



Prendre en compte la sécurité des personnes, des réseaux et des données

publié le 08/09/2008 - mis à jour le 21/02/2020

Une politique d'établissement à réfléchir

Descriptif :

Trouver un équilibre entre innovation pédagogique et sécurité.

Sommaire :

- Filtrer Internet
- Limiter la publication de données personnelles
- Former et sensibiliser les utilisateurs des réseaux
- Sécuriser les mots de passe

● Filtrer Internet

Le filtrage des contenus inappropriés est géré par la Direction des Systèmes d'Information (DSI), qui s'appuie sur les préconisations nationales et une [procédure d'alerte académique](#). Les chefs d'établissement ont la possibilité de faire évoluer les filtres pour leur établissement sur demande.

Certaines activités pédagogiques innovantes peuvent nécessiter l'utilisation dans l'établissement d'outils de communication couramment utilisés par les jeunes en dehors de l'école, tels que des réseaux sociaux.

- ▶ Pour le primaire, tout changement demandé dans le filtrage et accepté est appliqué à toutes les écoles de l'académie.
- ▶ Pour les collèges tout aménagement demandé par l'équipe de direction (par exemple ouverture de l'accès à un site de vidéo) concerne l'ensemble de l'établissement.
- ▶ Pour les lycées, à la demande du proviseur ou d'une personne mandatée par lui, ces filtres peuvent être adaptés provisoirement pour un projet précis (voir la procédure d'alerte académique).
- ▶ Un filtre spécifique peut aussi être installé, par exemple pour une section post-bac, dans un foyer ou en salle des professeurs, selon certaines conditions expliquées aux chefs d'établissement dans le Portail Intranet Académique (rubrique informatique).

Le but est de trouver un équilibre entre innovation pédagogique et sécurité.

● Limiter la publication de données personnelles

Les photographies permettant d'identifier les élèves ne doivent pas être visibles sur le site de l'établissement accompagnées du nom complet de la personne photographiée, par principe de précaution.

La personne photographiée doit pouvoir s'opposer à la publication de son image, et doit pouvoir demander son retrait du site si elle le souhaite. Des formulaires de demande d'autorisation d'utiliser l'image ou la voix sont téléchargeables notamment sur [le guide des auteurs du web](#) .

● Former et sensibiliser les utilisateurs des réseaux

L'information et la sensibilisation des élèves et des adultes à la prudence dans l'usage du matériel et d'Internet doivent être prévues, organisées et mises en place.

Les chefs d'établissement doivent rédiger une **charte du bon usage des TIC** annexée au règlement intérieur et signée par chaque élève. Plusieurs chartes peuvent être prévues pour tenir compte des possibilités variables selon les lieux ou les statuts.

Des animations et témoignages sont régulièrement publiés pour faciliter cette **sensibilisation des personnels et des élèves**.

Voir des exemples [provenant de lycées](#) (site compétences numériques).

Voir des exemples [provenant de collèges](#).

Pour éclairer les **comités de pilotage du numérique** en établissement un article fait le point sur "[l'utilisation d'Internet en établissement scolaire](#)".

● Sécuriser les mots de passe

Chacun doit apprendre à choisir et gérer des mots de passe de manière à éviter toute usurpation de compte ([voir des conseils et astuces](#)).

Certaines applications informatiques donnent accès à des données dites "sensibles", et nécessitent un accès particulièrement sécurisé pour ceux qui peuvent y saisir des contenu.

Cet accès se fait alors par une **clef OTP**¹. Les conditions de commande et d'utilisations de ces clefs sont indiquées aux directeurs et aux chefs d'établissement dans le portail intranet académique.

 [Guide d'utilisation d'une clef OTP](#) (PDF de 914.7 ko)
Un document du Rectorat de Poitiers, 2010.

(1) One Time Password

Liens complémentaires

 [Eduquer aux risques d'Internet](#)

 [Pour respecter le droit à l'image des personnes : Documents adaptables](#)