Protection de la vie privée

Il y a de forte chance que les contacts relatifs au respect de la vie privée en ligne relèvent de trois grandes catégories : des demandes de conseils sur les bonnes pratiques de respect de la vie privée, des problèmes d'atteinte à la vie privée et des préoccupations de « réputation numérique » ou « d'empreinte numérique ».

Comme exemple de contact demandant conseil sur les bonnes pratiques en matière de respect de la vie privée, il peut s'agir d'un enfant désireux de savoir comment faire pour protéger sa vie privée en ligne (choix de mot de passe, gestion de profil numérique, etc.).

Les contacts en cas d'atteinte à la vie privée se rapportent à des violations de la vie privée : quand quelqu'un par exemple soupçonne quelqu'un d'autre de connaître son mot de passe, ou reçoit des contacts indésirables.

Un enfant peut aussi appeler pour faire part de ses préoccupations au sujet de son « empreinte numérique » ou de sa « réputation en ligne » : par exemple, si lui-même ou un ami a partagé des informations ou des contenus qui auraient dû rester privés et s'il se préoccupe de l'impact que cela pourra avoir. Il peut s'agir notamment de partage d'images sexuelles ou de « sextos », ou de « porno de revanche » :

- Sexto : Image explicite de soi nu/partiellement nu/sexuellement explicite, produite par soi-même
- Porno de revanche : Matériel sexuellement explicite qui est rendu public en ligne sans le consentement de la personne qui en est l'objet. Souvent ce type de matériel est téléchargé par des ex-partenaires dans l'intention de causer du tort ou de l'embarras de la personne concernée, en reliant le contenu à d'autres contenus en ligne (son profil numérique par exemple) la concernant.

PRISE DE CONTACT DIRECTEMENT PAR L'ENFANT

Félicitez l'enfant d'avoir pris contact et posez-lui des questions : c'est en écoutant l'enfant que vous serez en mesure de mieux comprendre la raison pour laquelle il vous a contacté.

Posez des questions pour déterminer si sa prise de contact vise à en savoir plus sur les « bonnes pratiques » concernant la vie privée, porte sur une atteinte à la vie privée ou sur la réputation numérique de l'enfant.

Si l'enfant a appelé pour faire part de sérieuses préoccupations concernant sa réputation en ligne ou une atteinte à la vie privée, rassurez-le et accordez-lui une oreille attentive. Il est possible qu'il se sente assailli par toutes sortes d'émotions : menaces, honte, bouleversement. Félicitez l'enfant d'avoir pris contact et saluez son courage à parler ouvertement. Il est essentiel de rassurer le jeune en lui disant qu'il a pris la bonne décision et que vous êtes là pour l'écouter et l'aider. Il est tout aussi important de veiller à bien lui dire qu'il n'est pas fautif ni à blâmer.

Énoncez clairement la position de votre ligne d'assistance aux enfants en matière de confidentialité, pour que l'enfant sache ce qu'il va advenir des informations qu'il va vous donner. Expliquez-lui notamment que tout ce qu'il vous confie restera privé, à moins qu'il ne vous dise quelque chose qui vous fait penser qu'il court un danger et que vous pouvez faire quelque chose pour l'aider, auquel cas vous lui indiquerez les mesures que vous allez prendre.

Mettez l'enfant en confiance en lui consacrant le temps et l'espace nécessaires pour qu'il se confie davantage et vous donne plus d'informations. Ne manquez pas de reconnaître l'impact émotionnel de ce qui est arrivé, et veillez à ne pas tirer de conclusions hâtives de la situation.

Donnez-lui votre soutien. En plus de collecter des informations sur la nature de l'atteinte ou du problème de réputation numérique, essayez de comprendre les effets émotionnels que cet événement a pu avoir sur l'enfant, pour l'aider à y faire face, et faire remonter ces informations et assurer sa sécurité si nécessaire. Par exemple, dans les cas où « l'empreinte numérique » de l'enfant est utilisée pour le soumettre à du chantage, il est nécessaire de relayer cette information aux autorités (voir le guide sur l'extorsion sexuelle).

Les questions que vous posez doivent être claires et ouvertes, par exemple :

- Peux-tu nous dire quand ça s'est passé ?
- Des menaces ont-elles été proférées par quelqu'un désireux de te faire mal ? Est-ce qu'on t'a invité à produire d'autres images ?
- Quels contenus as-tu partagés ? Avec qui ? Sur quels appareils/réseaux sociaux ces contenus ont-ils été partagés ?

Essayez de l'aider à comprendre que même s'il peut avoir l'impression que c'est la fin du monde, ça n'est pas le cas. Parlez-lui des diverses stratégies qui peuvent l'aider à reprendre contrôle de la situation.

Si lors du contact, l'enfant ne souhaite pas entrer dans les détails, encouragez-le à rappeler plus tard : donnez-lui le temps et l'espace.

Discutez des options pratiques qui sont pertinentes en fonction du contact (voir ci-dessous).

PRISE DE CONTACT PAR UN PARENT/TUTEUR

Félicitez le parent/tuteur de sa démarche de demander conseil.

Posez des questions pour déterminer si sa prise de contact vise à en savoir plus sur les « bonnes pratiques » concernant la vie privée, porte sur une atteinte à la vie privée ou sur la réputation numérique de l'enfant, et adaptez votre réponse en conséquence.

Pour appuyer les discussions sur les bonnes pratiques de vie privée avec les parents/tuteurs, vous pouvez vous servir d'un cadre élaboré par O2 et la NSPCC : Explorer, Parler, Convenir et Gérer

Explorer : Aidez-le à comprendre ce qu'on entend par données à caractère personnel.

- Votre enfant doit protéger ses données à caractère personnel, au risque qu'elles tombent entre de mauvaises mains. Son adresse, son nom complet, sa date de naissance, son numéro de téléphone et le nom de son école sont autant d'exemples de données à caractère personnel. Toutes ces informations peuvent être utilisées à des fins d'intimidation, de chantage, de grooming ou de vol d'identité.
- Il peut arriver qu'une demande de coordonnées personnelles ne paraisse pas suspecte de prime abord. Pourtant vous devez vous assurer que votre enfant ne communique jamais ses données à caractère personnel avec autrui sur Internet. Il arrive que les gens mentent sur leur identité.

Parler : Faites-lui comprendre l'importance d'avoir des conversations avec son enfant

- Expliquez-lui que tout contenu partagé en ligne pourrait finir par ne jamais disparaître, même après l'avoir effacé. Il est impossible de savoir qui a copié ou partagé les informations en question. Demandez à votre enfant de réfléchir à ce qui pourrait se passer si ses informations tombaient entre de mauvaises mains. Demandez-lui d'envisager les conséquences : c'est le meilleur moyen qu'il en retienne les leçons.
- Dites à l'enfant que vous êtes là pour l'aider si quelque chose venait à mal tourner. Promettez-lui de ne pas vous mettre en colère et de ne pas vous fâcher.

Convenir : Faites-lui comprendre l'importance de fixer des règles avec son enfant.

- Mettez-vous d'accord sur les sites, les applications et les jeux qui sont appropriés pour votre enfant. Si votre enfant veut utiliser un salon de tchat, assurez-vous qu'il est géré par un modérateur et que vous l'avez vous-même vérifié.

Gérer : Aidez votre enfant à comprendre son empreinte numérique.

- Faites une recherche en ligne du nom de votre enfant, de son surnom, de son école ou de son adresse. Vérifiez aussi les résultats sous forme d'images. Cela vous indiquera si les informations le concernant qui sont publiques. Si quelque chose vous préoccupe, parlez-en avec votre enfant et aidez-le à modifier son profil pour le rendre plus sûr.

SIÈGE DE LA GSMA
Floor 2, 5 The Walbrook Building, 25 Walbrook, London, EC4N 8AF, Royaume-Uni
Tél : +44 (0)20 7356 0600

Pour les appels réactifs à propos d'atteinte à la vie privée ou de problèmes tenant à la réputation numérique d'un enfant, il vous faudra vous montrer rassurant. Il est probable que le parent/tuteur éprouve tout un ensemble d'émotions s'il apprend que son enfant a partagé des images/vidéos de lui en ligne nu ou quasiment nu. Il peut ressentir de la colère, de la confusion, de la peur et il est possible même qu'il se sente coupable de la situation. Ce qui prime avant tout, c'est qu'il comprenne bien que la situation n'est la faute de son enfant.

Encouragez le parent à essayer de garder son calme, d'éviter de porter des jugements et de s'abstenir de toute solution prise dans la panique. Conseillez-lui particulièrement de ne pas interdire à son enfant d'avoir accès à Internet : une telle mesure aurait comme conséquence la plus probable que l'enfant s'abstiendra de lui parler de problèmes futurs de crainte d'être coupé de sa vie numérique.

Présentez au parent des conseils pratiques (voir ci-dessous) et rappelez-lui que votre ligne d'assistance aux enfants est mis à la disposition de son enfant qui peut appeler pour demander de l'aide. Insistez bien sur le fait que le contenu de toute conversation avec l'enfant restera confidentiel, à moins que l'enfant ne vous donne son consentement d'en parler au parent.

Il est important aussi que vous discutiez avec lui de l'impact émotionnel potentiel que cela peut avoir sur l'enfant : c'est un moyen d'aider le parent à rester vigilant aux manifestations qu'il peut présenter tout en offrant du soutien à son enfant. Posez au parent les questions suivantes :

- A-t-il remarqué des changements de comportement chez leur enfant ?
- S'inquiète-t-il de la santé mentale de l'enfant, que ce soit actuellement ou depuis quelque temps déjà.

Ces informations vous éclaireront s'il est utile d'avoir recours à d'autres services de soutien. Ne manquez pas de demander au parent de rester attentif à tout changement de comportement ultérieur chez l'enfant, même si à ce stade le parent n'a remarqué aucun changement visible.

CONSEILS PRATIQUES :

Prenez le temps de réfléchir avec l'enfant ou le parent/tuteur des options pratiques qui pourraient lui être utiles en fonction du contexte spécifique dont vous discutez.

Voici quelques exemples de mesures pratiques dont vous pouvez discuter pour garder le contrôle de la vie privée en ligne :

- **Examiner les politiques et les paramètres de respect de la vie privée** des sites Internet et des applications que vous utilisez.
- **Mots de passe.** Ne partagez jamais vos mots de passe avec quelqu'un. Si vous pensez que quelqu'un connaît votre mot de passe, changez-le. Choisissez un mot de passe qui ne risque pas d'être deviné et utilisez différents mots de passe pour différents services et différentes activités.
- **Profils et partage d'informations.** Gérez activement les paramètres de votre profil pour faire en sorte que vos messages ne soient visibles que par le groupe d'amis de votre choix. N'oubliez pas que tout ce que vous publiez pourrait malgré tout être copié et partagé en dehors de votre groupe choisi. Ne partagez pas d'informations en ligne susceptibles de vous rendre vulnérable à des contacts indésirables ou inappropriés ou au vol de votre identité (par ex. adresse, e-mail, numéro de téléphone, date de naissance, etc.).
- **Amis**. Réfléchissez soigneusement aux demandes de vos amis : que savez-vous vraiment à propos de la personne qui vous a contacté ?
- **Nom d'utilisateur.** Les noms d'utilisateur ne doivent jamais inclure des renseignements personnels (comme son année de naissance, son adresse ou son nom complet).
- **Historique**. Supprimez votre historique de recherche et déconnectez-vous des sites Internet quand vous vous éloignez de votre ordinateur.
- **Utilisez un logiciel antivirus** sur vos appareils et maintenez-le à jour.
- **Consultez des sites Internet sécurisés.** Avant de saisir des informations privées comme le mot de passe ou les détails de paiement, vérifiez la présence du symbole du cadenas après l'adresse web ou la mention « https » au début de l'adresse web dans votre navigateur.
- **Réfléchissez avant de cliquer** : Si vous recevez un e-mail d'un inconnu, réfléchissez avant de cliquer sur un lien ou une pièce jointe : il pourrait contenir un virus.
- **Couvrez votre webcam** : Si vous n'êtes pas en train d'utiliser votre webcam, débranchez-la, recouvrez la lentille ou tournez-la vers un mur blanc.
- **Blocage**. Utilisez des paramètres de confidentialité ou des outils de blocage pour éviter tout contact indésirable.

SIÈGE DE LA GSMA
Floor 2, 5 The Walbrook Building, 25 Walbrook, London, EC4N 8AF, Royaume-Uni
Tél : +44 (0)20 7356 0600

- **Restez vigilant à tout risque de vol d'identité**. Par exemple, si vous recevez des factures pour des choses que vous n'avez pas commandées ou des e-mails d'organisations inconnues, il se pourrait que quelqu'un est en train d'utiliser votre identité. Changez tous vos mots de passe, vos questions secrètes et les autres informations que vous utilisez pour vous identifier sur les services en ligne.

Pour les contenus qui ont déjà été partagés et qui suscitent des regrets de l'avoir fait, vous pouvez discuter des options disponibles avec l'enfant. Par exemple :

- L'enfant peut-il modifier ou supprimer le contenu, si c'est lui qui l'a téléchargé ?

- Si quelqu'un d'autre l'a téléchargé, ou si le contenu que vous avez téléchargé a été partagé par quelqu'un d'autre, l'enfant pourrait-il demander à cette personne de le supprimer ? Discutez avec l'enfant des manières dont il pourrait formuler sa requête.

- Est-il bénéfique de supprimer le compte à partir duquel le contenu a été partagé, et de configurer un nouveau profil sur ce site ?

Si le problème est lié à des « sextos » ou à la perte de contrôle d'images/de matériels sexuels autoproduits en ligne, suggérez à l'enfant ou au parent de prendre contact avec le centre de sécurité sur le site de médias sociaux, ainsi qu'avec tous les services disponibles (la ligne nationale de signalement Internet), pour faire effacer ces contenus. En cas de chantage, reportez-vous au guide sur l'extorsion sexuelle.

Pour les questions relatives aux contacts indésirables, consultez le guide sur les contact non sollicités.

SIGNAUX D'ALARME :

- Révélation par l'enfant qu'il est l'objet d'images sexuelles produites par un pair ou un adulte

- L'enfant exprime des pensées suicidaires, des intentions d'automutilation ou manifeste un traumatisme émotionnel.

- L'enfant fait l'objet de menaces ou est victime de chantage.

Si des signaux d'alarme se manifestent lors de votre conversation, observez la procédure standard de recours en faisant intervenir les forces de l'ordre, les services de protection de l'enfance, etc., s'il y a lieu de le faire.

SIÈGE DE LA GSMA
Floor 2, 5 The Walbrook Building, 25 Walbrook, London, EC4N 8AF, Royaume-Uni
Tél : +44 (0)20 7356 0600