

## Messagerie et réseaux sociaux : quels sont les dangers et les précautions à prendre ?



**RESPECTER LA  
FRONTIÈRE ENTRE  
VIE PRIVÉE ET  
VIE PUBLIQUE**

**FAIRE LES BONS  
CHOIX DANS SES  
CONTACTS**

**NE PAS DIVULGUER  
DES INFORMATIONS  
TRÈS PERSONNELLES**

**RESPECTER LES  
RÈGLES DE  
COMMUNICATION ET  
DU SAVOIR-VIVRE**

### Que faut-il éviter sur les réseaux sociaux ?

#### 1 - Ne pas se mettre soi-même en danger :

- ♦ évaluer le temps passé sur les réseaux pour éviter la cyberdépendance, l'isolement et l'apparition de problèmes scolaires,
- ♦ ne pas divulguer d'informations ou d'images très personnelles pour éviter de voir attaquer sa réputation ou usurper son identité,
- ♦ se souvenir qu'il est presque impossible de stopper la diffusion d'une information une fois lancée ;

#### 2 - Faire attention aux autres mineurs :

- ♦ ne pas se livrer au cyberharcèlement : intimidations, rumeurs, usurpation d'identité, création d'une page sur un réseau social, publication de photos ou de vidéos, *sexting*,
- ♦ ne pas en devenir une victime,
- ♦ un mineur peut cacher un adulte : des réseaux de pédophiles qui cherchent à entrer en contact avec des victimes potentielles ;

#### 3 - Ne répondre à aucune demande de renseignement confidentiel (numéro de carte bancaire, coordonnées bancaires, identifiant et mot de passe d'un compte quelconque, etc.) ;

#### 4 - Se méfier des phénomènes collectifs incontrôlés : les apéros Facebook, anniversaires, les pages *spotted*, où on déclare sa flamme sur une page Facebook dédiée.

### Des sites pour s'informer :

La Cnil : <http://www.cnil.fr/les-themes/scolarité-mineurs/>

Données personnelles, quels sont mes droits ? :

<http://www.cnil.fr/vos-droits/exercer-vos-droits/>

## Quelles précautions prendre sur les réseaux sociaux ?

### 1 - Pour la sécurité du matériel et des données :

- ◆ mettre à jour systématiquement et régulièrement système d'exploitation, antivirus, autres programmes de sécurité, toutes les applications utilisées,
- ◆ installer un contrôle parental sur tout appareil connecté à l'internet (ordinateur, téléphone portable, console de jeu, télévision, etc.) ;



### 2 - Dans le choix et l'utilisation des outils :

- ◆ prendre le temps de lire les C.G.U. (conditions générales d'utilisation) du service en question,
- ◆ utiliser les paramètres et les outils de confidentialité, vérifier le paramétrage des réseaux sociaux dès qu'apparaissent de nouvelles fonctionnalités,
- ◆ changer de mot de passe 3 à 4 fois par an ou selon le besoin :
  - \* utiliser un mot de passe suffisamment complexe (constitué au minimum de 8 caractères différents : lettres minuscules, majuscules, chiffres et symboles),
  - \* utiliser des mots de passe différents pour des services différents.

### 3 - Dans les échanges :

- ◆ ne pas injurier ou diffamer,
- ◆ ne pas tenir de propos discriminatoires (par exemple racistes, sexistes, homophobes, etc.),
- ◆ ne pas présenter crimes ou délits de manière élogieuse,
- ◆ n'entrer en relation qu'avec des amis que l'on connaît en dehors de l'internet,
- ◆ gérer sa webcam : ne l'allumer qu'en cas de besoin ; par sécurité, coller un morceau de sparadrap pour être certain qu'elle ne sera pas utilisée sans s'en apercevoir,
- ◆ ne pas diffuser d'informations personnelles ou d'images sur autrui sans son autorisation et celle de ses responsables légaux s'il s'agit d'un mineur.

## Des sites pour s'informer :

Surfer prudent : <http://www.surferprudent.org/>

Agir contre le harcèlement : <http://www.agircontrelharcelementalecole.gouv.fr/>

Fiches pratiques d'utilisation des réseaux sociaux : <http://www.netpublic.fr/2015/01/11-reseaux-sociaux-en-fiches-pratiques-pour-une-utilisation-pedagogique/>