Qu’est-ce qui reste privé ?

Essayez ensemble avec un adulte de confiance. C’est une conversation, pas un test. Tous les exemples sont fictifs.

QUESTION POUR COMMENCER

Quelles questions devrions-nous poser avant de partager des informations ou d’autoriser un outil à utiliser une caméra, un microphone ou la localisation ?

Essayez ensemble

Fabriquez des cartes en utilisant uniquement des catégories : « dessin de dragon imaginaire », « mot de passe », « code de connexion », « adresse du domicile », « emploi du temps quotidien » et « photo d’une autre personne ». Classez-les dans les groupes suivants : exemple inventé, à garder privé ou demander d’abord à un adulte. Une application de dessin fictive demande ensuite l’accès au microphone et aux contacts. A-t-on besoin de l’une ou l’autre de ces autorisations pour colorier ? Entraînez-vous à choisir « pas maintenant ». Une réponse à pratiquer

« Je peux utiliser des informations inventées à la place. Je ne téléverserai pas la photo d’une autre personne sans son autorisation et sans qu’un adulte ait vérifié que cela ne présente pas de risque. » Ce n’est pas parce qu’on peut téléverser quelque chose qu’on devrait le faire.

NOTRE RÈGLE FAMILIALE

Utilise moins d’informations. Demande avant de partager. Protège aussi les autres.

Tu peux parler, dessiner, montrer du doigt, faire une pause, passer une activité ou arrêter. Aucun compte d’IA, aucun enregistrement ni aucune véritable information privée n’est nécessaire.

Nos questions

Parlez, dessinez ou écrivez ensemble. Il n’est pas nécessaire de remplir toutes les lignes ni de noter quoi que ce soit de personnel.

Quelles catégories devraient rester privées ?

Quelle autorisation semble inutile ?

Quel exemple inventé pourrait remplacer les données d’une personne réelle ?

Une action à essayer cette semaine

Discutez ensemble des autorisations d’une application, ou utilisez l’application fictive si aucun appareil n’est disponible. Respectez le refus des autres d’être photographiés ou de voir leur photo partagée.

NOTRE RÈGLE FAMILIALE

Utilise moins d’informations. Demande avant de partager. Protège aussi les autres.

Gardez les fiches remplies à la maison. N’y inscrivez jamais de vrais noms, mots de passe, codes de connexion, phrases privées, renseignements sur l’école ou coordonnées.

Défi pour les ados : discussion 2

Une situation fictive pour les enfants plus âgés et les adolescents. Aucun message en direct, vrai camarade de classe, enregistrement ou compte d'IA n'est nécessaire.

QUE FERAIS-TU ?

Un groupe veut téléverser une photo publique d'un camarade de classe dans un outil de retouche d'images utilisant l'intelligence artificielle (IA), créer une fausse « annonce » humiliante, puis la faire circuler pour plaisanter. La page de téléversement du service n'explique pas clairement combien de temps la photo est conservée.

Une démarche pour décider de façon plus sûre

1. Ne téléverse pas la photo et ne crée pas le faux contenu. Une publication publique ne vaut pas consentement à n'importe quelle réutilisation.
2. Explique que l'humiliation, l'usurpation d'identité et le partage peuvent causer du tort, que l'image paraisse réaliste ou non.
3. Demande ce que deviennent les contenus téléversés : stockage, partage avec d'autres, utilisation par le modèle, suppression et accès.
4. Si un harcèlement ciblé a lieu, parle à un adulte de confiance et utilise les moyens de signalement adaptés de l'école ou de la plateforme. Discutes-en avec un adulte de confiance

Qu'est-ce qui rend une photo risquée, même lorsqu'un ami l'a publiée publiquement ?

Que pourrait créer le groupe à la place, sans impliquer une personne réelle ?

PRINCIPE COMMUN

Utilise moins d'informations. Demande avant de partager. Protège aussi les autres.

Notes pour l'adulte

Un support de discussion, pas une grille de notation. Gardez cette page à part des fiches destinées aux enfants ; le défi pour les ados est facultatif.

Les éléments à repérer dans les réponses

Les mots de passe, les codes de connexion, l'adresse et l'emploi du temps quotidien ne doivent pas figurer dans les outils d'IA ni dans les fiches d'activité. Une autorisation est nécessaire, mais elle ne suffit pas toujours à justifier l'envoi d'un contenu. Vérifiez comment le contenu peut être conservé ou partagé ; les options de suppression ne garantissent pas que toutes les copies disparaissent.

Ajoutez un prolongement pertinent

Alternative positive : inventez un personnage fictif ou utilisez un dessin vierge. Expliquez comment limiter les autorisations au strict nécessaire et les bases de la récupération d'un compte.
Adaptation selon l'âge

Moins de 5 ans : photos imaginaires. 5-7 ans : demander avant d'utiliser la caméra ou le micro. 8-12 ans : trier les informations selon leur caractère privé. 13-17 ans : consentement, conservation des données et traces numériques.

Faites le point sans faire honte

Demandez : « Qu'est-ce qui a rendu cela difficile ? » et « Que ferais-tu en premier ? »

Valorisez la vérification indépendante, la protection de la vie privée, la liberté de choix et le fait de demander de l'aide à une personne.

Ne demandez pas à un enfant de faire une démonstration avec de vrais contenus préjudiciables ni de raconter des expériences personnelles privées dans le cadre d'une activité.

SI UNE PRÉOCCUPATION RÉELLE SURVIENT

Arrêtez l'activité, remerciez l'enfant et vérifiez sa sécurité. Suivez le guide de réponse aux incidents destiné aux adultes responsables. En cas de danger immédiat ou de crainte que l'enfant se fasse du mal, cherchez d'urgence une aide humaine qualifiée près de chez vous, et non des conseils d'une IA.