** Droits d'auteur
  mcult.gouvernement.lu/dam-assets/publications/guide-manuel/minist-culture/guide-droit-auteur/droits-auteur-droits-voisins-et-autres-droits-numerique.pdf

- **Saferinternet.at.** Sichere Internet-und Handynutzung macht Schule!
  saferinternet.at/wie-koennen-regeln-fuer-die-handynutzung-in-der-schule-aussehen

- **Saferinternet.at.** Tipps für Lehrende.
  saferinternet.at/zielgruppen/lehrende

- **Sécher.Digital**
  secher.digital/fr/utilisation-smartphone/

- **SNJ.** Activités analogiques
  erliewen.snj.lu

- **TISSERON, S.** Grandir avec les écrans « La règle 3-6-9-12 ». Bruxelles : Yapaka, 2013. (Temps d'arrêt lectures) 57 Pages. Document PDF
  yapaka.be/livre/livre-grandir-avec-les-ecrans-la-regle-3-6-9-12

NOTE DE BAS DE PAGE

[1]Le droit à l'image repose sur différentes lois relatives à la protection de la vie privée.
À titre d'exemple :
- Convention européenne des droits de l'homme, article 8 ;
- Loi du 8 juin 2004 sur la liberté d'expression dans les médias, telle que modifiée, l'article 14.(1) dispose que chacun a droit au respect de sa vie privée ;
- Loi du 11 août 1982 concernant la protection de la vie privée, qui interdit toute atteinte volontaire à l'intimité de la vie privée d'autrui, « *en fixant ou en faisant fixer, par un appareil quelconque, les images d'une personne se trouvant dans un lieu non accessible au public, sans le consentement de celle-ci* ». Ce texte interdit également la publication de telles images.

Éditeur : Service national de la jeunesse (SNJ)
Service national de la jeunesse - B.P. 707 L-2017 Luxembourg
www.snj.lu | www.bee-secure.lu

Guide - Conseils et Outils
Un modèle à l'ère du numérique
pour le personnel enseignant
01.2026

ISBN 978-2-919828-99-9
Ressource numérique

Initié par :
LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse

Opéré par :
Service national de la jeunesse
KJT.lu

Cofinancé par :
Cofinancé par l'Union européenne