Sécurité en ligne

- L'envoi de SMS ou messages privés sont interdits. N'envoyer des messages (SMS, e-mails ou autres moyens de communications) qu'en groupe ou en public.
- Mettre en copie un parent et un superviseur/collègue (de préférence un agent de protection de l'enfance ou un défenseur des droits de l'enfant) lorsque cela est possible, par souci de transparence.
- Avoir une politique claire sur l'utilisation des photos des enfants par les participants, le personnel et l'organisation sur les réseaux sociaux et les supports marketing.
- Avoir dans les dossiers les formulaires d'autorisation de droit à l'image pour chaque enfant, membre du personnel et bénévole pour l'utilisation de leur image.
- Les adultes souhaitant poster des messages politiques, ou n'importe quel contenu ou code de conduite inappropriés sur les réseaux sociaux doivent avoir un compte professionnel distinct de leur compte personnel.
- Inclure dans le code de conduite de l'organisation un énoncé sur le comportement à adopter en ligne et le signalement des infractions, à l'intention des participants, du personnel et des bénévoles.
- Utilisez les paramètres de confidentialité pour limiter l'usage des réseaux sociaux et autres réseaux de communication en fonction de la nature de leur utilisation, en particulier pour la publication d'événements et d'activités pour enfants – groupes et publications privés.
- Enseigner aux jeunes concernés les dangers des réseaux sociaux et d'Internet (drogue, harcèlement, arnaques, trafics, revenge porn, redistribution de matériel, …)
- Disposer d'une méthode pour signaler ou noter toute violation de politique ou tout contact inapproprié de la part des enfants.
- Afficher les règles d'utilisation d'Internet et des réseaux sociaux et/ou le code de conduite sur Internet dans des endroits spécifiques pour rappeler au personnel et aux participants le comportement à adopter en ligne.
- Utiliser le contrôle parental sur les télévisions, smartphones, tablettes et ordinateurs pour limiter l'accès aux enfants à certains sites.
- Pensez à limiter l'accès et le temps passé sur Internet et à créer un historique du contenu visionné.

  Méthodes possibles :
  - des comptes individuels pour chaque utilisateur
  - limiter la taille des fichiers téléchargés
  - limiter le type de fichiers qui peuvent être téléchargés
  - Limiter l'accès à certains sites
  - Interdire tous les téléchargements

- Si l'usage d'ordinateurs est autorisé en public:
    - Disposer les écrans face à face afin qu'ils puissent être facilement surveillés.
    - Vérifier de temps en temps l'historique du navigateur et le fichier des téléchargements.
    - Mettre en place la surveillance et l'enregistrement de l'utilisation d'Internet (l'organisation doit être assez grande pour disposer d'un système d'admin ou d'un membre du personnel informatique).

Translated by Romane Belin, Sarah Pockett and Kim Tang as part of the Support for Access to Audiovisual Media (SAAM) Project. Supported by Alumni Fund, University of East Anglia (UK)