Futé
Vigilant
Secret
Sympa
Courageux

Les Cyber Héros

Dossier pédagogique pour aborder la sécurité en ligne et la citoyenneté numérique avec les 8-14 ans

Dossier pédagogique
édité par Bibliothèques Sans Frontières
en 2024

Les
Cyber Héros

Bienvenue dans le programme « Les Cyber Héros » issu d'une collaboration entre Google, Bibliothèques Sans Frontières, Test Achat et Child Focus.

Ce dossier pédagogique est spécialement conçu pour inculquer aux enfants les compétences clés pour surfer sur internet de manière réfléchie et sécurisée. Il fournit aux enseignants les outils et méthodologies nécessaires pour aborder le thème de la citoyenneté numérique en classe.

Les cinq piliers de la citoyenneté et de la sécurité numériques – détaillés dans la charte des Cyber Héros – sont :

- **Réfléchis bien avant de partager** : protéger son empreinte numérique et communiquer responsablement sur les réseaux sociaux.
- **Ne tombe pas dans le panneau** : se méfier de l'hameçonnage, des escroqueries, des fake news et vérifier la crédibilité des sources.
- **Un secret, c'est sacré** : promouvoir la sécurité en ligne et les mots de passe sécurisés.
- **Être gentil, c'est cool** : lutter contre les mauvais comportements en ligne et le cyberharcèlement.
- **Si tu as un doute, parles-en** : encourager le dialogue en cas de problème.

Les activités de ce dossier sont classées en fonction desdits piliers des Cyber Héros et sont destinées à un usage autonome, c'est-à-dire qu'elles requièrent très peu de préparation de la classe en amont et aucun équipement particulier.

Le programme est essentiellement destiné aux élèves de 4e primaire jusqu'à la 6e primaire. Cependant, les enseignants donnant cours à des élèves plus jeunes ou plus âgés peuvent également y trouver du contenu utile, notamment le vocabulaire clé, les discussions en classe (en fonction de l'âge) et les jeux. Nous vous encourageons à tester différentes méthodes pour trouver ce qui convient le mieux à vos élèves ; soit en suivant le programme du début à la fin, soit en approfondissant l'une ou l'autre leçon en fonction des besoins de la classe.

Les compétences abordées à travers l'univers des Cyber Héros seront prochainement incluses dans les programmes scolaires en Fédération Wallonie-Bruxelles et permettent de travailler celles définies par DIGCOMP, le cadre de référence européen des compétences numériques.

Pour compléter le programme, vous trouverez des ressources pédagogiques supplémentaires destinées aux enseignants, aux parents et aux enfants sur le site de Bibliothèques Sans Frontières : www.bibliosansfrontieres.be - par exemple de nouvelles fiches d'activités, des cahiers d'activités à imprimer, un guide pour les parents ou des conseils pour la maison.

Si vous désirez de plus amples informations sur Les Cyber Héros, les contenus disponibles ou les formations dispensées dans le cadre du programme, n'hésitez pas à nous contacter par mail à l'adresse suivante : cyberheros@bibliosansfrontieres.be.

À vous de jouer !

Google

Bibliothèques Sans Frontières
Libraries Without Borders

Sommaire

Guide de l'enseignant

Thématique 1 : Réfléchis bien avant de partager

Thématique 2 : Ne tombe pas dans le panneau

Thématique 3 : Un secret, c'est sacré

Thématique 4 : Être gentil, c'est cool

Thématique 5 : En cas de doute, parles-en

BONUS

Guide de lecture du programme

« Les Cyber Héros » est un outil flexible que vous pouvez adapter aux besoins spécifiques de votre classe. Vous pouvez moduler à souhait chaque leçon en fonction du temps à disposition et du groupe d'élèves. En fonction de la personnalité de vos élèves, vous pouvez, par exemple, leur demander de réaliser l'activité en sous-groupes plutôt que d'animer l'activité avec la classe entière. Nous sommes certains que vous serez capable de laisser libre cours à votre créativité pour adapter le programme selon vos besoins. Place à vos super pouvoirs de prof !

Quelques points d'attention concernant le programme :

1. Chaque module contient une liste des mots de vocabulaire qui sont repris tout au long des leçons. Vous pouvez imprimer cette liste et la distribuer à vos élèves.

2. Le nombre de leçons varie d'un module à l'autre. Chaque leçon est structurée de la même façon :
   - **Objectifs des élèves**
   - **Discussion** (informations générales pour l'enseignant, qui permettent d'en savoir plus sur l'activité ou le thème - en fonction de l'activité, vous pouvez choisir de lire le texte à titre informatif ou vous en servir comme base de discussion avec vos élèves)
   - **Activité** (prêtez attention à l'âge recommandé pour certaines activités)
   - **Conclusion** (résumé du contenu de la leçon et pistes de réflexion)

3. En regard de l'intitulé de chaque leçon, vous trouverez un écusson indiquant l'âge recommandé des élèves.

4. Vous pouvez utiliser ce programme de deux façons : soit en suivant les leçons une par une selon l'ordre pré-établi, soit en décidant vous-même de l'ordre des leçons en fonction des besoins d'apprentissage propres à votre classe. L'ordre des modules a été pensé pour des élèves qui ne possèdent aucune connaissance en la matière et démarrent de zéro, mais la plupart des élèves de primaire ont déjà des notions de base et peuvent vous faire part de leurs lacunes dans certains domaines et des points qu'ils souhaitent approfondir. Vous pourriez commencer par entamer un dialogue avec eux pour comprendre leurs habitudes en matière de navigation internet. Nous espérons que vous passerez d'excellents moments tous ensemble à la conquête du titre de **Cyber Héros** !

Modèle d'email ou de lettre de présentation aux parents

Cher(s) parent(s),

Lorsque nos enfants sont encore petits, nous faisons de notre mieux pour les accompagner dans leur découverte du monde numérique tout en veillant à leur sécurité en ligne. Lorsqu'ils entrent dans l'adolescence, nous leur apprenons à naviguer sur internet et à utiliser le numérique de manière sécurisée et réfléchie.

Nous pensons, dans notre établissement, qu'il est crucial d'accompagner et encadrer nos élèves afin qu'ils :

- **développent leur esprit critique et fassent preuve de discernement** face aux applications, aux sites internet et autres contenus numériques.
- **apprennent à se protéger** contre les risques en ligne, tels que le cyberharcèlement et l'escroquerie.
- **partagent les informations en ligne** de manière plus réfléchie : quel contenu, quand et avec qui ?
- **fassent preuve de gentillesse et de respect** envers les autres et leur vie privée.
- **osent demander de l'aide** à une personne de confiance dans les situations délicates.

Cette année, notre école s'investira dans ce domaine à travers l'initiative 'Les Cyber Héros', un programme spécialement conçu pour inculquer aux enfants les compétences dont ils ont besoin pour surfer sur Internet de manière sécurisée. L'un de ces outils est Interland, un jeu en ligne interactif et éducatif relatif à la sécurité sur Internet, accessible depuis n'importe quel navigateur. Vous pouvez aussi y jouer à la maison (votre enfant sera sûrement ravi de vous montrer comment ça marche).

Le programme « Les Cyber Héros » propose une méthode pédagogique ludique, adaptée en fonction du niveau scolaire et articulée autour de cinq thématiques fondamentales :

- Réfléchis bien avant de partager
- Ne tombe pas dans le panneau
- Un secret, c'est sacré
- Être gentil, c'est cool
- Si tu as un doute, parles-en

Un emploi intelligent et sécurisé de la technologie représente un enrichissement pour tout environnement d'apprentissage et peut aider les établissements scolaires à améliorer leur fonctionnement et la réalisation de leur objectif d'éveil à la citoyenneté. Nous sommes convaincus que le programme 'Les Cyber Héros' peut nous aider à faire en sorte que les élèves de (nom de l'établissement) utilisent le Net pour apprendre et explorer en parfaite sécurité.

Cela vous intéresse ? Nous nous ferons un plaisir de vous informer plus en détail à propos de ce nouveau programme et des outils que vos enfants peuvent aussi éventuellement utiliser à la maison. Et comme la communication reste la meilleure des préventions, nous vous encourageons à discuter ouvertement avec eux de ce qu'ils ont appris. Qui sait, peut-être glanerez-vous aussi des informations utiles à propos de la confidentialité et de la sécurité en ligne.

Cordialement,

[votre nom]

Questions fréquentes

Les élèves ont-il besoin d'une adresse mail pour suivre les activités ?
Non. Par ailleurs, le dossier pédagogique "Les Cyber Héros" est accessible à tous depuis www.bibliosansfrontieres.be. Aucune adresse e-mail ni aucun nom d'utilisateur ou mot de passe ne sont nécessaires.

Quelles sont toutes les URL nécessaires ?
- Pour accéder à la page d'accueil du programme "Les Cyber Héros", rendez-vous sur https://www.bibliosansfrontieres.be/cyber-heros/
- Pour accéder au jeu Interland, rendez-vous sur https://beinternetawesome.withgoogle.com/fr_be/interland
- Pour accéder au dossier pédagogique "Les Cyber Héros", rendez-vous sur https://www.bibliosansfrontieres.be/ressources/cyber-heros-pour-les-enseignants/

Ai-je besoin d'une formation spéciale ? Faut-il être professeur d'informatique pour dispenser ces thématiques ?
N'importe quel enseignant de la maternelle à la 6e secondaire peut dispenser ces thématiques à ses élèves. Aucune formation supplémentaire n'est nécessaire. Le dossier pédagogique s'adresse aussi à tous les professionnels de l'éducation et aux bibliothécaires.

À quels âges ce dossier pédagogique est-il le mieux adapté ?
Le programme complet, y compris le dossier pédagogique, le jeu et les ressources sur le site Web, ont été développés pour des élèves âgés de 8 à 14 ans. Toutefois, selon la façon dont l'enseignant adapte le dossier, les sujets abordés peuvent être utiles à n'importe quelle classe.

Faut-il impérativement couvrir les discussions et activités avant de jouer à Interland ?
Non, mais nous vous recommandons effectivement de le faire avant de jouer. Le jeu Interland est plus constructif lorsqu'il reprend les sujets traités dans le dossier. De même, il sera plus plaisant que les élèves puissent dialoguer avec vous et réfléchir avant d'y jouer.

Les élèves peuvent-ils enregistrer leur travail sur Interland ?
Pas dans la version actuelle, et cela ne changera probablement pas. Le programme ne génère ni ne stocke aucune information personnelle, y compris des fichiers de sauvegarde. Ceci est totalement délibéré. Nous voulons que le contenu soit accessible à tous, sans qu'il soit nécessaire d'avoir un compte, un nom d'utilisateur ou un mot de passe.

Où puis-je trouver d'autres ressources destinées aux enseignants ?
Tous les documents destinés aux enseignants dans le cadre de ce programme sont disponibles sur notre page des ressources à l'adresse : https://www.bibliosansfrontieres.be/ressources/cyber-heros-pour-les-enseignants/

Je souhaite obtenir de l'aide ou des renseignements ?
C'est simple, contactez-nous à l'adresse cyberheros@bibliosansfrontieres.be

Définitions et cadre légal

Citoyenneté Numérique
« Un citoyen numérique est une personne qui est capable, parce qu'elle a acquis un large éventail de compétences, de participer de façon active, positive et responsable, aux communautés en ligne et hors ligne, au niveau local, national ou mondial. Les technologies numériques étant par nature en constante évolution, l'acquisition des compétences nécessaires est l'affaire de toute une vie et devrait commencer dès l'enfance, à la maison et à l'école, dans des contextes éducatifs formels, informels et non formels. »
– Le Conseil de l'Europe

Droit à l'image
L'autorisation d'une personne doit être demandée pour fixer, exposer, communiquer ou reproduire son image sur internet, dans un journal ou dans un magazine. En ce qui concerne les mineurs, l'autorisation des parents ou du tuteur légal est nécessaire et, à partir du moment où la personne représentée a atteint l'âge de la raison, la personne mineure doit donner ce consentement avec ses parents ou son tuteur légal.

Droit à l'oubli
Le droit à l'oubli concerne les données à caractère personnel. La législation sur la protection de la vie privée prévoit un droit d'opposition, de rectification au traitement de nos données personnelles pour des raisons sérieuses et légitimes.
En voici un exemple concret : « Un Arrêt de la Cour de justice de l'Union européenne du 13 mai 2014 a donné, à l'époque, une nouvelle interprétation à ce « droit à l'oubli » et a remis cette terminologie teintée d'un certain glamour révolutionnaire à l'ordre du jour. La Cour a estimé qu'un moteur de recherche (en l'occurrence Google) traitait des données au même titre qu'un gestionnaire de site internet. La Cour a également établi que dès qu'une entreprise disposait de filiales commerciales sur le territoire européen, le droit européen de la protection de la vie privée s'appliquait. La cour a alors établi ce « droit à l'oubli » comme un droit au déréférencement par les moteurs de recherche afin que certaines données personnelles n'apparaissent plus dans les résultats de recherche. Les données en question seront supprimées des résultats de recherche si les faits concernés ne présentent plus/pas d'intérêt public et en effectuant toujours un exercice de pondération entre le droit à la protection de la vie privée et la liberté d'information et d'expression et d'autres droits fondamentaux, comme la liberté des médias. »
Source : https://www.jeminforme.be/le-droit-a-l-oubli/

L'usurpation d'identité
En ligne, comme hors ligne, l'usurpation d'identité désigne le fait de s'emparer de l'identité d'une autre personne, la victime, sans le consentement de cette dernière. L'usurpation d'identité n'est pas en soi punissable en Belgique. Si vous remarquez que quelqu'un d'autre se fait passer pour vous sur les réseaux sociaux, vous pouvez le signaler à la plateforme concernée. Voler l'identité d'une autre personne ne devient un délit punissable en Belgique que si ces données sont également utilisées de manière inappropriée : pour effectuer des achats, faire du cyberharcèlement ou encore diffuser des messages de phishing... On parle alors de fraude à l'identité, qui peut faire l'objet d'une plainte auprès de la police.

Anonymat sur internet
Les gens pensent souvent qu'ils sont totalement anonymes sur le Web. Ce n'est pas vrai. Les plateformes de réseaux sociaux gardent une trace de qui crée quel compte. Si une plainte est déposée auprès de la police contre un compte anonyme sur les réseaux sociaux, les réseaux sociaux sont obligés de révéler qui se cache derrière ce compte. C'est pourquoi on parle de pseudonymat sur le web plutôt que d'anonymat.

Règlement général de protection des données
Disponible en tapant « Règlement général de protection des données » sur un moteur de recherche, le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne. Il renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant (accès, contrôle, correction et suppression de ces données).

Guide de l'enseignant (ressource 5)

Le Cyberharcèlement

Pourquoi en parler dans ce kit ?

L'objectif principal de ce kit est de vous permettre d'aborder la citoyenneté numérique sous 5 thématiques (nos 5 cyber) avec vos élèves. Il s'agit de faire de la prévention et de la sensibilisation aux attitudes et comportements à avoir sur les réseaux sociaux et le « web » de manière générale.
Cela dit, il est possible que vous rencontriez des situations de cyberharcèlement nécessitant une intervention de votre part, qu'elles soient de l'ordre de l'accompagnement, du conseil ou de la résolution de conflit et nous proposons ici quelques pistes vous permettant d'agir directement dans votre classe ou votre établissement scolaire. De plus, toute situation conflictuelle liée à un usage néfaste du numérique ne pouvant pas toujours être résolue grâce à votre action, nous vous partagerons ici les contacts de différents organismes, associations ou autres qui peuvent prendre en charge des cas de cyberharcèlement.
Le principal est d'agir vite et cela comprend l'accueil de la parole de l'élève, la création d'un espace de confiance et si nécessaire l'orientation vers des organismes spécialisés dans la gestion de ce malheureux phénomène sociétal.
À la suite de cette introduction vous trouverez de quoi mieux comprendre le cyberharcèlement, tant au niveau de ses tenants que de ses aboutissants ainsi que des pistes d'actions pour y remédier.

Définitions

Qu'en dit la loi ?
Au niveau légal il n'existe pas de définition légale *per se* du cyberharcèlement mais lors de procès pour actes d'harcèlement en ligne les décisions de justice s'appuient sur le texte de droit pénal relatif au harcèlement :
« Le harcèlement, visé à l'article 442bis du Code pénal, est passible d'une peine de 15 jours à 2 ans d'emprisonnement et/ou d'une amende de 50 à 300€. Pour que la plainte soit reçue, il faut que plusieurs conditions soient réunies : qu'il s'agisse d'un comportement répétitif, que le comportement soit abusif, qu'il y ait une atteinte à la tranquillité de la victime, le harceleur devait savoir qu'avec ses agissements, il allait préjudicier la victime. »
Source : https://www.jeminforme.be/que-faire-en-cas-de-cyberharcelement/

En théorie
Tout d'abord, pour qu'il y ait harcèlement il faut qu'il y ait une succession d'agissements hostiles d'une personne ou d'un groupe (harceleurs) envers une personne ou un groupe (victime). Ces agissements doivent être réalisés avec intention de nuire et ce de manière répétitive dans le temps. Ils sont donc à distinguer de la taquinerie (absence de mauvaise intention) ou de la « simple » attaque personnelle (absence de répétition).

Piliers du harcèlement, les rôles des acteurs sont toujours les mêmes et sont figés au sein de chaque situation : Le dominant (harceleur), le dominé (victime) et les témoins (spectateurs ou intervenants). Ces témoins, lorsqu'ils sont simples spectateurs, servent de « renfort » au harceleur car ils laissent la situation se faire, accentuant la sensation d'isolement de la victime. Lorsqu'ils sont témoins agissants, cela signifie qu'ils décident d'intervenir en faveur de la victime, que ce soit en lui apportant un soutien moral ou en allant en parler avec des responsables de l'établissement scolaire par exemple.

Le **Cyberharcèlement** suit la même logique et la même structure que le harcèlement de manière générale. Sa particularité est qu'il a lieu en ligne. Au-delà d'une simple particularité, le passage du harcèlement en ligne implique des conséquences encore plus graves et change considérablement l'impact du harcèlement sur la victime. En plus du sentiment d'isolement créé par la situation dans laquelle elle se trouve, se crée un sentiment d'**étouffement**. Le harcèlement n'a plus uniquement lieu à l'école ou dans un endroit « physique » déterminé, il se poursuit au-delà et vient « empoisonner » la sphère privée de la victime.

Ce qui change considérablement la donne, c'est également le **faux sentiment d'anonymat** créé par internet. On peut contacter quelqu'un en utilisant un pseudo, en se faisant passer pour quelqu'un d'autre et de ce fait, le web passe pour une « **zone de non-droit** » aux yeux des personnes les plus mal intentionnées. Comme on n'a pas à affronter directement la personne à qui on s'adresse, il est plus facile de s'adonner à une communication beaucoup plus violente sans prendre conscience de l'impact que cela peut avoir sur la personne qui se trouve de l'autre côté de l'écran. Cela dit, un harceleur agit par définition en connaissance de cause et sait qu'il fait du mal à la personne qu'il cible. Il est d'ailleurs important de noter qu'il n'y pas de « stéréotypes » de la victime ou du harceleur.

Comment agir ?

Posture de l'adulte

La première chose à faire lorsqu'un élève témoigne d'un acte qu'il a subi est d'accueillir la parole de l'enfant et d'en être le garant. En effet, il est essentiel de laisser la place à l'expression des émotions de l'enfant en question. Si l'adulte les refoule ou tente d'en amoindrir la gravité, l'enfant risque de se renfermer sur lui-même et de se sentir coupable d'avoir été ému, touché ou blessé par l'acte qui le visait. Dès lors, le caractère insidieux et latent du cyberharcèlement sera encore plus prégnant et plus grave en conséquence sur le vécu et la construction identitaire de l'enfant.

Il est important de faire s'exprimer les élèves concernés par l'acte rapporté. Leurs explications sont centrales pour remédier à cette situation. Il n'est pas nécessaire de mener une enquête de fond, de rechercher toutes les preuves possibles, à ce moment-là. Le principal est de « crever l'abcès ». À cette fin, la création d'un climat de confiance qui favorise l'ouverture des élèves quant à ce qu'ils vivent n'est pas

chose aisée mais se construit au fil de l'année et permet au dialogue de s'effectuer beaucoup plus rapidement.

Quel que soit l'acte identifié par l'élève comme malveillant (partage d'une photo désobligeante, régularité de messages violents et dégradants, usurpation d'identité, commentaires malveillants, humiliation publique, chantage (émotionnel ou non), …), le mot d'ordre est d'AGIR VITE. Il faut arriver à identifier les différents acteurs de la situation et de les faire s'expliquer sans culpabiliser personne. L'important est donc de créer un environnement au sein duquel la parole est possible et encouragée mais surtout protégée. Chaque enfant ne dispose pas de cette sécurité à la maison, il est dès lors essentiel que l'école puisse prendre le relais.

Actions concrètes
Premièrement, en amont de toute intervention, il faut construire le vivre-ensemble à l'école. Cette dernière doit faire société dans le sens où elle est la courroie de transmission des valeurs et des lois de la société dans laquelle elle s'insère. Ce faisant, les règles de bonne conduite auxquelles tout établissement éduque ses élèves sont la traduction de celles à adopter en dehors de l'école, en société. Il est important de rappeler aux élèves que ces règles sont d'autant plus d'application sur internet. Tout n'y est pas autorisé. Ce qui est illégal dans la société, l'est également sur internet. Ce faisant, les conséquences de ce qu'il s'y passe sont réelles et ne s'arrêtent pas à la vie « en ligne » des utilisateurs.

Méthodes

L'Espace de Parole Régulé (EPR)
(d'après Bruno Humbeeck, informations sur : www.ecolecitoyenne.org)

Les espaces de paroles régulés, ce sont des moments où un adulte permet à chacun de s'exprimer. Ce moment peut être court : une dizaine de minutes et désamorce les crises.

Le professeur peut utiliser des sanctions (carton jaune et rouge, exclusion du groupe) pour faire respecter les 5 règles qui permettent son succès :
- Une émotion se dit et ne se contredit pas.
- C'est le professeur qui donne et reprend la parole (en veillant à ce que tout le monde ait son temps de parole).
- On ne nomme pas, on ne désigne pas, on n'accuse pas, on n'insulte pas, on ne fait le procès de personne.
- La solution vient du groupe. L'intelligence collective est plus forte que l'intelligence émotionnelle.
- Régularité des moments de débat et permanence du lieu.

Programme KiVa
KiVa est une approche anti-intimidation développée en Finlande, couvrant dix thèmes au cours d'une année scolaire complète. Kiva est le mot finlandais pour « amusant » ou « sympa » et c'est exactement l'objectif de cette méthode : créer un environnement agréable pour tout le monde. L'accent est mis sur la formation de groupes positifs.

Une attention particulière est accordée aux compétences sociales, au développement socio-émotionnel, aux stratégies visant à décourager le harcèlement et à accroître la résilience des enfants. Le programme Kiva peut être appliqué en première, deuxième et troisième année de l'enseignement primaire. Plus d'explications : https://belgique.kivaprogram.net/

No Blame
No Blame est une méthode de lutte contre le harcèlement basée sur quatre piliers essentiels :
• Personne n'est puni
• L'empathie est encouragée
• La responsabilité est partagée
• La résolution de problèmes est utilisée

Le harcèlement est considéré comme un événement de groupe.
Pour résoudre le problème, il est important que l'ensemble du groupe soit mobilisé. No Blame suggère sept étapes pour gérer une situation d'intimidation :

1. Parlez à la victime. Comment a-t-il vécu la situation de harcèlement ? Demandez comment la victime se sent et demandez des informations générales. Si nécessaire, demandez à la victime de créer une histoire ou un dessin que vous pourrez utiliser dans les étapes suivantes. Expliquez la procédure et insistez sur le fait qu'il n'y aura aucune sanction. Donnez à la victime son mot à dire dans la composition du groupe (voir étape suivante) et sur les informations qui peuvent ou non être partagées.
2. Constituez un groupe comprenant les intimidateurs, les suiveurs, les assistants et les spectateurs neutres.
3. Expliquez au groupe que vous avez un **problème qui doit être résolu.** Expliquez en termes généraux ce qui se passe, sans accuser.
Si nécessaire, utilisez l'histoire ou le dessin que la victime a réalisé.
4. Rendre chaque membre du groupe responsable. Puisque les membres du groupe ont le plus de contacts avec la victime, ils sont également les mieux placés pour résoudre le problème.
5. Demandez des propositions et des idées pour résoudre le problème. Évitez les propositions générales et assurez-vous que les idées sont suffisamment concrètes. Formulez les propositions sous forme de messages en "je".
6. Donnez au groupe la liberté et la confiance nécessaires pour résoudre le problème de manière indépendante. Donnez aux membres du groupe un délai d'une semaine, après quoi vous leur reparlerez individuellement.
7. Parlez individuellement aux membres du groupe et demandez-leur en quoi ils ont spécifiquement contribué à résoudre le problème. (Questions clés : 'Comment vas-tu maintenant ?', 'Es-tu satisfait ?', 'Est-ce que ça s'est arrêté ?'...).

Si la victime ne se sent pas (entièrement) satisfaite, la procédure peut être répétée. Vous pouvez expérimenter vous-même la méthode No Blame, ou faire appel à un organisme certifié.

Associations « Relai »

Child Focus
La fondation pour enfants disparus et sexuellement exploités s'occupe aussi de gérer et de conseiller des personnes en situation de cyberharcèlement. Vous pouvez les contacter pour leur raconter votre histoire ou celle dans laquelle se trouve un de vos élèves, ils sauront vous conseillez afin de mettre fin à cette situation.
Plus d'informations sur leur site : https://childfocus.be/fr-be/Sécurité-en-ligne/Professionnels

OpenAdo
« L'Openado est un lieu convivial d'accueil, d'écoute, d'information, de prévention et d'accompagnement psycho-social. Il a pour objectif de permettre aux jeunes et à leurs familles d'exprimer en toute confidentialité leurs inquiétudes, leurs questions et leurs réflexions au sujet de toute situation liée à l'enfance et à l'adolescence et d'y trouver une réponse psycho-médico-sociale pertinente. » Ils sont actifs surtout sur la province de liège mais peuvent être de très bon conseil quoi qu'il en soit.
Source et informations complémentaires : https://www.provincedeliege.be/fr/openado

Service Ecoute-Enfants
« Ecoute-Enfants est un service qui répond, par l'intermédiaire du téléphone (numéro 103), aux questions des enfants, des adolescents, mais aussi de toute personne qui s'interroge ou s'inquiète à propos d'elle-même ou éventuellement d'autrui lorsqu'un enfant est en cause. »
Source et informations complémentaires : https://www.103ecoute.be/

Police locale

Conseils par thématique

Cyber Futé

Cinq conseils pour protéger son identité numérique

- **Vérifiez régulièrement vos paramètres de confidentialité.**
  Vérifier vos paramètres de confidentialité, c'est contrôler si vos publications sont publiques (visibles par tous) ou privées, par exemple. Cela permet d'éviter que vos données personnelles soient accessibles à tous et récupérables à des fins malveillantes ou commerciales.

- **Gardez les informations sensibles pour vous.**
  Il y a des choses qu'il ne vaut mieux pas publier qu'on appelle les informations sensibles. Ce sont des informations qui, si elles sont publiées, pourraient être utilisées contre vous par des personnes mal intentionnées. Par exemple : numéro de téléphone, numéro de compte en banque, adresse postale, etc... Il est important de savoir quand ne pas partager.

- **Respectez les limites et la vie privée des autres (même de sa propre famille).**
  Si une personne ne veut pas ou n'a pas l'âge d'apparaître sur les réseaux sociaux, il est important de respecter cela et de ne pas publier des informations personnelles la concernant. Notez que l'âge minimum pour ouvrir un compte sur les médias sociaux en Belgique est fixé à 13 ans. Pour WhatsApp et Signal, il s'agit même de 16 ans !

- **N'acceptez pas systématiquement tous les cookies.**
  Les cookies sont de petits fichiers placés sur votre ordinateur ou votre smartphone par les sites web que vous visitez. Ils gardent une trace de tout ce que vous lisez et regardez sur l'internet et stockent également des informations personnelles comme votre nom ou votre adresse. Sur la base de ces informations, un profil fictif est créé et celui-ci détermine quelles publicités ou actualités vous seront proposées, même si ce n'est pas forcément ce que vous vouliez voir. D'un autre côté, les cookies peuvent avoir certains avantages, comme faciliter la connexion automatique ou se rappeler des articles consultés sur une boutique en ligne. Alors demandez-vous toujours si les avantages des cookies l'emportent vraiment sur les inconvénients avant d'accepter tous les cookies d'un site web.

- **Souvenez-vous que "Internet n'oublie jamais".**
  En général, vous pouvez facilement retirer les informations ou contenus que vous avez publiés en ligne. Dans le cas où ce serait un tiers qui les aurait mis sur Internet, vous pouvez également demander à la personne ou au site web de supprimer ces informations. Il arrivera que le site approuve cette demande, mais pas toujours. En effet, le droit à la vie privée et le droit à l'oubli sont contrebalancés par le droit à l'information. Mais sachez que, sur Internet, les informations que vous

ou d'autres personnes publiez peuvent être copiées et partagées très rapidement. De fait, si quelqu'un commence à partager ou à stocker des informations ou des contenus sur vous, vous perdez rapidement le contrôle et il devient très difficile de tout tracer et de tout supprimer. Ces informations pourront donc continuer à circuler sur Internet à votre insu et ressurgir sans que vous vous y attendiez.

Cyber Vigilant

Cinq conseils pour contrer la désinformation et l'hameçonnage

- **Apprenez à distinguer un contenu factuel d'une opinion.**
  Un contenu factuel est quelque chose que vous pouvez prouver. Une opinion est le point de vue ou l'interprétation personnelle de quelqu'un. Il n'est pas toujours facile de distinguer les opinions des faits. L'information peut-elle être étayée par des arguments solides et vérifiables ? Alors, c'est généralement un fait. Si vous pouvez dire : « Je pense que... », il s'agit généralement d'une opinion.

- **Recoupez les informations de différents médias et comparez la façon dont celles-ci sont traitées.**
  Pouvez-vous retrouver la même information sur différents sites d'information ? Il y a alors de fortes chances pour que celle-ci soit vraie. Souvent, ces différentes plateformes d'information ont chacune leur propre angle et donc certains détails recevront plus ou moins d'attention. Ainsi, pour vous faire une meilleure idée de comment interpréter un fait d'actualité, il peut être utile de consulter différents médias : vous pourrez ainsi avoir une vision plus nuancée et plus complète de ce qui se passe.

- **Vérifiez que l'auteur / la source / la provenance soit sûr(e).**
  L'auteur est-il un expert dans le domaine dont il parle ? Quelles sont ses intentions ? A-t-il un programme politique ou économique particulier ? Le site web et/ou la plateforme médiatique ont-ils une bonne réputation ? L'information est-elle récente ou dépassée ? Voyez-vous beaucoup de fautes d'orthographe ? Ces questions peuvent vous aider à évaluer la fiabilité d'une source.

- **Exercez votre esprit critique et questionnez ce que vous lisez/entendez.**
  Les questions ci-dessus peuvent vous aider à réfléchir de manière critique. (Qui, quoi, où, quand, comment). Est-ce que quelque chose vous semble complètement inattendu, ou est-ce que quelqu'un dit quelque chose qui va à l'encontre de votre expérience de la réalité ? Alors vous devriez être sur vos gardes. (Par exemple, avez-vous déjà entendu un chien parler ou vu quelqu'un rajeunir en mettant une certaine crème sur sa peau ? D'autre part, nos connaissances et notre expérience sont limitées. Il y a beaucoup de choses que nous ne savons pas ou qui ne sont pas encore prouvées. Gardez l'esprit ouvert et recherchez des exemples concrets ou des arguments solides.

- **Redoublez de vigilance si un message est trop beau pour être vrai.**
  Un message vous annonce que vous avez gagné le dernier modèle

de smartphone ? Ou encore que vous avez hérité d'une fortune astronomique ? Méfiez-vous quand c'est trop beau pour être vrai ! Vérifiez la source et scrutez les éléments suspects. De même, si l'information vous semble en inadéquation avec la réalité (on vous dit que votre colis est bloqué à la douane alors que vous n'avez rien commandé), ne vous empressez pas de répondre ou de cliquer.

Cyber Secret

Cinq conseils en matière de sécurité en ligne

- **Choisissez un mot de passe fort que vous changerez régulièrement et optez pour la validation en 2 étapes.**
  Pour accéder à votre compte, vous devez être en mesure de prouver que vous êtes bien la personne que vous prétendez être. Cela se fait généralement à l'aide d'un mot de passe. Un mot de passe fort contient des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Il est également suffisamment long, au moins 8 caractères. La validation en deux étapes suppose que vous prouviez qu'il s'agit bien de vous de deux manières. Par exemple, via un code PIN et une empreinte digitale ou un mot de passe et un code personnel qui est envoyé sur votre téléphone.

- **Installez un antivirus et/ou un pare-feu.**
  Il arrive que des contenus malveillants s'introduisent dans notre ordinateur par le biais de courriels, de téléchargements ou d'une clé USB. Il est donc important d'avoir une protection contre ces menaces extérieures. L'antivirus protège votre ordinateur en scannant les programmes et fichiers potentiellement infectés par un virus informatique. Si une menace est détectée sur votre ordinateur (ou tablette, smartphone, etc.), l'antivirus tentera de récupérer le fichier infecté ou de le placer en quarantaine. Le pare-feu, lui, filtre le trafic Internet et de messagerie afin d'empêcher les programmes d'origine suspecte d'avoir accès à votre ordinateur. De nombreux pare-feu et antivirus offrent une protection de base gratuite.

- **Vérifiez que les sites sur lesquelles vous naviguez sont sécurisés.**
  Un bon indicateur qu'un site internet est sécurisé est que l'URL commence par HTTPS, confirmé par un cadenas fermé au début de la barre d'adresse. Le « s » de HTTPS signifie « sécurisé ». En pratique, cela signifie que toutes les données que vous saisissez sur le site sont protégées : seul le propriétaire du site peut voir ces données. Malheureusement, le HTTPS n'est pas étanche. Certains pirates peuvent également créer un site web HTTPS. C'est pourquoi il est important, en plus du cadenas, de prêter attention au nom du site, aux logos, à l'orthographe... Voyez-vous beaucoup de fautes d'orthographe ou les logos sont-ils différents de ce que vous attendez ? Réfléchissez-y à deux fois avant de saisir des informations personnelles.

- **Privilégiez les réseaux wifi sécurisés.**
  Un réseau sécurisé est un réseau auquel vous avez accès après avoir saisi un mot de passe. Sans celui-ci, les pirates peuvent

facilement intercepter ce que vous encodez sur l'internet, comme vos coordonnées bancaires ou vos identifiants. Sur un réseau non sécurisé, vous êtes également beaucoup plus vulnérable face aux virus. Vous souhaitez quand même vous connecter à un réseau non sécurisé, par exemple dans le train ou à l'aéroport ? Marquez-le alors comme réseau « public » la première fois que vous vous connectez. Votre ordinateur saura ainsi qu'aucune donnée ne devra être partagée.

- **Ne répondez pas aux mails ou messages qui vous semblent suspects.** Avez-vous reçu un e-mail ou un message de quelqu'un que vous ne connaissez pas, vous promettant de l'argent ou vous demandant des informations personnelles sensibles ? L'auteur vous semble-t-il suspect ? Un conseil en or : ne réagissez pas et signalez l'incident à un adulte ou une personne de confiance.

Cyber Sympa

Cinq conseils pour encourager la bienveillance en ligne

- **Efforcez-vous de vous exprimer avec gentillesse et empathie.** L'empathie consiste à essayer de comprendre ce que ressent une autre personne. C'est une qualité nécessaire pour établir des relations solides et saines dans la vie quotidienne et sur Internet. La gentillesse est également très importante. Il arrive que nos propos en ligne puissent être mal compris car ils sont souvent décontextualisés. Par conséquent, évitons les déclarations qui pourraient être mal interprétées et clarifiez vos propos en utilisant un emoji par exemple.

- **Ne réagissez pas systématiquement à tout : "Don't feed the troll"** Un troll est une personne qui publie des commentaires dans le but de volontairement susciter des débats conflictuels ou de lancer des polémiques. Souvent, cette personne poste anonymement ou via un faux profil. Répondre aux trolls vous entraine généralement dans un cercle vicieux : en prêtant attention à cette personne, vous la motivez dans son intention et celle-ci continue ses provocations. Il est donc préférable d'ignorer les trolls et de les signaler si nécessaire.

- **Protégez votre vie privée.** Votre lieu de résidence, l'endroit où vous allez régulièrement dîner, votre amoureux.se, l'hôtel où vous passez vos vacances... Ce sont tous des exemples de choses qui appartiennent à votre vie privée. Sachez qu'il est préférable de garder certaines de ces informations pour soi. Si elles tombent entre les mains de personnes malveillantes, elles peuvent être utilisées à mauvais escient pour vous nuire ou porter atteinte à votre réputation. Faites donc attention aux informations que vous partagez et aux photos que vous publiez !

- **Sachez comment réagir en cas de souci (garder des preuves, bloquer, signaler, etc).** Vous êtes confronté à un message, une photo ou une vidéo qui vous met mal à l'aise ? Ne vous sentez jamais obligé de répondre ou de la regarder. D'autres options sont possibles : empêcher l'expéditeur de vous contacter en le bloquant, signaler le message ou la vidéo (s'ils

violent la loi ou les conditions générales d'utilisation de la plateforme) ou tout simplement supprimer ce contenu. Nous vous recommandons également de faire des captures d'écran des messages indésirables ou offensants. Ainsi, vous gardez des preuves et il est plus facile de retracer l'historique et de prendre des mesures pour sanctionner si nécessaire.

- **Pensez à appeler à l'aide des personnes ou organisations extérieures compétentes.**
  Quand vous êtes face à un contenu qui vous choque, vous blesse ou vous met mal à l'aise, n'hésitez pas à en parler à un adulte que vous connaissez et en qui vous avez confiance. Après tout, il est tout à fait normal de demander de l'aide ou des conseils. Vous n'osez pas parler à quelqu'un de votre entourage ? Alors vous pouvez toujours raconter votre histoire de façon anonyme à Ecoute-Enfants, une ligne d'écoute gratuite pour enfants et adolescents accessible au numéro 103. Il existe également de nombreux autres services d'aide et associations prêts à vous aider.

Cyber Courageux

Cinq conseils pour réagir courageusement en cas de souci

- **Parlez à un(e) adulte de confiance si une situation vous semble inappropriée ou vous met mal à l'aise.**
  Nous l'avons dit plusieurs fois ci-dessus, et nous le répéterons. Vous voyez, lisez ou entendez quelque chose sur Internet qui vous met mal à l'aise ? Ne le gardez pas pour vous ! Parlez (ou écrivez) à un adulte que vous connaissez et en qui vous avez confiance. Cette personne peut vous aider à voir les choses autrement ou simplement écouter votre histoire. N'oubliez pas que parler aide vraiment à se sentir mieux et moins seul.

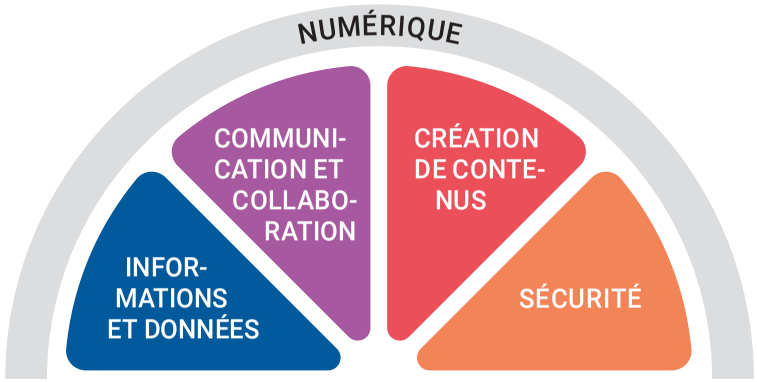
- **Ne culpabilisez pas et ne stigmatisez pas.**
  Face à une même situation, tout le monde ne réagit pas de la même façon. Les émotions ne sont jamais bonnes ou mauvaises. Elles sont juste des réactions spontanées face à un événement extérieur. Il n'est pas nécessaire de se sentir coupable de ressentir quelque chose.
  Le plus important, c'est d'accepter ce qu'on ressent sans se laisser submerger et de chercher une solution qui sera bénéfique pour tous.

- **Rappelez-vous que demander de l'aide pour soi-même ou pour d'autres est un signe de courage.**
  Qu'est-ce qui fait qu'un super-héros est un super-héros ? Le fait qu'il aide ou sauve d'autres personnes. C'est une preuve de courage. Et si vous pouviez aider quelqu'un d'autre (ou vous-même !) en parlant à un adulte ? Cela fait un peu de vous un super-héros aussi, n'est-ce pas ?

- **Apprenez à utiliser à bon escient les outils en ligne qui permettent de signaler un abus.**
  Souvenez-vous que vous pouvez toujours bloquer des numéros ou des profils sur les médias sociaux. Cela signifie que la personne qui

se cache derrière le numéro ou le profil ne peut plus vous contacter. La plupart des plateformes offrent également la possibilité de signaler les profils, messages ou images inappropriés. Cela envoie une notification à l'administrateur de la plateforme ou du groupe et lui permet d'intervenir et de supprimer le contenu inapproprié. Cependant, toutes ne disposent pas de cette option car les messages sont cryptés. Prenez, par exemple, WhatsApp. Dans ce cas, il peut être utile de faire une capture d'écran pour conserver des preuves.

- **Renseignez-vous sur les aides (associations, services d'écoute, etc) disponibles.**
  Idéalement, tournez-vous d'abord vers vos parents, un membre de votre famille, un enseignant ou des personnes de confiance dans votre entourage immédiat. Si vous n'avez personne, si personne n'est disponible ou si votre possibilité d'action est limitée, contactez des services comme Ecoute-Enfants ou Childfocus, par exemple. En effet, il existe de nombreuses organisations à qui vous pouvez vous adresser en cas de questions ou de problèmes. Faites une recherche sur Internet pour en trouver une près de chez vous.



Guide de l'enseignant (ressource 7)

Equivalence des activités avec le référentiel de Formation manuelle, technique, technologique et numérique

NOTE : Dans cette grille, nous n'avons pas tenu compte des âges conseillés pour les activités, le référencement est basé uniquement sur les compétences. Libre à chacun d'adapter les activités en fonction du niveau.

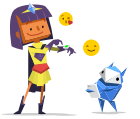
NIVEAU	SAVOIRS	SAVOIRS FAIRE	COMPÉTENCES	ACTIVITÉS CYBER-HÉROS
P3		Utiliser un contenu médiatique, en respectant les droits de propriété de la personne physique ou morale à qui appartient l'image. Expliquer le principe de droit à l'image lié au consentement de la personne prise en photo.		***Cyber Futé*** *Activité 1 : Que partager ?*
P4	Expliquer la notion de « Fake News » comme une information délibérément fausse.	Identifier les éléments permettant le questionnement d'une source	Effectuer une recherche pour répondre à un besoin suivant une stratégie pertinente Évaluer la fiabilité contextuelle d'une source	***Cyber Vigilant*** *Activité 3 : Vrai ou faux* *Activité 4 : Détecter les arnaques en ligne* *Activité 5 : Les outils du parfait fact-checkeur* *Activité 6 : Bataille numérique* *Activité 7 : Est-ce bien vrai ?* *Activité 8 : Repérer la désinformation en ligne* *Activité 9 : Dans la tête d'un moteur de recherche* *Activité 10 : S'exercer à faire des recherches sur internet*

NIVEAU	SAVOIRS	SAVOIRS FAIRE	COMPÉTENCES	ACTIVITÉS CYBER-HÉROS
P4	Expliquer les grands principes de droit à l'image dont le droit de propriété et le consentement de la personne prise en photo.	Appliquer les notions enseignées de droits de propriété Appliquer les notions enseignées de droits à l'image		***Cyber Futé*** *Activité 1 : Que partager ?* 
P5	Notions spécifiques liées à l'éthique des médias numériques	Participer dans un espace collaboratif numérique S'intégrer dans un espace collaboratif numérique, en respectant la cohérence de l'environnement Respecter la nétiquette* du média	Interagir/communiquer	***Cyber Sympa*** *Activité 3 : Dites-le gentiment* *Activité 4 : Débat mouvant – le cyberharcèlement* *Activité 5 : Commenter sans froisser* *Activité 9 : Comment faire preuve de gentillesse* 
				Cyber Courageux *Activité 6 : Gérer la méchanceté en ligne* 
	Chercher le taux de présence (e-réputation) d'un auteur, d'une célébrité, d'un personnage public Expliquer l'importance du choix d'un avatar et d'un pseudonyme			***Cyber Futé*** *Activité 2 : Qui est cette personne ?* *Activité 3 : Question de point de vue !* *Activité 4 : Miroir numérique* 

NIVEAU	SAVOIRS	SAVOIRS FAIRE	COMPÉTENCES	ACTIVITÉS CYBER-HÉROS
P6	Utiliser, adéquatement en contexte, les termes dont identité numérique, cyberharcèlement, cyberdépendance*.	Réagir face à des situations de cyberattaque*, de cyberharcèlement, de cybermanipulation	Prévenir et limiter les risques de déséquilibre social et psychologique de la personne (cyberattaque*, cyberharcèlement, cyberdépendance*)	**Cyber Futé** *Activité 2 : Qui est cette personne ?* *Activité 4 : Miroir numérique* **Cyber Vigilant** *Activité 2 : Mais qui est-ce exactement ?* **Cyber Sympa** *Activité 1 : Passer à l'action* *Activité 2 : Comment intervenir ?* *Activité 4 : Débat mouvant – le cyberharcèlement* *Activité 7 : Pratiquer l'empathie* **Cyber Courageux** *Activité 1 : À qui demander de l'aide* *Activité 2 : Signaler le problème* *Activité 3 : Que signifie être courageux ?* *Activité 5 : Contenu inapproprié en ligne. Que faire ?* *Activité 6 : Gérer la méchanceté en ligne*
P6	Utiliser, adéquatement en contexte, les termes dont sauvegarde, mise à jour, cookie, hameçonnage, spam, piratage, cyberattaque*, antivirus, mot de passe, authentification	Créer un mot de passe respectant un niveau de sécurité élevé	Prévenir et limiter les risques relatifs à la protection des données	**Cyber Vigilant** *Activité 3 : Vrai ou faux* *Activité 4 : Détecter les arnaques en ligne* **Cyber Secret** *Activité 1 : Créer un mot de passe sécurisé* *Activité 2 : Paramètres de sécurité* *Activité 3 : La course aux mots de passe* *Activité 4 : Mais ce n'était pas moi !*
S1	Expliciter des spécificités de différents réseaux socionumériques. Utiliser, adéquatement en contexte, les notions et les termes dont droit à la vie privée, droit à l'oubli, droit de retrait, liberté d'expression/de censure/de modération, licence open source*	Sélectionner un outil d'interaction en fonction de l'(des) interlocuteur(s) Respecter les droits de propriété dans des situations de communication Respecter, dans un environnement numérique d'interaction et de communication, une nétiquette* définie Préserver la confidentialité ou l'anonymat		**Cyber Futé** *Activité 1 : Que partager ?* *Activité 3 : Question de point de vue* *Activité 5 : Ce n'est pas ce que je voulais dire !* *Activité 6 : Le jeu de l'oie de la suppression de compte* **Cyber Sympa** *Activité 5 : Commenter sans froisser* *Activité 9 : Comment faire preuve de gentillesse*

* Nétiquette : charte de bienséance régissant les règles de conduite et de politesse, lors d'échanges numériques. * Cyberattaque : ensemble coordonné d'actions menées en ligne qui visent l'attaque d'un dispositif informatique via Internet. * Cyberdépendance : dépendance à l'utilisation d'outils numériques. * Licences « Creative Commons » : contrats types ou licences pour la mise à disposition d'œuvres en ligne, qui permettent aux titulaires de droits d'auteur d'accorder des permissions spécifiques à leurs œuvres.

NIVEAU	SAVOIRS	SAVOIRS FAIRE	COMPÉTENCES	ACTIVITÉS CYBER-HÉROS
	Utiliser, adéquatement en contexte, les termes dont profil, protection de la vie privée. Décoder une signalétique (PEGI…) Distinguer HTTP et HTTPS	Repérer les informations relatives à la vie privée, lors de l'encodage de données personnelles	Gérer son identité numérique, ses traces et ses données personnelles, pour protéger sa vie privée et celle des autres	**Cyber Futé** *Activité 1 : Savoir quand ne pas partager* *Activité 4 : Protéger les informations confidentielles* **Cyber Vigilant** *Activité 1 : Ne pas mordre à l'hameçon* **Cyber Secret** *Activité 2 : Garder son mot de passe secret*
		Réagir face à des situations de cyberattaque*, de cyberharcèlement, de cybermanipulation	Prévenir et limiter les risques de déséquilibre social et psychologique de la personne (cyberattaque*, cyberharcèlement, cyberdépendance*)	**Cyber Sympa** *Activité 4 : Passer à l'action* *Activité 2 : Comment intervenir ?* *Activité 6 : Petit clic, grandes conséquences* *Activité 9.2 : Pratiquer l'empathie* **Cyber Courageux** *Activité 1 : Quand demander de l'aide* *Activité 2 : Signaler le problème en ligne* *Activité 3 : Que signifie être courageux ?* *Activité 7 : Gérer la méchanceté en ligne*



* Nétiquette : charte de bienséance régissant les règles de conduite et de politesse, lors d'échanges numériques. * Cyberattaque : ensemble coordonné d'actions menées en ligne qui visent l'attaque d'un dispositif informatique via Internet. * Cyberdépendance : dépendance à l'utilisation d'outils numériques. * Licences « Creative Commons » : contrats types ou licences pour la mise à disposition d'œuvres en ligne, qui permettent aux titulaires de droits d'auteur d'accorder des permissions spécifiques à leurs œuvres.