INTERNET DANS LES MAISON RELAIS ?

SÛREMENT !

GUIDE

APERÇU

✖ Ce guide s'adresse aux responsables et au personnel (éducateurs/-trices) des Maisons Relais et s'intéresse à la question suivante :

« Comment garantir une utilisation d'Internet en toute sécurité au sein de la Maison Relais tant pour le personnel que pour les enfants ? »

Il vise à orienter la mise en place d'un concept de sécurité approprié pour l'utilisation d'Internet au sein de la Maison Relais. Il offre un aperçu pratique des principales réflexions à propos de cette thématique et en déduit des principes qui permettent d'élaborer son propre concept, en prenant en considération des aspects techniques, juridiques, et pédagogiques.

Dans le cadre d'une collaboration entre la Croix-Rouge et BEE SECURE, un projet pilote a été lancé en 2017 au sein de la Maison Relais de Dippach. Les participants à ce projet pilote ont testé l'utilisation d'une tablette en tant qu'offre pédagogique. Ce guide reprend les conclusions et enseignements qui en ont été tirés. Certaines recommandations du plan d'action « Secure MJ » (développées en 2013 pour les Maisons des Jeunes) ont par ailleurs été adaptées à la réalité de la Maison Relais.

LA SÉCURITÉ EST RELATIVE.
LA SÉCURITÉ N'EST PAS UN ÉTAT, MAIS UN PROCESSUS.

BEE SECURE

Editeur : SNJ
Annexe Forum Geesseknäppchen
40, bld. Pierre Dupong
L-1430 Luxembourg
B.P. 707 · L-2017 Luxembourg
www.bee-secure.lu/fr/form
www.snj.lu

Service National de la Jeunesse · kanner jugend telefon · SECURITY MADEIN.LU
LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG · Co-financed by the European Union Connecting Europe Facility

ISBN: 978-2-9199499-4-6

Notice légale
Cette publication a été réalisée par le SNJ (Service National de la Jeunesse) dans le cadre du projet BEE SECURE.
Le projet est mis en oeuvre par le Service National de la Jeunesse (SNJ), KannerJugendTelefon (KJT) et SecurityMadeIn.lu (SMILE g.i.e.).

Création graphique : Takaneo

Tirage 500 exemplaires
Internet dans la Maison Relais - 12.2018

SOMMAIRE

INTRODUCTION

Toute Maison Relais a besoin de mesures de sécurité pour Internet.

Société numérique, « smart home » connectée et bientôt voitures autonomes : la liste des mots clés et des thématiques allant de pair avec la « numérisation » s'est allongée à une vitesse fulgurante durant ces dernières années. La gestion et l'organisation de la Maison Relais en tant qu'institution ne peuvent plus se faire sans les ordinateurs et Internet.

Les membres du personnel, les parents et autres personnes (stagiaires, visiteurs, etc.) portent généralement sur eux un smartphone (privé) lors de leur séjour au sein de l'établissement et sont connectés à un réseau mobile ou au Wi-Fi interne. L'établissement lui-même a sa propre présence en ligne (site web), la communication professionnelle implique bien entendu des échanges d'e-mails et les données du personnel ainsi que des enfants sont souvent enregistrées sur des dispositifs de stockage numériques (tels que disques durs, clés USB, cloud).

Les enfants et Internet : milieu de vie et mission éducative.

Il va donc de soi qu'aujourd'hui les enfants grandissent dans un monde connecté, qui leur offre la possibilité de découvrir et d'expérimenter Internet de plus en plus tôt. Il est dès lors d'autant plus important de les encourager dans l'acquisition des compétences (médiatiques) indispensables, en lien avec les possibilités et défis liés au monde (numérique) d'aujourd'hui et de demain.

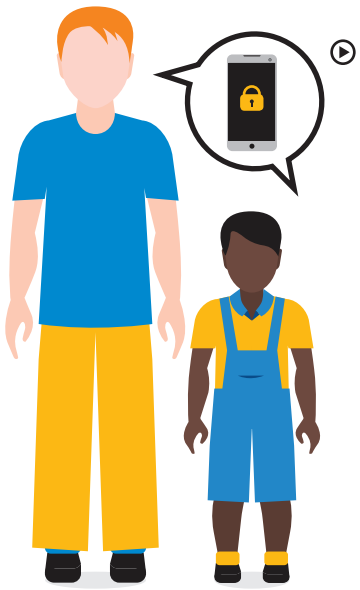
L'un des objectifs primordiaux de cette promotion consiste à sensibiliser les enfants à une utilisation positive, responsable et critique des nouveaux médias et des nouvelles technologies. Ainsi, la promotion des compétences médiatiques et le recours aux médias numériques au sein de la Maison Relais font également partie intégrante de la mission éducative, décrite plus en détail dans le cadre de référence national de l'éducation non formelle des enfants et des jeunes.

Dans sa rubrique « Langue, communication, médias », le cadre de référence national (2018) prévoit que les Maisons Relais traitent sur le plan pédagogique les médias numériques en tant que partie intégrante de l'environnement quotidien des enfants, en proposant des offres médiatiques individualisées et adéquates.

*« Dans le contexte d'une société de la connaissance technique, les médias numériques font **partie intégrante** de l'environnement quotidien des enfants. La mission éducative des institutions non formelles est donc de promouvoir la compétence médiatique des enfants. Celle-ci rend les enfants aptes à utiliser les différents médias de façon de plus en plus autonome et réfléchie, tant **dans leur intérêt propre qu'au profit d'échanges sociaux ou pour participer à la société**. L'utilisation ludique, créative et pratique des technologies de l'information et de la communication par les enfants plus âgés s'observe notamment dans le développement et l'application d'une langue propre aux jeunes, influencée par le groupe de pairs et qui est surtout utilisée dans la communication numérique (SMS, Internet).*

***La confrontation créative et ludique aux médias numériques** s'étend avec l'âge, lorsque les enfants commencent à les utiliser de manière ciblée comme outils de travail et d'information. La coopération avec les parents permet aux pédagogues de développer des méthodes en fonction des acquis des enfants, de planifier des offres médiatiques complémentaires individuelles et, ainsi, de contribuer à **l'équilibre des chances**. »*[1]

[1] Citation extraite du cadre de référence national sur l'éducation non formelle des enfants et des jeunes, p. 64, édition 2018



✖ Promouvoir les compétences médiatiques – avec ou sans Internet

La promotion des compétences médiatiques peut se faire de différentes manières. Il existe beaucoup de possibilités intéressantes, qui peuvent s'avérer passionnantes à découvrir pour les éducateurs également – en effet, désormais il est normal en tant qu'adulte d'avoir rapidement le sentiment de ne rien comprendre à ce que les enfants et les jeunes semblent maîtriser avec tant de facilité et de naturel.

Il vaut la peine d'apprendre, de préférence dans le cadre de formations continues pratiques et d'ateliers, comment diversifier sa pratique pédagogique en matière de médias ; il s'agit également d'une bonne occasion de partager ses expériences avec des pairs (voir contacts et liens en annexe). De nombreux forums d'échange de connaissances et d'expériences se sont créés sur Internet et il peut s'avérer utile de les parcourir. Il est également possible d'y trouver des idées pour promouvoir les compétences médiatiques des enfants.

De plus, il est très intéressant d'apprendre que des activités dont le but est de promouvoir les compétences médiatiques n'impliquent pas forcément une connexion à Internet, telles que :

▸ la définition, tous ensemble, de règles d'utilisation d'Internet au sein de la Maison Relais ;

▸ des jeux de société didactiques tels que « Tubes » de BEE SECURE ;

▸ d'autres activités et fiches de travail (voir « Leitfaden zur Informationssicherheit » de BEE SECURE)[2]

▸ des activités avec des tablettes, telles que la programmation de jeux vidéo pour ordinateurs avec « Scratch »[3], un langage de programmation adapté aux enfants et destiné aux débutants (aucune connexion Internet requise).

✖ Bien entendu, il existe également nombre d'activités pour lesquelles un accès à Internet est requis :

▸ des offres telles que des « coins ordinateurs » ;

▸ des ateliers ou des projets média (créer des bandes dessinées, des posters, son propre journal) ;

▸ des activités avec tablette (jeux éducatifs, conception créative de matériel audio, visuel, vidéo, création de pièces audio, recherche d'informations, recherches pour les devoirs à domicile...).

[2] www.bee-secure.lu/leitfaden (en allemand)
[3] https://scratch.mit.edu/

I. SÉCURITÉ SIGNIFIE RÉDUCTION DES RISQUES

L'utilisation de TI (technologies de l'information) va toujours de pair avec des risques en matière de sécurité. C'est en quelque sorte « dans la nature de la technologie ». La nature de ces risques et le degré de probabilité que « quelque chose de grave se produise » dépendent de différents facteurs.

EN PRINCIPE, L'OBJECTIF DEVRAIT ÊTRE D'ATTEINDRE LA PLUS GRANDE SÉCURITÉ POSSIBLE DANS LE DOMAINE D'UTILISATION DES TI.[4]

L'on dit volontiers que chaque domaine d'utilisation concret s'accompagne d'une multitude de « scénarios de menace », dont certains sont plus ou moins probables ou réalistes.

Exemple

Les serveurs (= ordinateurs destinés au stockage de données) d'une grande banque, active à l'échelle mondiale, sont davantage exposés à des risques d'actes de criminalité économique ou de piratage, étant donné le stockage massif de données sensibles, que le petit ordinateur destiné à des recherches pour les devoirs à domicile installé dans la salle média d'une Maison Relais.

Toutefois, consentiriez-vous à y sauvegarder vos données bancaires ? Et qu'en est-il des ordinateurs de l'administration de la Maison Relais : quelles données (confidentielles) y sont enregistrées ? Qui a accès aux informations personnelles d'un enfant, telles que son nom, son adresse et les informations sur sa santé ?

[4] Pour davantage de réflexions intéressantes sur le thème de la gestion des risques en matière de sécurité des informations, consultez la page : https://www.cases.lu/gestion-du-risque.html

Seul(s) le(s) responsable(s) de la Maison Relais ? Ou bien également le personnel, voire les stagiaires ou encore toute personne accédant à la pièce ? Mis à part l'exemple frappant du « piratage classique de données », quelles sont les menaces à garder véritablement à l'esprit lors de l'utilisation d'Internet dans la Maison Relais (par l'administration, le personnel éducatif, les enfants, les parents, des visiteurs...) et à l'extérieur (p. ex. accès extérieur aux appareils/données de la Maison Relais via une connexion Internet) ?

Créer un environnement sécurisé consiste donc à trouver un équilibre entre l'utilisation (souhaitée) et les risques (potentiels). Qu'est-ce que cela signifie concrètement pour l'objectif consistant à mettre en place un concept de sécurité Internet dans la Maison Relais ?

Cela signifie qu'en matière de sécurité deux aspects entrent en jeu et permettent, une fois combinés, de garantir une réduction des risques et de maximiser le niveau de sécurité:

1. le comportement des éducateurs/ utilisateurs ;

2. l'aspect technique
Création de zones de réseau séparées, recours à des filtres Internet, sécurité des appareils, maintenance.

Afin de comprendre pourquoi il ne suffit pas d'installer un programme anti-virus pour que les enfants soient « en sécurité » sur Internet et pourquoi un comportement critique de l'utilisateur (ici : l'enfant) d'Internet est si important, le chapitre suivant propose un rapide aperçu des risques auxquels les enfants sont en règle générale confrontés sur Internet.

LES RISQUES LIÉS À INTERNET POUR LES ENFANTS : APERÇU

Les risques au fil du temps

Les enfants sont exposés à certains risques, en particulier lorsqu'ils surfent seuls (ou sans l'accompagnement d'un adulte) sur Internet.

C'est pourquoi BEE SECURE propose depuis plusieurs années des formations de sensibilisation initiale pour une utilisation sécurisée et responsable d'Internet. Il ressort de cette longue expérience et d'échanges avec des experts internationaux que de nouvelles tendances peuvent, le cas échéant, entraîner des risques spécifiques.

LES PRINCIPAUX DOMAINES DE RISQUES POUR LES ENFANTS ET LES ADOLESCENTS SONT TOUTEFOIS PLUTÔT INDÉPENDANTS DE CES TENDANCES PASSAGÈRES.

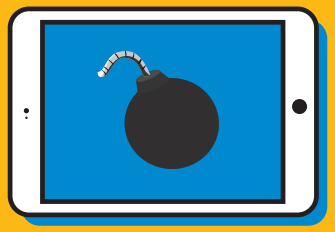
Un exemple : le cyber-harcèlement, c'est-à-dire les insultes intentionnelles, les menaces, la ridiculisation ou l'harcèlement d'autres personnes sur une plus longue période de temps en se servant d'Internet et des services de téléphonie mobile. Ce comportement à l'égard des autres se manifeste sur Internet (p.ex sur les réseaux sociaux, sur les plateformes) et sur les smartphones (p.ex. via les les applications de messagerie instantanée telles que WhatsApp, des appels embêtants, etc.) Particulièrement parmi les enfants et les adolescents, les victimes et les harceleurs se connaissent généralement de l'environnement personnel (« réel ») comme l'école, le quartier résidentiel, le village ou la communauté ethnique. C'est pourquoi le cyber-harcèlement va souvent de pair avec le harcèlement dans le monde hors ligne : d'une part le harcèlement continue en ligne, d'autre part le harcèlement commence en ligne, puis continue dans la vie quotidienne de l'école. C'est la raison pour laquelle, le harcèlement et le cyber-harcèlement sont inséparables dans la majorité des cas.

De tels risques, qui sont également pris en considération par la pédagogie en-dehors du « monde en ligne » ou, du moins, devraient l'être, se retrouvent ainsi « uniquement » sous différentes formes dans l'« univers en ligne » des enfants. Il s'agit donc en fait d'« anciens » risques ayant pris une nouvelle forme.

AU FUR ET À MESURE DE L'AVANCÉE DE LA NUMÉRISATION, D'AUTRES « NOUVEAUX » RISQUES PEUVENT TOUTEFOIS FAIRE LEUR APPARITION ET DOIVENT ÊTRE PRIS EN CONSIDÉRATION DE MANIÈRE DURABLE PAR LA PÉDAGOGIE.

Les jouets connectés en constituent un exemple : certains jouets sont équipés d'un micro, d'une caméra et d'une connexion Internet. Actuellement, toutes les personnes achetant ou utilisant ces jouets, ne sont pas conscientes des risques ou dangers qui peuvent en découler. Cette évolution technologique est relativement récente, mais restera certainement assez longtemps un sujet de préoccupation en termes de sécurité.

Il importe dans un premier temps d'identifier les domaines de risques essentiels pour les enfants et les adolescents qui ont émergé jusqu'à présent.



✖ Les différentes catégories de risques

Afin de disposer d'un meilleur aperçu des risques typiques auxquels les enfants sont exposés sur Internet et de pouvoir dégager les besoins de sécurité qui en découlent, il peut s'avérer utile de définir des catégories de risques :

▸ 1. les risques liés aux contacts (« contact risks ») ;

▸ 2. les risques liés aux contenus (« content risks ») » ;

▸ 3. les risques de consommation (« consumption risks »).

Même si ces trois catégories ne sont pas complètement indépendantes les unes des autres et qu'il peut y avoir des recoupements (certains exemples pourraient appartenir à plusieurs catégories), cette répartition permet de donner une bonne orientation de départ.

RISQUES LIÉS AUX CONTACTS

Lorsque des enfants entrent en contact avec autrui via Internet (contact risk), les principaux risques sont les suivants :

▸ Cyber-harcèlement
Harcèlement via Internet et les services de téléphonie mobile (cf. page 10 pour une description détaillée).

▸ Grooming
Le grooming décrit un processus durant lequel un adulte établit une relation de confiance avec un mineur sur Internet pendant une longue période (semaines ou mois) dans le but de le/la persuader de se livrer à des pratiques sexuelles (en ligne et hors ligne).

▸ Sexting
Le terme « sexting » se compose des mots anglais « sex » (sexe) et « texting » (envoi de messages textuels via SMS). Il décrit l'échange de photos intimes par téléphone mobile ou via les réseaux sociaux. Le plus grand danger du sexting est que ces photos dénudées, censées être un témoignage de confiance privé, circulent tout à coup sur la toile ! Le sexting est un phénomène qui se répand de plus en plus, surtout chez les adolescents et les jeunes adultes.

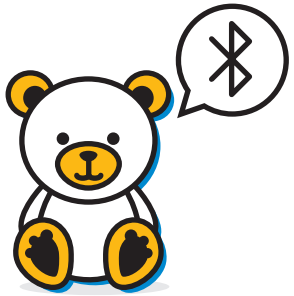
▸ Sextortion
Le terme sextorsion désigne le chantage basé sur du matériel à contenu sexuel (images, vidéos). La victime est amenée à envoyer des photos/vidéos d'elle dans des postures sexuelles et est ensuite soumise à un chantage suite à ces photos, ou alors un chantage est exercé sur la victime par une personne qui prétend disposer d'images embarrassantes d'elle dénudée (obtenues par piratage de l'ordinateur de la victime) et de les publier.

▸ Défis en ligne
Il ne doit pas toujours forcément s'agir d'actes sexuels, d'abus ou de harcèlement lors du contact dangereux avec autrui ; il existe également d'autres risques imaginables et possibles par la manipulation psychologique des enfants.

Les « défis en ligne » sont des jeux dangereux qui sont souvent diffusés via les réseaux sociaux et incitent les participants à des actes impliquant des automutilations qui, dans certains cas, peuvent mener jusqu'à la mise en danger de leur propre vie.

Les phénomènes dangereux de ce type peuvent parfois très vite se transformer en tendances et ainsi être particulièrement attirants pour les enfants et les adolescents.

▸ Chaînes de lettres
Les chaînes de lettres, qui se répandent via des applications de chat, e-mail ou par d'autres voies similaires, sont très fréquentes et constituent donc presque un phénomène quotidien. Souvent, celles-ci sont censées semer la crainte et la panique puisque le destinataire reçoit des menaces s'il ne réalise pas une tâche particulière dans un délai précis (p. ex. retransmettre rapidement le message).



▸ **« Smart toys »**
jouets connectés

Il existe sur le marché de plus en plus de jouets connectés à Internet. Ces « smart toys » peuvent être utiles mais comportent également certains risques. Dans le cas d'ours en peluche connectés (« cloud pet »), des étrangers ont pu, à une distance de 10 m et grâce à la connexion bluetooth du jouet, écouter les discussions de l'enfant avec son ours en peluche ou les conversations tenues dans la pièce.

En outre, il était très simple d'écouter sur Internet les conversations des ménages dans lesquels cet ours en peluche était activé, vu que les fichiers vocaux des peluches étaient envoyés sur un smartphone via bluetooth puis transférés et enregistrés sur un serveur Internet assez vulnérable. Tant du point de vue de la protection de la vie privée que de celui du risque que des étrangers, via des jouets connectés insuffisamment protégés, puissent le cas échéant, établir un contact avec un enfant, ces « smart toys » sont toujours à examiner d'un œil critique.

Il y a lieu de souligner que souvent, ni l'enfant ni les parents n'ont la moindre idée du fait que ces « smart toys » (jouets connectés) sont reliés à Internet. Dès lors, ils n'ont souvent pas du tout conscience des risques qui y sont liés, contrairement aux risques des appareils connectés « traditionnels » (tels qu'ordinateurs, smartphones ou tablettes).[5]

[5] Vous trouverez des conseils utiles à suivre lors de l'achat de tels jouets et des informations détaillées relatives aux risques respectifs sur le site www.bee-secure.lu/fr/factsheet/smart-toys

RISQUES LIÉS AUX CONTENUS

Internet offre de nombreux contenus qui sont inadaptés voire nuisibles pour les enfants. On les trouve sous forme de photos, d'images, de vidéos, de jeux ou encore de textes. Il y a, en outre, lieu de tenir compte du fait que les enfants ne font pas seulement face aux contenus des autres, mais produisent aussi de plus en plus tôt des contenus eux-mêmes.

Les contenus douteux sont notamment les suivants :

▸ **L'abus sexuel des enfants en ligne**

L'abus sexuel des enfants prend une dimension en ligne lorsque, par exemple, des actes de violence sexuelle sur des enfants sont photographiés ou filmés, puis téléchargés et rendus accessibles en ligne, que ce soit pour un usage personnel ou pour le partage avec d'autres personnes. Toute consultation ou chaque partage de ce matériel est considéré comme un délit renouvelé puisqu'il s'agit d'une violation répétée des droits de l'enfant.

Les contenus à abus sexuel des enfants peuvent être signalés à la BEE SECURE Stopline (stopline.bee-secure.lu).

▸ **Pornographie**

Pour les enfants, le contact avec de la pornographie peut s'avérer très problématique pour diverses raisons, en particulier, lorsqu'ils ne sont pas aptes à bien comprendre ce qu'ils ont vu et ressenti à ce moment et/ou lorsque cette expérience leur fait développer une mauvaise représentation de la sexualité.

▸ **Violence**

Il existe également des contenus violents ou des contenus visuels (images/vidéos) qui ne sont pas adaptés aux enfants.

▸ **Influenceurs**

Chez les enfants et les adolescents, on parle désormais d'« influenceurs » qui, sur YouTube ou Instagram par exemple, trouvent une grande audience parmi ces tranches d'âge. Étant donné leur grande importance pour le jeune public, ils peuvent rapidement être considérés comme des sources d'informations fiables, même si derrière ces personnes se mettant en scène se cachent, généralement, des motivations commerciales (revenus liés à la publicité) et, la recherche d'un maximum de clics. Il est donc important que les enfants apprennent également à traiter de façon critique ces « stars » qu'ils considèrent comme leurs modèles.

Tous ces exemples illustrent le fait qu'il peut être bénéfique pour le bien-être des enfants de prévoir au sein de la Maison Relais un local dans lequel, peuvent s'exprimer au sujet d'expériences ou d'un contact avec des contenus (problématiques) sans être jugés et mieux comprendre, avec l'aide d'un éducateur, ce qui a été vu et vécu (faits ou fiction, publicité, compétence relative au contenu des médias).

RISQUES LIÉS À LA CONSOMMATION

Cette catégorie reprend pratiquement tous les risques pouvant résulter d'une inscription sur des applications/plate-formes ou à des services. Voici quelques-uns des risques les plus courants liés à la consommation :

▸ **Risques financiers**
Arnaques, factures de téléphone portable élevées imprévues,...

▸ **Publicité**
Publicité ou information ?
Comment puis-je les distinguer alors que les frontières s'amenuisent de plus en plus ? Les enfants doivent apprendre à gérer le contact avec les différentes formes de publicités, d'influences ou les invitations à réaliser des actions en particulier (p. ex. l'achat de crédits/d'objets virtuels dans une application).

▸ **Qualité et durée de la consommation/de l'utilisation**
L'ampleur (trop importante ou trop faible) de l'utilisation des TI doit toujours être évaluée dans le contexte et/ou en tenant compte également de l'aspect qualitatif. La question : « Pourquoi et comment les technologies de l'information sont-elles utilisées ? » doit toujours être prise en considération dans ce type de discussion afin de favoriser un développement sain - ce qui ne vaut pas uniquement pour les enfants.

▸ **Protection des données et vie privée**
Certain(e)s applications/fournisseurs récoltent, par différents moyens, des données personnelles sur leurs utilisateurs, y compris les enfants et les utilisent et/ou les vendent à des fins commerciales.

L'un des objectifs de l'éducation aux médias devrait être d'aider les enfants à devenir des coacteurs et participants portant un regard critique sur notre société (numérique). Il est important de leur apprendre très tôt à utiliser leurs données personnelles en toute conscience et à en connaître la valeur. En effet, des données supposées non personnelles peuvent dévoiler des informations très personnelles sur une personne (caractère, sentiments, lieu de résidence, etc.). Les applications et services destinés aux enfants doivent dès lors toujours être sélectionnés après avoir fait l'objet d'une analyse critique et être utilisés tout en prêtant attention à la protection des données personnelles.

GARDER UN REGARD POSITIF MALGRÉ LES RISQUES

Cet aperçu des risques montre à quel point il est important de ne pas uniquement protéger les enfants de contenus inappropriés à l'aide de mesures techniques (p. ex. par l'installation de filtres de contenu techniques, comme décrit ci-dessous), mais que l'ensemble des expériences et comportements humains peut jouer un rôle dans la question de la sécurité sur Internet – c'est la raison pour laquelle l'accompagnement pédagogique et le comportement exemplaire personnel sont si importants lors de l'utilisation d'Internet. Puisque ce chapitre porte quasi-exclusivement sur les aspects négatifs d'Internet, voici pour conclure, encore trois réflexions essentielles sous forme de conseils :

Conseil 1 :
Adopter un point de vue équilibré

Conseil 2 :
Vous ne pouvez généralement pas changer les dangers, mais par contre rendre les enfants plus forts

Conseil 3 :
Garder son calme - il existe des solutions pour tout problème

Conseil 1
Adopter un point de vue équilibré
Lors de discussions portant sur les risques, la sécurité et la protection, il peut rapidement arriver que l'on ne se concentre que sur les aspects négatifs/dangereux liés à l'utilisation des TI et que l'on en perde de vue les aspects positifs et utiles. Lorsque vous portez les « lunettes de sécurité », veillez donc à régulièrement réfléchir de manière active à l'aspect positif de l'utilisation des TI et à leur valeur ajoutée afin de conserver une perspective équilibrée.

Conseil 2
Vous ne pouvez généralement pas changer les dangers, mais par contre rendre les enfants plus forts
Rendez-vous à l'évidence que les médias numériques font partie intégrante du quotidien des enfants et que grâce à votre influence positive sur le plan pédagogique, vous contribuez à les rendre plus compétents dans leur utilisation de ces médias. Cela signifie également que vous contribuez à rendre les enfants moins vulnérables ou plus résistants en ce qui concerne les risques/dangers mentionnés ci-dessus.

Conseil 3
Garder son calme - il existe des solutions pour tout problème
Lorsqu'un appareil/une application ne fonctionne pas comme il/elle devrait, lorsqu'un enfant tombe sur une page inappropriée, lorsque vous soupçonnez que votre appareil est infecté par un virus… Gardez votre sang-froid et faites en sorte (dans la mesure du possible) que l'enfant assiste à la manière dont vous tentez de résoudre le problème en question.

La capacité à gérer de manière constructive les problèmes qui se présentent (inopinément) et à développer des stratégies de solution est indispensable dans le « monde numérique » d'aujourd'hui et de demain. Soyez donc conscient que vous pouvez servir d'exemple positif dans ce contexte. Il est également normal que vous vous heurtiez rapidement aux limites de vos connaissances et expériences personnelles. Il vous suffit alors de trouver où, ou auprès de qui, vous pouvez obtenir de l'aide (p. ex. qui est la personne de contact au sein de la Maison Relais).

2. CONSEILS DE SÉCURITÉ POUR LA PRATIQUE

Dans le cas de la Maison Relais, la sécurité sur Internet signifie donc qu'il faudrait garantir la meilleure sécurité possible, ce en fonction des besoins (de protection) des personnes et de leurs données au sein de l'établissement. Que ce soit sur Internet ou ailleurs, comme dans tous les domaines de la vie, la sécurité ne peut jamais être assurée à 100 %. Par conséquent, la sécurité est relative.

Elle dépend de mesures prises ponctuellement et de procédures régulières. Ainsi, la sécurité n'est pas un état, mais un processus.

Afin de garantir la clarté de ce processus pour les Maisons Relais, les conseils de sécurité suivants ont été répartis en cinq grands thèmes :

- **1. Comportement des éducateurs/utilisateurs**
- **2. Mesures techniques**
- **3. Déterminer les responsabilités**
- **4. Fixer des règles et les communiquer**
- **5. Se tenir informé(e)**

1. COMPORTEMENT DES ÉDUCATEURS/UTILISATEURS

La sujet de la sécurité devrait se refléter dans la manière de penser et d'agir des éducateurs/utilisateurs. Le comportement adopté par chacun constitue la protection la plus importante – également lors de l'utilisation d'Internet au sein de la Maison Relais.

Au-delà de toutes les mesures techniques relatives à la sécurité, il conviendrait donc en premier lieu que les responsables et le personnel de l'établissement se basent de préférence sur trois principes d'action en matière d'utilisation d'Internet/d'appareils connectés :

-Principe n°1
Placer la protection des données au centre de ses actions

- Principe n°2
Être conscient de son rôle d'exemple

- Principe n°3
Discuter avec les enfants de leurs activités sur Internet et les accompagner

▸ **Principe n°1**
Placer la protection des données au centre de ses actions

AU NIVEAU DE L'ADMINISTRATION, LA PROTECTION DES DONNÉES EST LA PRIORITÉ ABSOLUE.

Il est impératif de protéger les données confidentielles des enfants et du personnel contre tout accès non autorisé. En cas de questions d'ordre juridique relatives à la protection des données, notamment concernant la conformité légale de sa propre gestion des données, la CNPD[6] est l'interlocuteur privilégié.[7]

Pour se conformer au règlement général sur la protection des données, tout établissement devrait pouvoir prouver qu'il traite les données à caractère personnel de façon responsable et réfléchie, et qu'il stocke et exploite ces données dans le respect des lois. Ce principe vaut pour tous types de stockage et de gestion de données : ainsi, il concerne aussi bien le format numérique qu'analogique (p. ex. l'archivage de documents dans des dossiers).

[6] Commission nationale pour la protection des données, www.cnpd.lu
[7] Le site Web de la CNPD comporte un formulaire de contact, via lequel vous pouvez poser des questions générales et spécifiques aux experts compétents à tout moment. De plus, vous y trouverez des conseils pratiques qui peuvent s'avérer utiles pour les Maisons Relais.

▸ **Principe n°2**
Être conscient de son rôle d'exemple

LE PERSONNEL ÉDUCATIF DEVRAIT ADOPTER UN COMPORTEMENT EXEMPLAIRE, ORIENTÉ SÉCURITÉ ET CONFORME AUX LOIS DANS SA PROPRE UTILISATION D'INTERNET ET DES APPAREILS CONNECTÉS.

L'objectif est, d'une part, de contribuer à la sécurité informatique au sein de la Maison Relais en général et, d'autre part, de donner l'exemple en tant qu'éducateur afin que les enfants puissent apprendre à utiliser correctement les TI et assimiler d'importants réflexes en matière de sécurité, en suivant l'exemple qui leur est donné.

Ce comportement exemplaire implique, dans le cadre de l'utilisation professionnelle (durant les heures de travail), d'utiliser les appareils informatiques (ordinateurs, tablettes, smartphones et autres appareils connectés) et les mots de passe de façon responsable, de traiter les contenus selon une approche réfléchie et critique (textes, vidéos, photos), mais aussi d'adopter une attitude responsable et conforme aux lois lorsqu'il s'agit de prendre/d'enregistrer des photos/vidéos et de les diffuser (droit à l'image, droits d'auteur). Il peut s'avérer très utile de formuler certains points concrets sous forme de règles simples au sein de l'établissement (voir la section « Règles pour le personnel »).

Le personnel devrait également veiller à sa réputation dans le cadre de sa navigation « privée » en dehors des heures de travail, p. ex. sur des réseaux sociaux comme Facebook[8].

[8] Vous trouverez plus d'informations et de conseils à ce sujet dans l'ouvrage *Donner l'exemple dans son usage du numérique* : Guide d'utilisation des réseaux sociaux pour les éducateurs et les enseignants de BEE SECURE (disponible en allemand et en français) : www.bee-secure.lu/fr/guide-exemple

▸ **Principe n°3**
Discuter avec les enfants de leurs activités sur Internet et les accompagner

Surtout en ce qui concerne l'univers Internet, il peut être **particulièrement important que les enfants, encadrés par les éducateurs, apprennent à discuter de leurs propres expériences en rapport avec Internet,** à y réfléchir et à mieux les cerner et comprendre. Ceci peut également s'avérer utile pour assimiler des réflexes fondamentaux en matière de sécurité (p. ex. éviter de divulguer ses données de connexion/mots de passe à autrui) et pour identifier ultérieurement et de façon préventive les situations qui nécessitent de faire appel à ses réflexes en matière de sécurité (p. ex. un joueur inconnu demande à un enfant de lui fournir ses données personnelles lors d'un jeu en ligne ; l'enfant refuse et raconte la situation à ses parents/l'éducateur).

Lorsque les enfants surfent sur Internet à la Maison Relais, ils devraient en principe bénéficier d'un accompagnement pédagogique. Cette approche vise également à ce que l'éducateur devienne un interlocuteur de confiance pour l'enfant qui explore l'univers Internet.

2. MESURES TECHNIQUES

Les recommandations suivantes, de nature générale, peuvent en principe être mises en œuvre au sein de toutes les Maisons Relais. Il convient toutefois de veiller à ce que vos techniciens (internes ou externes) sur place disposent d'une vue d'ensemble précise quant au sens (ou non-sens) des mesures de protection techniques suivantes et à la possibilité de leur mise en œuvre au sein de votre établissement spécifique et vous présentent, si nécessaire, d'autres propositions ou solutions. Ces autres solutions sont tout à fait envisageables, tant qu'elles tiennent compte des besoins du personnel et des données propres à l'établissement. « Tous les chemins mènent à Rome » – or, les chemins suivants vous y conduiront sans trop d'escales.

Il convient de prendre les trois mesures techniques de protection suivantes :

- Mesure de protection n°1
Sécuriser l'accès à Internet

- Mesure de protection n°2
Créer des zones de réseau séparées (enfants, personnel)

- Mesure de protection n°3
Utiliser des filtres Internet

▸ Mesure de protection n°1
Sécuriser l'accès à Internet

Dans certains établissements, l'accès à Internet est fourni par l'école à proximité, la commune et/ou un autre fournisseur, et est peut-être même déjà configuré selon des prescriptions de sécurité adéquates. Par conséquent, il peut être utile de se renseigner concernant les solutions en matière de sécurité que l'école/la commune/ou d'autres acteurs et établissements pertinents ont choisies, et de déterminer si ces solutions pourraient s'appliquer à la Maison Relais, et de quelle manière.

Alternativement, il est également possible de collaborer avec une entreprise externe qui pourra prendre en charge l'installation technique, mais aussi, le cas échéant, la maintenance et d'autres services qui seront évoqués par la suite (création d'une liste noire ou d'une liste blanche de sites Internet, répartition du réseau en différentes zones, etc.).

Il conviendrait d'empêcher tout accès non autorisé au réseau par des tiers à l'aide de mesures de sécurité courantes. Cela signifie que pour le Wi-Fi, il faudrait utiliser un réseau WLAN crypté (WPA2) et un mot de passe sécurisé pour y accéder, et pour le réseau relié au câble (LAN), il faudrait veiller au contrôle par port/filtrage par adresse Mac.

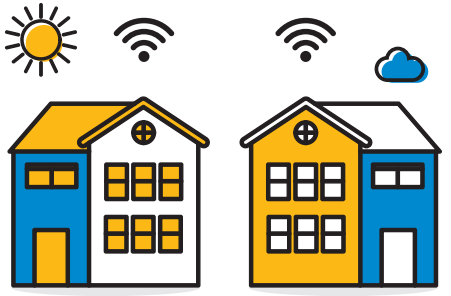
▸ Mesure de protection n°2
Créer des zones de réseau séparées (enfants, personnel)

Pour un contrôle efficace de l'accès aux informations, il convient au préalable de diviser le réseau interne en zones de réseau séparées pour différents groupes d'utilisateurs : une pour les enfants et une pour le personnel. La création d'une troisième zone destinée aux visiteurs peut être envisagée si nécessaire. Deux zones de réseau pour les enfants et le personnel devraient toutefois suffire dans la plupart des Maisons Relais.

En quoi cette division du réseau est-elle importante ?

Lorsque tous les appareils de l'établissement (PC, tablettes, PC portables, imprimantes, etc.) sont connectés au même réseau, ils peuvent en principe accéder les uns aux autres ou communiquer entre eux. D'ailleurs, il est possible de désactiver cette communication entre les appareils avec la plupart des routeurs/points d'accès ; en ce qui concerne les réseaux reliés au câble, il est également possible d'effectuer les réglages correspondants à l'aide de pares-feux afin de limiter cette communication dans la mesure souhaitée.

Dans tous les cas, il faudrait faire en sorte que les enfants ne puissent pas accéder aux ordinateurs de l'administration via leurs appareils connectés (p. ex. tablettes et PC) ni communiquer avec d'autres appareils du réseau (comme une imprimante de l'administration du personnel) de



façon abusive. Il ne s'agit pas seulement d'empêcher les enfants de semer la pagaille : le but est surtout de limiter les risques liés aux logiciels malveillants (virus ou malwares) et aux pirates informatiques, qui pourraient, si aucune mesure n'est prise, accéder sans difficulté à l'ensemble des appareils du réseau via les appareils des enfants.

D'un point de vue technique, il existe différents moyens de créer des zones séparées, p. ex. en configurant des règles de pare-feu spécifiques ou en installant deux ou plusieurs routeurs en série.

La création de plusieurs zones de réseau permet à toutes les personnes concernées d'utiliser Internet et les systèmes informatiques selon leurs besoins et leurs compétences au sein de la Maison Relais. Ces zones sont liées à différentes libertés, en fonction des rôles de leurs utilisateurs.

La première zone, nommée « Enfants », engloberait l'accès à Internet pour tous les appareils susceptibles d'être utilisés par les enfants. Cette zone utilisée par les enfants, sous surveillance des éducateurs, ne pourrait en aucun cas contenir des informations ou des données personnelles. Elle servirait à utiliser des appareils connectés dans le cadre d'activités pédagogiques. L'accès à Internet pour les enfants serait filtré (voir « Internet filtré »). L'objectif est d'empêcher les mineurs d'entrer en contact avec des contenus dangereux ou illégaux.

La deuxième zone « Personnel éducatif » serait réservée aux salariés permanents (donc interdit aux intérimaires et aux stagiaires), car elle permettrait d'accéder à des informations personnelles. Il est absolument nécessaire que le personnel éducatif se connecte au réseau avec un mot de passé sécurisé. Les données de connexion ne peuvent en aucun cas être divulgées aux enfants ou à des tiers autres que les personnes habilitées ; l'objectif est d'empêcher tout abus ou toute violation de la protection des données.

La troisième zone est facultative, la « zone intermédiaire ». Elle serait la zone la plus « adaptable » aux besoins individuels. Ainsi, elle peut être réservée aux collaborateurs non permanents ou encore aux visiteurs, qui disposent de plus de libertés au sein du système informatique. Cette zone empêche l'accès à des informations personnelles. Il est possible de la configurer individuellement, selon les besoins actuels.

Suivant les locaux et les besoins, l'utilisation d'un **hotspot Wi-Fi** délimité physiquement peut également s'avérer intéressante. Il est possible de le configurer localement de façon à ce que, par exemple, les enfants ne puissent accéder à Internet sur des tablettes (sur lesquelles l'accès ne se fait généralement pas à l'aide d'un câble LAN, mais bien uniquement via le Wi-Fi ou une connexion sans fil) que dans un local média spécialement prévu à cet effet. En dehors de ce local, les enfants ne pourront donc pas accéder à Internet, ce qui, dans la pratique et selon les caractéristiques des locaux, pourra faciliter l'encadrement continu des enfants lorsque ceux-ci surfent sur la toile.

Pour empêcher tout accès non autorisé par des utilisateurs non habilités, les deux ou trois zones seront strictement séparées les unes des autres. Il est recommandé que chaque utilisateur s'identifie à l'aide d'un nom d'utilisateur et d'un mot de passe. Cela permet de déterminer qui a eu accès à quelle zone, et à quel moment.

La segmentation du réseau est une mesure essentielle pour garantir le contrôle d'Internet et la sécurisation des processus informatiques au sein de la Maison Relais. Elle permet d'attribuer des droits personnalisés à l'aide de moyens simples, facilitant ainsi la sécurisation de l'accès à Internet, l'accès à des informations et la protection préventive contre les malwares (programmes malveillants, comme les « virus classiques »).

▸ **Mesure de protection n°3**
Utiliser des filtres Internet pour les enfants

L'USAGE DE « FILTRES INTERNET » PERMET D'EMPÊCHER LES ENFANTS D'AVOIR UN ACCÈS DIRECT À DES CONTENUS NUISIBLES AU SEIN DE LA MAISON RELAIS.

Il existe deux types de filtre : les **listes noires** et les **listes blanches**.

✖ Liste noire :
Cette liste répertorie certains sites Internet ou noms de domaines afin qu'ils soient bloqués pour les utilisateurs, en l'occurrence les enfants. Dès lors, ces listes noires sont par exemple recommandées dans les Maisons des Jeunes. La configuration d'un tel filtre peut également être conseillée comme mesure fondamentale pour l'accès à Internet au sein de l'établissement (également pour les adultes), étant donné que tout contenu illégal/dangereux est automatiquement bloqué. Certaines de ces listes noires sont même gratuitement mises à la disposition des écoles ou des établissements d'enseignement.[11]

✖ Liste blanche :
Pour les enfants de moins de 12 ans, l'utilisation d'une liste blanche peut toutefois s'avérer plus adaptée dans bon nombre de cas, puisqu'elle est nettement plus facile à mettre en place et qu'en plus, elle offre « davantage de protection » qu'une liste noire. Une liste blanche répertorie les pages ou domaines auxquels l'utilisateur (donc l'enfant) peut accéder. Toutes les pages ou tous les domaines qui ne font pas partie de cette liste sont en principe bloqués. Cela signifie par exemple que les fenêtres publicitaires qui proviennent souvent de pages (serveurs) externes ne s'afficheront pas. Cependant, les contenus adaptés aux enfants qui proviennent de serveurs externes sont eux aussi, dans un premier temps bloqués par le filtre. Il est toutefois possible, selon le filtre, d'ajouter ultérieurement d'autres pages à la liste blanche.[12]

[11] Exemple de liste noire : http://www.shallalist.de
[12] Une liste blanche répertoriant environ 200 sites adaptés aux enfants est disponible à l'adresse www.bee-secure.lu/beefilter

Une solution « Do it yourself » pour la configuration d'une « liste blanche » a été développée et testée dans le cadre du projet pilote « Secure MR Dippach » : le « BEE Filter ». Celui-ci se compose en quelque sorte d'un mini-ordinateur (Raspberry Pi). Connecté comme un petit serveur pour l'accès des enfants à Internet, il filtre l'accès selon les sites web répertoriés sur la liste blanche pour enfants. Il a pour avantage d'être peu onéreux (environ 70€) ; de plus, il peut être paramétré par le gestionnaire des appareils de l'établissement lui-même ou par une autre personne compétente.[13]

La mise en place et la prise en charge de cette solution devraient de préférence être confiées à une personne à l'aise en technologies. Par conséquent, le « BEE Filter » se prête à des établissements au sein desquels une personne dotée de ces capacités travaille sur place ou est disponible, et qui cherchent une solution peu coûteuse.

[13] Vous trouverez des instructions techniques incluant une liste blanche à l'adresse suivante : www.github.com/msilvoso/beefilter

Bon à savoir :
En cas d'accès filtré, l'enfant découvre un Internet « irréel » et limité artificiellement, ce qui, selon la situation (âge et stade de développement de l'enfant, objectif pédagogique d'une activité), peut être considéré comme judicieux ou non.

L'établissement peut alors envisager de filtrer l'accès à Internet pour tous les enfants à l'aide d'une liste blanche, mais de débloquer certaines pages temporairement en fonction de la situation/de l'enfant ou de permettre à certains enfants d'utiliser temporairement certains appareils dans la zone intermédiaire (qu'il conviendrait en principe de protéger par une liste noire et qui permet à l'enfant de surfer sur le « véritable Internet » en étant accompagné). Selon l'activité ou l'objectif pédagogique et le degré de maturité des enfants, ceux-ci peuvent bénéficier d'un apprentissage personnalisé (p. ex. apprendre, à l'aide d'exemples, à faire la distinction entre une publicité et des informations).

3. DÉTERMINER LES RESPONSABILITÉS

Différentes possibilités peuvent être envisagées pour désigner qui peut s'occuper du volet technique au sein de l'établissement. Cependant, la sécurité sur Internet relève toujours de la responsabilité de la direction de l'établissement.

Les solutions suivantes peuvent être recommandées :

Un « gestionnaire des appareils » au sein de l'établissement
Désignez une personne compétente (et un remplaçant) qui assumera la fonction de gestionnaire des appareils pour les équipements terminaux (ordinateurs, tablettes, PC portables, appareils connectés...) de l'établissement. Cette personne jouera le rôle d'interlocuteur interne en cas de problèmes techniques avec les appareils utilisés par les enfants (ordinateurs, tablettes, etc.) et le réseau afférent. Suivant les compétences de cette personne, elle pourra elle-même prendre en charge les tâches suivantes ou veiller à leur exécution **RÉGULIÈRE** :

▸ Mises à jour
(des systèmes d'exploitation/logiciels)

▸ Sauvegarde de données importantes
(« backup »)

▸ Établir une gestion sécurisée et adéquate des mots de passe (protéger l'accès aux comptes des utilisateurs et aux appareils par des mots de passe, administrer les mots de passe si nécessaire, sensibiliser les utilisateurs à une utilisation appropriée des mots de passe et leur fournir une assistance)

▸ Éliminer les données superflues sur les appareils utilisés en commun (supprimer les données/logiciels inutilisés ou sans importance)

▸ Garder un œil sur les droits d'accès (qui peut installer un programme sur un appareil ? Qui peut accéder à quelles données ?)

Option complémentaire :
La télémaintenance au sein de l'établissement
Selon la situation, la maintenance des appareils, comme les tablettes, peut également (et de façon complémentaire) s'effectuer par télémaintenance. Dans ce cadre, le technicien accède à distance aux appareils de la Maison Relais via Internet, les gère selon les logiciels utilisés et définit les paramètres de filtrage. Pour les tablettes, il existe à présent des logiciels qui permettent p. ex. de bloquer le téléchargement de certaines applications. Ce mode de gestion des appareils ou du réseau est fréquemment utilisé dans les écoles.

4. FIXER DES RÈGLES ET LES COMMUNIQUER

Il ne suffit pas d'établir des règles relatives à l'utilisation des ordinateurs, des tablettes et d'Internet : encore faut-il les communiquer clairement à toutes les personnes concernées. Certains établissements ont déjà fixé leurs règles en matière de navigation sur Internet. Il est utile de vérifier et de revoir ces règles régulièrement et de veiller à ce que l'ensemble du personnel les connaisse.

Au lieu de proposer ici des règles détaillées, ce guide conseille d'établir des règles personnalisées en fonction des spécificités concrètes de la Maison Relais. Cependant, pour vous donner un coup de pouce, la section suivante reprend quelques thèmes qu'il conviendrait d'aborder dans les règles.

▸ **Règles pour le personnel**
Pour le personnel, il conviendrait d'établir des règles fondées sur les trois principes susmentionnés (protection des données, modèle, accompagnement). Il importe que tous les éducateurs comprennent que

CHAQUE UTILISATEUR PARTAGE LA RESPONSABILITÉ DES APPAREILS ET DOIT TRAITER LES DONNÉES PERSONNELLES ET UTILISER LES APPAREILS DE FAÇON CONSCIENCIEUSE

même si un « gestionnaire des appareils » interne surveille déjà les appareils et veille à leur maintenance régulière.

Les règles devraient viser à formuler clairement certaines thématiques importantes, surtout en ce qui concerne la gestion/l'utilisation :

- des données personnelles
  (numériques ou sur format papier)
- des mots de passe/accès
- des e-mails
- des smartphones (personnels)
  sur le lieu de travail
- des photos et des vidéos

D'autres thèmes se dégageront sans doute des réalités internes à l'établissement. Faites en sorte que les règles soient claires et faciles à respecter. Pour les Maisons des Jeunes, BEE SECURE a formulé en 2013 des règles à l'attention des éducateurs, dont les Maisons Relais peuvent également s'inspirer si nécessaire.[14]

Il peut être particulièrement utile de discuter de ces règles lors de réunions du personnel régulières et, à cette occasion, de dresser régulièrement un bilan intermédiaire. Cela permet de garantir que les règles correspondent toujours aux nouvelles évolutions (techniques) et à d'autres facteurs pertinents, et restent judicieuses.

[14] Vous trouverez le modèle sur la page www.bee-secure.lu/fr/secure-MJ

▸ Règles pour les enfants

Règles relatives à la navigation sur Internet
Pour les enfants, il est recommandé d'établir des règles concernant l'utilisation d'Internet. BEE SECURE propose de familiariser les enfants avec les 10 règles d'or relatives à l'utilisation d'Internet par les enfants » (voir annexe), qui constituent un bon point de départ. Le message le plus important de ces règles est que **les enfants devraient considérer les éducateurs de la Maison Relais comme leurs interlocuteurs pour toute question ou tout problème et qu'ils devraient pouvoir en parler librement, sans craindre d'être punis.**

Permis Internet – oui ou non ?
Un « permis de surfer » peut s'avérer un excellent outil lorsqu'il s'agit d'autoriser les enfants à surfer de façon classique ou à parcourir Internet librement. Deux versions en ligne de ces permis sont disponibles sur la plateforme pédagogique « internetabc.de »[15].

Elles peuvent être utilisées à titre de jeu éducatif ou comme « examen », à la manière d'un petit test du permis de conduire, qui servirait en fait de base pour autoriser ou non les enfants à surfer sur Internet au sein de la Maison Relais. Il convient ici d'évaluer ce qui, d'un point de vue pédagogique, peut s'avérer pertinent et réalisable dans la pratique quotidienne, puisque cela dépendra fortement des réalités spécifiques de l'établissement.

Le « petit examen du permis de surfer » dure environ 15-20 minutes et s'adresse plutôt à des enfants âgés, entre 9 et 12 ans. Le grand permis est un peu plus difficile que le petit et dure entre 30 et 60 minutes.

Règles relatives à l'utilisation des appareils
En outre, il est judicieux, pour garantir une utilisation correcte des appareils (ordinateurs, tablettes, etc.) de fixer des règles internes, de préférence avec la participation active des enfants. Cette activité constituera une bonne entrée en matière.[16]

[15] www.internet-abc.de/kinder/lernen-schule/surfschein (en allemand)
[16] Pour inspiration : www.mediennutzungsvertrag.de (en allemand)

× 5. SE TENIR INFORMÉ(E)

DANS LE DOMAINE DE L'ÉDUCATION AUX MÉDIAS, IL IMPORTE, COMME MENTIONNÉ PRÉCÉDEMMENT, DE SE TENIR INFORMÉ.

▸ Sources utiles
Vous trouverez une liste des sites Web/portails utiles en annexe. Le site Web de BEE SECURE[17] regorge d'informations et d'astuces intéressantes, spécialement pour le Luxembourg, à l'attention des éducateurs, des enseignants et des parents sur des thèmes généraux et actuels en rapport avec la sécurité sur Internet, qui sont pertinents aussi bien pour la pratique pédagogique que pour l'usage privé.

▸ Formation et perfectionnement
Il est particulièrement recommandé d'organiser régulièrement des formations, au cours desquelles le personnel éducatif aura non seulement la possibilité d'approfondir ses connaissances relatives à la sécurité des enfants sur Internet et à son usage personnel, mais aussi d'échanger avec des pairs. Sur le site Web de BEE SECURE, il est possible d'introduire des demandes de formation via le formulaire de contact.[18]

En outre, les formations continues relatives à l'éducation aux médias sont vivement recommandées. Les participants peuvent y tester et découvrir des activités (créatives) concrètes en rapport avec Internet et des appareils connectés pour leur propre pratique (voir les portails relatifs aux formations continues en annexe).

[17] www.bee-secure.lu/fr
[18] www.bee-secure.lu/fr/form

LES 10 RÈGLES D'OR DESTINÉES AUX ENFANTS POUR UNE UTILISATION D'INTERNET EN TOUTE SÉCURITÉ

1. Sur Internet, je me montre courtois, respectueux et je n'insulte personne.

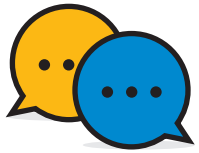
2. Sur Internet, je ne révèle pas mes informations personnelles. Je ne divulgue à personne mon vrai nom, mon adresse, mon numéro de téléphone portable et des informations sur mes amis et ma famille.

3. Je garde secret mes mots de passe/codes et ne les communique à personne – même pas à mes amis. Astuce : « Je crée un mot de passe à partir d'une phrase et le protège comme un trésor ».

4. Si un internaute souhaite me rencontrer, j'en avertis directement mes éducateurs et mes parents.

5. Si quelqu'un se montre méchant envers moi ou d'autres personnes, j'en avertis mes éducateurs et demande de l'aide. Je peux trouver de l'aide et obtenir des conseils gratuitement et de façon anonyme auprès de la BEE SECURE HELPLINE (8002-1234). Si je demande de l'aide, je ne dois pas avoir peur d'être puni.

6. Si l'on m'envoie des informations ou des images désagréables, j'en avertis mes éducateurs et mes parents immédiatement. Je ne dois ni avoir peur, ni être gêné de le faire. Si cette situation m'arrive, ce n'est pas de ma faute.



7. Je parle régulièrement avec mes éducateurs et mes parents de ce que je fais sur Internet.

8. Je ne peux pas partager ou envoyer des photos ou vidéos d'autres personnes sur Internet ou avec un smartphone/une tablette sans leur autorisation.

9. Réfléchir avant de cliquer ! J'utilise Internet et des appareils comme les smartphones, les ordinateurs et les tablettes avec prudence et à des fins utiles.

10. Si je souhaite faire des photos ou des vidéos d'autres enfants ou d'adultes, je dois toujours leur demander la permission avant. Si quelqu'un m'autorise à faire des photos ou des vidéos, elles ne doivent pas être embarrassantes. De même, les autres doivent d'abord me demander la permission avant de me prendre en photo/vidéo.

ANNEXE

Points de contact

BEE SECURE:
▶ www.bee-secure.lu/fr

Commission Nationale pour la Protection des Données (CNPD):
▶ www.cnpd.public.lu

BEE CREATIVE:
▶ www.bee-creative.lu

BEE SECURE HELPLINE: 8002 1234
▶ *La BEE SECURE Helpline offre gratuitement aux enfants, adolescents, parents et éducateurs des conseils et une orientation concernant toutes les questions relatives à l'usage des nouveaux médias.*

Portails de formation continue pour les éducateurs

▶ www.bee-secure.lu/formations

▶ www.enfancejeunesse.lu

▶ www.ifen.lu

▶ www.salto-youth.net

Liens utiles

Plan de sécurité « Secure MJ » pour les Maisons des Jeunes
▶ www.bee-secure.lu/fr/secure-MJ

Liste blanche de sites adaptés aux enfants
▶ www.bee-secure.lu/beefilter

Guide pédagogique pour le développement de la compétence aux nouveaux médias et de la sécurité de l'information (en allemand)
▶ www.bee-secure.lu/leitfaden

Publications de BEE SECURE
▶ www.bee-secure.lu/fr/publications

Formulaire de contact pour les formations BEE SECURE
▶ www.bee-secure.lu/fr/form

Conseils utiles à suivre lors de l'achat de jouets connectés et des informations détaillées relatives aux risques
▶ www.bee-secure.lu/fr/factsheet/smart-toys

Guide pratique de la CNPD pour le monde associatif relatif à la protection des données – également utile pour les Maisons Relais
▶ www.cnpd.public.lu/fr/actualites/national/2018/06/guidance-associations.html

Description technique du « BEE Filter » sur github
▶ www.github.com/msilvoso/beefilter

Exemple de liste noire gratuite
▶ www.shallalist.de

Offres d'ateliers dans le Makerspace « Base1 » de BEE CREATIVE, qui s'adressent également à des groupes d'enfants des Maisons Relais
▶ www.base1.lu/workshops

Permis de surfer (en allemand)
▶ www.internet-abc.de/kinder/lernen-schule/surfschein

Programmation et création d'histoires de jeux par les enfants (en plusieurs langues)
▶ www.scratch.mit.edu

Règles de maniement des équipements
▶ www.mediennutzungsvertrag.de (en allemand)

Notes

Notes

www.bee-secure.lu