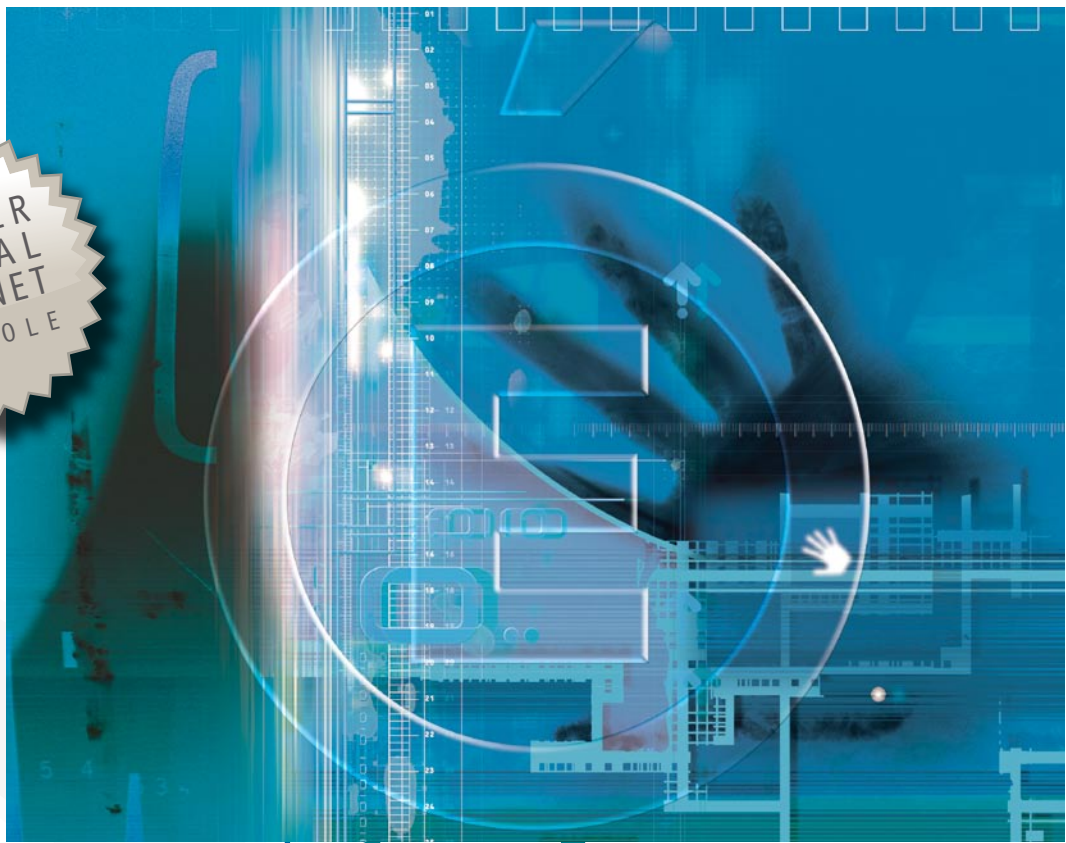


DOSSIER
SPECIAL
INTERNET
À L'ÉCOLE



PROTECTION DES
MINEURS DANS LE
CADRE PÉDAGOGIQUE

:: avec internet à l'école,
**la protection des mineurs
dans le cadre
pédagogique,**

***vous en avez
entendu parler ?***

Les usages développés par les **TIC**, impulsés par les pouvoirs publics, constituent un des axes majeurs pour l'enseignement et la recherche.

TIC :
Technologies
de l'Information
et de la
Communication

Aujourd'hui, avec la généralisation de l'internet haut-débit, les pratiques pédagogiques, déjà développées par l'Education Nationale, se sont généralisées.

C'est pourquoi, **il faut penser à la sécurité des mineurs et mettre en œuvre des mesures ou dispositifs adéquats pour les protéger.**



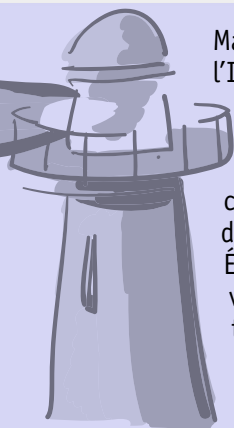
Plus
d'information
disponible
sur le document
«Référentiel de
la sécurité à
l'école»
(2006-2007)



:: les risques liés à internet,

Des précautions s'imposent ...

INTERNET : UN OUTIL INDISPENSABLE ...



Malgré les risques, la maîtrise de l'Internet s'avère indispensable à l'ensemble des élèves. Face à ces nouveaux défis, l'École a un rôle crucial à jouer comme lieu d'apprentissage et de familiarisation à l'Internet. Élèves et enseignants doivent à la fois s'appropriier ces technologies et leurs enjeux, en faire un véritable outil au service de la réussite scolaire.

Plus d'information disponible sur le document «Référentiel de la sécurité à l'école» (2006-2007)

:: Bien connaître le cadre réglementaire.

L'encadrement et la protection des mineurs, sont soumis à un **cadre réglementaire**.

En plus des principaux textes de loi traitant de la sécurité informatique, **il existe, au sein de l'Éducation Nationale, plusieurs textes officiels** (circulaires, projets et recommandations) ayant pour thème la protection des mineurs.

À savoir :

- la **Circulaire n°2004-035** du 18 février 2004 a vocation à organiser l'usage de l'Internet dans le cadre pédagogique et la protection des mineurs,
- le "**Plan d'action national de sensibilisation aux enjeux et aux risques de l'Internet**" qui dresse un premier bilan des mesures prises au sein de l'Éducation Nationale,
- les **guides pratiques** sur la sensibilisation et la protection des élèves mineurs face aux dangers de l'Internet. Un site internet à consulter : «legamedia»
- le **Brevet Informatique et Internet** qui atteste des compétences développées par les élèves tout au long de leur cursus scolaire lors d'activités intégrant les technologies d'information et de communication.



circulaire n°2004-035 : connue aussi sous le nom de circulaire «DARCOS»

LEGAMEDIA sur internet : <http://www.educnet.education.fr/legamedia>

1:: UTILISATION D'INTERNET les risques liés aux usages :



- La **consultation de sites avec contenus** pouvant porter atteinte au développement physique et mental des mineurs (pornographie, violence,...) voire illicites (pédophiles, xénophobes, racistes, antisémites, ...).
- Les **atteintes aux droits** de la propriété intellectuelle (musique, logiciels, films, dessins, ...).

Les conséquences ? :

Les **risques pénaux** portés sur les personnes physiques ou morales.

Plus d'information disponible sur le document «Référentiel de la sécurité à l'école» (2006-2007)

2:: UTILISATION D'INTERNET les risques liés à la sécurité des équipements informatiques :

- La **consultation de sites sans outil de protection**.

Les conséquences ? :

Réactions en chaîne, tels les virus, les codes malveillants, les **spywares** ou plus grave encore, la divulgation d'informations confidentielles.

SPYWARE : Logiciel espion (espionnage)

C'est essentiel !

Protection des mineurs : :: *Les moyens à mettre en œuvre !*

La sensibilisation des acteurs

Conformément aux textes officiels, un accompagnement des dispositifs de filtrage est prévu, avec des mesures de formation, de sensibilisation et de responsabilisation de l'ensemble des acteurs concernés :



Usagers, personnels de l'Éducation Nationale et élèves doivent être informés des spécificités de l'Internet.

Des actions d'information et de sensibilisation à destination des équipes éducatives et des élèves sont prévues par l'Éducation Nationale.

La responsabilisation, quant à elle, doit passer par la contractualisation de l'usage de l'Internet : chaque école devra établir **une charte d'utilisation de l'Internet** et l'annexer au règlement intérieur pour signature par les élèves et leurs parents.

Les mesures techniques

Conformément à la législation en vigueur, **c'est au maire, en collaboration avec l'Inspection Académique**, à qui il appartient de prendre les mesures nécessaires (obligation de moyens).

Il faut :

Identifier les besoins définis et validés par l'institution.

Choisir un dispositif technique qui permette de répondre aux impératifs de sécurité.

Prendre en compte les besoins des acteurs et des usagers.



Plus d'information disponible sur le document «Référentiel de la sécurité à l'école» (2006-2007)

En résumé, les moyens à mettre en œuvre au sein d'une école sont les suivants :

- 1) **le filtrage** : la mise en place d'un contrôle automatique des accès et pages consultés,
- 2) **l'authentification** : la reconnaissance des individus en tant que tels,
- 3) **la traçabilité** : une politique de stockage des écritures d'activité informatique.

La chaîne d'alerte

La chaîne d'alerte doit être utilisée afin d'informer l'ensemble des acteurs. La circulation de l'information est primordiale afin d'assurer une réponse optimale à chaque problème posé.



Directeur d'École



Inspection Académique



Cellule Académique



Cellule Coordination Nationale

+ sous cellule de gestion de la liste noire
+ sous cellule d'aide psychologique

La chaîne d'alerte doit être utilisée dans les cas suivants :

- 1) Découverte d'un site Internet inapproprié dans le cadre pédagogique et non filtré,
- 2) Découverte d'un site Internet approprié dans le cadre pédagogique et injustement filtré,
- 3) Découverte d'un site Internet illégal au regard de la loi française,
- 4) Demande de la part des médias d'explications en cas d'incident.



:: Une priorité ... la maîtrise des techniques usuelles de l'information et de la communication !

B2i :
Brevet Informatique et Internet.

Le B2i atteste des premières compétences acquises par l'enfant (dès la maternelle) pour lire et produire des documents, rechercher des informations, communiquer au moyen d'une messagerie et, déjà, adopter une approche citoyenne face aux informations véhiculées par les outils informatiques.

■ lire aussi sur internet :
<http://eduscol.education.fr/D0053/accueil.htm>

Après avoir été présentée comme l'une des priorités de la rentrée scolaire 2004, "la maîtrise des techniques usuelles de l'information et de la communication" est définie, dans la loi d'orientation et de programme, comme l'une des cinq composantes du socle commun de "connaissances et de compétences indispensables" qui doivent être acquises à la fin de la scolarité obligatoire. C'est dans ce cadre que l'attestation de compétences du **Brevet Informatique et Internet (B2i)**, graduée tout au long du cursus scolaire, est validée.



Il est important de noter que le B2i est accessible dès la maternelle.

Ainsi, dès aujourd'hui, nos enfants sauront transformer la maîtrise de ces outils en atouts

Plus d'information disponible sur le document «Référentiel de la sécurité à l'école» (2006-2007)

MINI QUIZZ

:: POINTS A VERIFIER //
LORSQUE VOUS N'ÊTES PAS SÛR(E) DE VOTRE RÉPONSE,
RÉPONDEZ «NON»

01 :: Evoquez-vous la sécurité informatique au cours du conseil d'école ?	OUI	NON
02 :: Existe-t-il des procédures de protection contre les virus ?	OUI	NON
03 :: Existe-t-il un document qui précise les règles de sécurité, les droits, les devoirs et les responsabilités des élèves utilisant l'informatique ?	OUI	NON
04 :: Chaque utilisateur(trice) est-il(elle) identifié(e) lorsqu'il(elle) utilise un système informatique ?	OUI	NON
05 :: Existe-t-il un filtrage des accès aux sites sur internet ?	OUI	NON
06 :: Un contrôle régulier du respect du droit à l'image, de la vie privée, de la conformité aux bonnes mœurs est-il effectué ?	OUI	NON

5 à 6 réponses OUI : Bravo, vous avez fait de réels efforts en matière de sécurité.
3 à 4 réponses OUI : Vous pouvez faire face à certains problèmes mais votre dispositif est encore trop exposé.
0 à 2 réponses OUI : La sécurité est désastreuse ! Vous êtes à la merci du moindre incident.

aix-marseille

rectorat
place Lucien Paye
13621 Aix-en-Provence, cedex 1

responsables de la publication
direction académique des technologies et des systèmes d'information (**datsi**)
téléphone 04 42 91 74 55
télécopie 04 42 91 70 10
ce.datsi@ac-aix-marseille.fr
conseiller pour les technologies de l'information et de la communication pour l'enseignement (**ctice**)
téléphone 04 42 91 75 91
télécopie 04 42 91 70 10
pole.tice@ac-aix-marseille.fr

date de parution
novembre 2006

illustration
marcel polo
photographies
licences computers art
& stéfane guilbaud
impression
spi imprimerie septèmes