

Utiliser Internet en milieu scolaire



Présentation de la leçon	2
Introduction	2
Navigation et recherche sur Internet	2
Le filtrage	3
Les listes noires	4
Signaler des sites illicites	5
Les cookies	5
Les signets	6
Échange avec des écoles étrangères	6
Le courrier électronique	6
L'interactivité	8
Forums	8
Le tchat ou clavardage	9
Les blogs	9
Glossaire	10

Présentation de la leçon

Objectifs :

Connaître les différents aspects éthiques et juridiques lors de l'utilisation de l'Internet en milieu scolaire.

Points du C2i2 : A.3. 2

« Prendre en compte les enjeux et respecter les règles concernant : la recherche et les critères de contrôle de validité des informations, la sécurité informatique, le filtrage Internet, etc ... »

Extrait du C2i.

Introduction

Internet se présente comme un outil pédagogique de premier ordre grâce aux facilités d'échanges et d'accès au savoir qu'il offre.

Cette facilité de création, d'échange ou de consultation de contenus ouvre de nouvelles perspectives à l'enseignement à la condition de respecter les valeurs et les principes du système éducatif.

Il ne serait question, sous prétexte de nouvelles capacités techniques, de bafouer les droits et intérêts des enseignants, des élèves ou des tiers.

Usage de l'internet dans le cadre pédagogique et protection des mineurs

La circulaire ministérielle du 18/02/2004 (parue au BO n° 9 du 26/02/2004) impose à tous les établissements scolaires une limitation et un contrôle de l'accès à Internet par les élèves.

Un certain nombre de dispositifs doivent donc être mis en place pour limiter l'accès à Internet et à protéger les mineurs.

Soucieux de la protection des mineurs, l'Education nationale mène une politique d'accompagnement sur Internet afin d'éviter l'accès à des sites inappropriés (par exemple pornographiques, pédophiles, xénophobes, racistes, antisémites, violents. En étroite coordination avec le correspondant sécurité (RSSI) présent dans chaque académie, les chefs d'établissements sont responsables de la mise en place des dispositifs de sécurité. Au sein des établissements, la protection des mineurs passe par les dispositifs de filtrage, la création de listes blanches ou noires de sites recommandés ou proscrits, le rappel des règles dans les chartes d'usage de l'Internet.

Le site pour la protection des mineurs sur l'Internet

<http://www.mineurs.fr/>

Des sites pour apprendre à surfer

<http://delegation.internet.gouv.fr/mineurs/juniors.htm>

Protection des mineurs sur Internet

<https://www.internet-mineurs.gouv.fr/>

Navigation et recherche sur Internet

En classe, il est de la responsabilité de l'enseignant de s'assurer que les élèves sont confrontés à des informations valides.

Dans les textes, il est aussi clairement écrit, qu'avec la lecture documentaire, non seulement, les élèves doivent comprendre les textes, mais aussi apprendre « par » les textes, pour confirmer ou valider des savoirs naissants.

Ainsi ils doivent apprécier de manière critique les informations trouvées au terme d'une recherche, ou plus précisément repérer l'auteur, la source de l'information et développer par rapport aux informations et aux connaissances véhiculées, des aptitudes à vérifier leur fiabilité.

Tous les B2i (école, collège, lycée) valident les compétences des élèves dans le domaine 2 : « **Adopter une attitude responsable** ». Et plus précisément on forme les élèves à « **Prendre conscience des enjeux citoyens de l'usage de l'informatique et de l'Internet et adopter une attitude critique face aux résultats obtenus** ». C'est le seul moyen de lutter contre les problèmes liés à la recherche sur Internet : **la surabondance, la désinformation, la contamination, l'invasion publicitaire.**

La validation de l'information repose sur l'utilisateur : c'est à l'internaute de valider, de vérifier sa fiabilité, d'évaluer sa qualité, de juger de sa pertinence...

Elle implique une formation longue et elle nécessite l'acquisition d'une véritable culture informationnelle. Connaissances qui ne sont pas simples à faire acquérir aux élèves.

Evaluer la fiabilité, la crédibilité, le sérieux... d'une source, d'un auteur, nécessite une connaissance minimale du sujet.

Evaluer la validité même d'une information, impose des connaissances disciplinaires, ou du domaine.

Juger de la cohérence interne, de la structuration d'un document et apprécier la lisibilité d'un document n'est pas simple pour des élèves. Ceci nécessite une grande maturité et un esprit critique développé.

Comment évaluer la qualité de l'information trouvée ? Démarche, questions à se poser.

- Pas de remède miracle, de solution technique satisfaisante, ni de "recettes" simples à appliquer...
- La vigilance, l'esprit critique, la culture générale et un certain nombre de compétences informationnelles sont les seules armes efficaces.

L'évaluation de la source ou de l'auteur : fiabilité, accessibilité, notoriété, degré de compétence... Ne suffisent pas forcément

L'évaluation de l'information proprement dite, du contenu : partie la plus difficile de l'évaluation, qui demande des connaissances minimales sur le sujet.. Il faut savoir apprécier la fiabilité de l'information, sa "fraîcheur", la précision, la qualité de l'expression, la richesse des sources, les références bibliographiques

...

L'évaluation de l'organisation du site ou du document, de la navigation... et donc distinguer tout ce qui relève de l'organisation, de la disposition de l'information, de la navigation dans les différentes pages par rapport au contenu.

L'évaluation de la mise en forme, de la lisibilité. Un site peut être très beau au plan visuel mais mal structuré et difficile à consulter (ou l'inverse).

L'évaluation de l'accessibilité, des aspects techniques

Pour une appropriation de l'internet à l'école et dans les familles

<http://www.educnet.education.fr/plan/proxima23.htm>

TP d'après Alexandre Serre

http://www.uhb.fr/urfist/Supports/StageEvalInfo/EvalInfo_TP.htm

Evaluer des sites Internet, Urfist Paris

<http://www.ext.upmc.fr/urfist/>

Propositions de démarches à mettre en oeuvre pour vérifier la fiabilité et des démarches à mettre en oeuvre pour vérifier la validité.

http://www.crdp-montpellier.fr/petiteshistoires/communs/docpp/la_validite.pdf

Comment évaluer de manière critique les ressources issues de l'Internet ?

<http://users.skynet.be/ameurant/francinfo/validite/>

Choisir les outils de recherche

Le filtrage

Les techniques de filtrage ne peuvent pas être efficaces à 100%, c'est pourquoi quelques précautions s'imposent dans le cadre d'un usage de l'Internet.

- Les élèves ont reçu des consignes de travail très précises (cadrage pédagogique).
- Les sites utiles ont été présélectionnés par l'enseignant (mise à disposition des adresses dans un traitement de texte par exemple)
- Dans le cas d'utilisation de moteurs de recherche, les élèves doivent avoir été sensibilisés, à travers la charte d'utilisation par exemple, à la conduite à tenir dans le cas où ils accéderaient malgré les dispositifs de filtrage à des sites jugés indésirables.

Chaque établissement doit à terme avoir mis en place un dispositif de filtrage. C'est la responsabilité du chef d'établissement. Il existe des solutions techniques ou logicielles pour bloquer l'accès des machines à certaines adresses ou certains types d'informations.

Le principe du filtrage repose sur une base de données qui liste l'ensemble des sites ou des mots-clés jugés indésirables. Si l'Internaute essaie d'accéder à un site listé ou classé sous un mot-clé interdit, son logiciel de navigation est bloqué par le filtre.

Le filtrage PICS sur les navigateurs (peu efficace)

C'est le concepteur de la page qui prend l'initiative de qualifier ces contenus en fonctions de critères prédéterminés.

Le navigateur prendra lui-même la décision d'afficher ou non la page à l'écran. Il s'agit d'une autoévaluation, qui n'est pas contrôlée par des organismes extérieurs ; seul un petit nombre de pages sont ainsi actuellement qualifiées. De plus, cette classification n'est applicable qu'au contenu d'une page web, et n'est pas adaptée ni adaptable aux services de messageries, de transfert de fichiers, de bavardage en ligne...

Le filtrage par logiciel dédié

Le logiciel de filtrage s'intercale entre le navigateur (ou tout autre logiciel) et internet. On trouve dans le commerce de nombreux logiciels de filtrage autonomes. Ces produits de filtrage reposent sur des listes de sites à filtrer, et des critères de filtrage par mots clés. Ces listes peuvent être des listes de sites interdits (liste noire), des listes de sites autorisés (liste blanche) ou une combinaison des deux.

Ce sont tantôt les éditeurs du logiciel de filtrage, tantôt les administrateurs du poste de travail qui dressent une liste de sites à interdire.

Le procédé de filtrage par mots clés permet dispense d'une classification des pages a priori en permettant analyse du site en direct. Il n'y a donc pas besoin de répertorier les sites.

Le filtrage des fournisseurs d'accès

Légalement, les fournisseurs d'accès sont tenus de proposer un dispositif de filtrage pour l'accès à l'Internet. (Article 43-7 de la loi relative à la liberté de communication n° 86-1067 du 30 septembre 1986) :

" Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée sont tenues, d'une part, d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, d'autre part, de leur proposer au moins un de ces moyens".

Les Académies fournissent des solutions d'accès à l'Internet accompagnée de services.

Exemple : Amplivia est le réseau haut débit déployé par la Région Rhône-Alpes. Les avantages à ce raccordement sont nombreux : filtrage, protection contre les intrusions, coût d'abonnement,...

Guide pratique de mise en place du filtrage sur Internet

<http://www.educnet.education.fr/aiedu/guide1.htm>

Les différents modes de filtrage

<http://www.mineurs.fr/pratique.htm>

Point de contact proposé par les fournisseurs d'accès adhérents

<http://www.pointdecontact.net/index.html>

Les listes noires

Une liste noire contient un ensemble de sites ou domaines à exclure de la navigation. C'est donc un ensemble de sites interdits.

En cas de problème ?

Alerter le chef d'établissement qui prendra une décision en fonction des solutions techniques disponibles :

- Supprimer localement l'accès au site.
- Communiquer l'adresse du site à l'éditeur du logiciel de filtrage par l'intermédiaire des moyens qu'il a mis à votre disposition.
- Signaler le site au fournisseur d'accès

Dans tous les cas, déclarer le site sur la "liste noire" nationale.

Ces listes noires permettent de créer, dans l'Éducation nationale un internet où tout est autorisé sauf la consultation de quelques sites. On garde donc la possibilité de naviguer librement d'un site à l'autre, tout en restreignant les risques d'accéder à un site inapproprié. La spécificité de l'internet reste donc conservée.

Informations sur les listes noires

<http://www.educnet.education.fr/aiedu/listenoire.htm>

Les alternatives aux systèmes de filtrage

http://www.aix-mrs.iufm.fr/C2i/article.php3?id_article=50

Signaler des sites illicites

Signaler le site au responsable de l'établissement qui, selon les cas, pourra alerter la cellule académique chargée de cet aspect, pour une prise en charge au niveau académique.

Tout signalement effectué au moyen du formulaire sur le site est enregistré automatiquement dans une base de données gérée par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC - Ministère de l'intérieur, Direction Centrale de la Police Judiciaire).

Ce service effectuera les premières vérifications (techniques et juridiques) et transmettra le signalement aux services de police ou de gendarmerie territorialement compétents. Après validation du formulaire que vous aurez rempli, il vous sera communiqué le numéro de référence de cet enregistrement. Vous pouvez faire un signalement anonyme. Dans ce cas, vous ne serez pas informé de la suite donnée.

Guide pratique de mise en place du filtrage sur Internet

<http://www.educnet.education.fr/aiedu/guide1.htm>

Les différents modes de filtrage

<http://www.mineurs.fr/pratique.htm>

Point de contact proposé par les fournisseurs d'accès adhérents

<http://www.pointdecontact.net/index.html>

Les cookies

Un cookie est un fichier qui va permettre au serveur de vous reconnaître la prochaine fois que vous reviendrez sur un site que vous avez visité. Il est stocké sur votre disque dur pendant plusieurs mois, voire plusieurs années ou bien seulement envoyé le temps de la visite du site et aussitôt supprimé dès la fin de la consultation (par exemple : cookie permettant le paramétrage des pages selon les caractéristiques de l'écran de l'internaute).

Le cookie enregistre vos préférences (par exemple : les options que vous aurez cochées) pour vous éviter des les ressaisir mais ne vous identifie pas en tant que personne.

Cela est a priori, sans danger sauf si un recoupement est effectué avec des renseignements personnels qui peuvent être glanés sur une page web en profitant de la naïveté de jeunes utilisateurs (par exemple : un jeu concours auquel il faut s'inscrire). Cela est désormais réglementé par des dispositions communautaires.

Il est possible de gérer les cookies :

- soit en éliminant les cookies conservés par votre ordinateur
- soit en paramétrant votre navigateur afin qu'il vous avertisse de la création d'un cookie ou bloque automatiquement l'accès à l'ordinateur.

De la protection de la vie privée : des cookies indigestes

<http://securinet.free.fr/annexe/cookiesindigestes.html>

Anonymat sur Internet

<http://www.commentcamarche.net/securite/anonym.php3>

Les signets

Le principal risque lié à la constitution d'une collection de signets se résume à la situation où l'un des signets conduit à un site non conforme aux règles de protection des enfants. Il peut s'agir de contenus à caractère violent, haineux, raciste ou pornographique. Il est donc de la responsabilité de l'enseignant ou de l'assistant « Internet » de vérifier périodiquement les sites listés par les signets et le cas échéant de remettre à jour la collection de signets.

Plus généralement, une information préventive des élèves sur les sites jugés « indésirables » compte tenu des règles d'utilisation de l'Internet en milieu scolaire, est un moyen simple et efficace de minimiser les risques, surtout si ce sont les élèves eux-mêmes qui créent la collection de signets.

Echange avec des écoles étrangères

On envisage ici la situation de coopération entre établissements scolaires participants à des projets pédagogiques internationaux. Il est souhaitable que l'utilisation de l'internet en milieu scolaire permette un plus grand rapprochement des cultures, à l'instar des échanges linguistiques.

Cependant, cela pose la question du droit applicable aux activités en ligne. L'enjeu est de savoir quelles règles s'appliquent aux activités en ligne. A titre d'exemple, les élèves d'un collège français et d'une école américaine échangent des propos sur un forum de discussion ou créent un site Web commun. Des propos négationnistes sont diffusés. Aux Etats- Unis, cet acte n'est pas répréhensible, alors qu'en France son auteur sera poursuivi pénalement. Il est donc important de connaître le droit applicable.

Correspondance scolaire

http://www.primlangues.education.fr/php/correspondance_scolaire-international.php

Le courrier électronique

Les fonctions de transmission du courrier électronique, dédient le courrier électronique à un usage interpersonnel qui favorise la correspondance privée.

C'est pourquoi les principaux risques liés à ce contexte de communication concernent avant tout les atteintes aux droits des personnes, et plus particulièrement à leur vie privée et incidemment au droit d'auteur. Dans une moindre mesure et comme tout service de communication, l'usage du courrier électronique peut également entraîner des risques pour la collectivité.

Un message électronique est un courrier privé dans la mesure où il est envoyé à une ou plusieurs personnes physiques ou morales déterminées. Il est de ce fait couvert par les dispositions légales concernant les correspondances privées. Il n'est pas permis de créer une boîte email à un élève mineur sans l'autorisation de ses parents ou tuteurs, ni d'ouvrir la messagerie d'un élève.

Attention : La fonction "faire suivre un message"

Un mauvais usage de la fonction "faire suivre un message" peut conduire à commettre un délit. Un contenu confidentiel envoyé à une personne déterminée peut ainsi être réexpédié à d'autres personnes. Le destinataire du message confidentiel doit prendre garde de ne pas le diffuser. Il doit respecter la confidentialité de la correspondance.

Attention : La fonction « fichier joint »

Cette fonction ne doit transmettre des photos privées d'une personne à des tiers qu'avec le consentement de la personne photographiée.

Par le biais de la fonction "pièce jointe", le courrier électronique peut transmettre des fichiers textuels, visuels ou musicaux sans l'autorisation de leur auteur. Dans ce cas, il y a atteinte au droit d'auteur ou plus précisément non respect du droit de reproduction.

Compte tenu du caractère privé reconnu au courrier électronique, il est risqué pour le responsable du serveur de contrôler les échanges. La loi protège le secret des correspondances.

« Le fait, (...), d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions »

Depuis quelques années, l'utilisation du courrier électronique est largement perturbé par le développement du spamming ou pollupostage.

A l'origine, le spamming résulte de la collecte d'adresses électroniques personnelles sur des sites webs, des listes de diffusion, des forums de discussion, sans que la personne concernée y ait consentie, et sans même en avoir été avertie. Ces adresses sont ensuite intégrées dans des listes constituées par des organismes dans le but de diffuser des messages non sollicités, c'est à dire sans qu'il y ait une demande expresse de la part des personnes visées.

Suite à cette collecte d'adresses électroniques, les messages sont envoyés sur les boites aux lettres, de manière répétée, avec des contenus préjudiciables, choquants, ou simplement inutiles. Ces courriers électroniques sont alors considérés comme abusifs.

Plusieurs conséquences :

Les atteintes aux droits des personnes : les données à caractère personnel, telles que les adresses électroniques, sont protégées. Avant d'envoyer des messages, la personne ou l'organisme émetteur devrait se conformer aux règles suivantes mises en place afin de protéger les titulaires d'adresses électroniques.

- Déclaration préalable à la CNIL
- Obligation d'information
- Droit d'opposition
- Obligation d'assurer la sécurité des informations

La pratique du spamming ne respecte pas ces obligations légales

Les perturbations du trafic : L'envoi massif de messages non sollicités, a pour conséquence directe l'encombrement du trafic sur l'Internet. Les délais de connexion sont plus longs, les détenteurs de boîte aux lettres perdent du temps à trier leur courrier.

Conseils :

- dans le cas d'ouverture d'une boîte à lettre pour chacun des élèves, il faut demander une autorisation parentale. Les parents sont responsables hors temps scolaire, l'enseignant est responsable dans le temps scolaire. Les contenus sont privés, donc soumis à l'autorisation de l'élève dès lors que l'enseignant souhaite en prendre connaissance. Il est plutôt souhaitable d'ouvrir une boîte collective pour la classe sous un nom générique.

Il existe un accord cadre entre la Poste et l'éducation nationale

<http://education.laposte.net>

Gestion du courrier électronique en établissement

<http://www2.ac-rennes.fr/crdp/29/ie/aides/internet/courrier.html>

L'interactivité

Les espaces interactifs (forum, tchat, blog) qui permettent aux élèves de diffuser des éléments sur le net doivent être contrôlés pour s'assurer de leur bon usage.

Les espaces de discussion présentent des risques (propos violent, injurieux, racistes ou diffamants).

Diffusés facilement auprès d'un grand nombre d'internautes, les messages postés sur les forums ou les listes peuvent porter un grave préjudice à la vie privée des personnes.

L'atteinte à la vie privée de victimes est répréhensible si la divulgation de messages indiscrets est faite sans leur consentement. C'est pourquoi une réparation civile au bénéfice des victimes est possible en vertu du droit à la vie privée. De plus, le ou les auteurs des messages indiscrets sont également condamnables pénalement.

• Forums

Les forums peuvent voir leur thème débordé par des messages dont le contenu a un caractère raciste, offensant, injurieux, diffamatoire ou haineux. Dans le cas du forum où les messages archivés sont libres d'accès, l'atteinte à la réputation est toujours publique et est réprimée comme diffamation et injure publique.

Conseil pratique :

- Privilégier les forums fermés, dont les thématiques dépendront de l'âge des participants,
- Prévoir un modérateur qui appréciera la licéité des messages avant publication,

- Elaborer une charte de participation au forum rappelant l'interdiction des propos diffamants ou injurieux, le respect des droits à l'image ou des droits d'auteur, l'interdiction de l'anonymat.

Peuvent être considérés comme responsables : l'auteur du message bien sûr, mais également l'éditeur du site et le modérateur du forum.

En particulier en milieu scolaire où est requis un cadre protecteur des mineurs, doit être proscrite toute discussion conduisant à des messages à caractère haineux, racistes ou antisémites ou pornographiques.

L'ordre public protège également les mineurs contre les contenus à caractère violent, pornographique ou pédophile. Autre risque pour un public mineur, les forums ou les listes de discussion sont aussi un des moyens privilégiés par les réseaux pédophiles pour atteindre leurs victimes.

Conseils pratique :

Il est recommandé aux enseignants d'informer les élèves des risques courus lors de discussions sur des listes ou forums avec des tiers inconnus, en particulier des dérives possibles en matière de pédophilie.

Forum de l'école de la providence

<http://ecolelaprovidence.free.fr/forum.php>

• Le tchat ou Clavardage

Les types de risques

Se sentant protégés par l'anonymat et la fugacité de la conversation, des participants, peuvent tenir des propos déplacés. Tout l'enjeu des règles à élaborer est de faire cesser ce sentiment d'impunité. Pour l'échange de tels contenus, leurs auteurs peuvent être poursuivis pénalement.

Le tchat est aussi un des moyens privilégiés par les réseaux pédophiles pour atteindre leurs victimes. Grâce à l'anonymat, des internautes adultes peuvent emprunter un âge, une personnalité différents pour correspondre avec des enfants.

Les enfants peuvent fournir des informations qui les identifient ou les localisent (nom, adresse, numéro de téléphone, école fréquentée, etc....) ou recevoir des images indécentes.

Clavardage = clavier + bavardage

<http://perso.wanadoo.fr/ecole.chabure/clavardage/>

• Les blogs

Les blogs, comme les sites Internet, doivent contenir des mentions légales. Même les enfants mineurs peuvent être pénalement responsables de leurs écrits.

Il appartient aux adultes encadrants d'intervenir auprès de l'enfant pour qu'il retire de son blog tout contenu illicite. L'adulte se doit d'organiser un travail de sensibilisation et d'information sur les enjeux et les risques des blogs.

Les blogs permettent un travail collaboratif et peuvent tout particulièrement contribuer à l'amélioration de

l'expression écrite des élèves. Mais ils doivent être particulièrement contrôlés par les adultes.

Les enfants ignorent souvent que la diffusion d'information sur l'internet peut les exposer à de nombreux recours légaux, contre eux-mêmes et leurs parents.

Dans un blog, le responsable de la publication ne peut :

- diffuser des productions intellectuelles sans l'accord des personnes qui en détiennent les droits
- diffuser des données sur la vie privée des personnes ou permettant leur identification sans obtenir l'accord de la personne concernée ou, le cas échéant, de la CNIL.
- diffuser des propos diffamatoires, injurieux, violents, pornographiques, qui porteraient atteinte au respect de la personne ou inciter à la violence, au racisme ou à la xénophobie
- inciter le banditisme, le vol, la haine ou tout crime ou délit

Les blogs sous le feu de l'actualité

<http://www.educnet.education.fr/articles/blogs.htm>

Le droit des blogs

http://www.droitdunet.fr/telechargements/guide_blog_net.pdf

Glossaire

Cache

Un cache stocke temporairement les informations contenues sur une page web dans le disque dur de votre ordinateur. La première fois que vous demandez une page, votre navigateur la récupère sur Internet et la place dans le cache. Ainsi, si vous demandez une page déjà consultée, il vérifie si elle est disponible dans le cache.

Cookie

Petit programme informatique qui vient s'insérer automatiquement et à l'insu de son utilisateur sur son disque dur à la suite d'une consultation internet et qui sert à mémoriser certaines de ses caractéristiques personnelles qu'il retrouvera à sa prochaine visite (ex : adresse de messagerie et mot de passe)

Proxy

Abréviation de Proxy Server. Ce terme désigne un serveur internet, généralement géré par un fournisseur d'accès, qui contient une copie des pages les plus demandées afin d'améliorer la distribution des informations aux internautes.

POP

Post Office Protocol sert à la ventilation du courrier électronique et donc à la réception de celui-ci .

SMTP

Simple Mail Transfert Protocol est spécialisé pour l'envoi, le transport des messages électroniques.