Guide pratique de mise en place du filtrage

De la nécessité du contrôle

Le taux de pénétration de l'Internet dans les écoles et établissements scolaires est de plus en plus important. La facilité d'accès et la multiplicité des sites posent le problème de la maîtrise de l'outil dans un cadre pédagogique. Afin d'aider les utilisateurs et d'accompagner les élèves dans leur utilisation de l'Internet, un contrôle des documents consultés et des informations fournies est nécessaire.

POUR LA PÉDAGOGIE

Lors d'une séquence pédagogique, l'enseignant peut souhaiter développer l'exploration des ressources de l'Internet par ses élèves en autonomie. La personne responsable de l'activité ne peut pas accompagner chacun des élèves en permanence, il faut donc que cette pratique soit encadrée afin de permettre une utilisation la plus enrichissante possible.

Ce cadrage de l'activité repose sur deux aspects : une formation et une sensibilisation à la spécificité de l'Internet pour tous les acteurs de l'établissement ou de l'école, et sur un contrôle des informations consultées.

POUR LA PROTECTION DES MINEURS

Un certain nombre de sites peuvent présenter un contenu préjudiciable voire illégal, pour les élèves mineurs ou l'ensemble de la communauté éducative. La navigation libre sur l'Internet est un processus de passage d'un site à un autre, parfois sans liens entre eux. Afin d'éviter l'accès à des sites inappropriés (par exemple pornographiques, pédophile, xénophobes, racistes, antisémites, violents, …), la navigation sur l'Internet doit être contrôlée.

Il est donc indispensable de mettre en place une politique d'accompagnement sur Internet.

Toute mise à disposition de documents suppose un choix et donc une sélection dans le fond comme dans la forme vers l'intérêt de l'élève. Il semble donc naturel et indispensable que les établissements et écoles disposent de moyens d'accompagnement et de contrôle de l'usage de l'Internet dans le cadre pédagogique.

Organisation des dispositifs

RÔLE DU CHEF D'ÉTABLISSEMENT ET DE LA COMMUNAUTÉ ÉDUCATIVE

La mise en place des dispositifs dans les établissements ou les écoles doit se faire sous la direction des chefs d'établissement ou des directeurs d'école, u plus près des usagers et en particulier des équipes éducatives.

La communauté éducative est en contact constant et direct avec les élèves. Elle est donc la plus à même de transmettre la sensibilisation et la pédagogie associée à l'Internet. C'est en effet au travers d'une véritable pédagogie que la bonne utilisation de l'Internet est possible.

Ces sensibilisations et formations doivent être coordonnées au niveau académique.

RÔLE DE L'ACADÉMIE

Pour mener à bien ces opérations de formations et de sensibilisations, l'académie possède un certain nombre de compétences, en particulier par l'intermédiaire du CTICE et de son équipe avec le support du correspondant sécurité (RSSI).

Ces actions pourraient revêtir la forme suivante :

- Formation/sensibilisation des chefs d'établissement et des directeurs d'école par les services de l'académie.
- Répercussion auprès de l'équipe pédagogique au sein de l'établissement ou de l'école.

Les moyens techniques à mettre en œuvre

Afin de rendre possible le travail en autonomie, un contrôle automatique des pages consultées doit être mis en place. Deux stratégies peuvent être mise en œuvre : un contrôle a priori des sites en interdisant l'accès à des sites inappropriés, et un contrôle a posteriori par analyse de la liste des sites consultés.

Des dispositifs techniques permettent de restreindre les accès à l'Internet selon le profil de l'utilisateur connecté. Le principe du filtrage permet de présenter les documents adaptés au profil de l'utilisateur.

LE FILTRAGE PICS SUR LES NAVIGATEURS :INSUFFISANT

Les principaux navigateurs proposent une fonction de filtrage des contenus Internet au niveau du poste de l'utilisateur. En pratique, cela signifie que c'est le navigateur lui même qui va prendre la décision d'afficher ou non une page à l'écran.

Cette fonctionnalité repose sur un système d'évaluation des sites des pages web visitées. Ce système d'évaluation consiste en une série de catégories et de niveaux dans chaque catégorie, utilisée pour classifier le contenu de la page.

Cependant, l'évaluation des sites est réalisée par les concepteurs même de la page et à son initiative. Il s'agit d'une auto-évaluation, qui n'est pas contrôlée par des organismes extérieurs ; seul un petit nombre de pages sont ainsi actuellement qualifiés. 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…

L'efficacité de PICS dépend très fortement de l' adhésion des concepteurs de sites ou des organismes d'évaluation externes. A l'heure actuelle, ce n'est pas le cas, peu de sites sont classifiés.

Si le choix est fait de refuser tous les sites non classifiés, l'utilisation de l'Internet se trouve fortement limitée : de nombreux sites, non classifiés, vont être bloqués lors de la navigation alors qu'ils peuvent correspondre au profil de l'utilisateur. Par conséquent, ce système ne peut pas remplir le rôle de filtrage et ne répond donc pas aux objectifs de l'éducation nationale.

LISTE NOIRE ET LISTE BLANCHE

Définition d'une liste noire

Une liste noire contient un ensemble de sites, motifs génériques (par exemple toutes les adresses contenant le mot « nue ») ou domaines à exclure de la navigation. C'est donc un ensemble de sites interdits.

Définition d'une liste blanche

Une liste blanche contient l'ensemble des sites sur lesquels la navigation peut avoir lieu. C'est dons un ensemble de sites autorisés.

FILTRER AU NIVEAU DU SERVEUR MANDATAIRE

Le serveur mandataire (« serveur proxy »), centralise l'ensemble des accès aux ressources web de l'Internet en provenance des postes clients. Les postes clients s'adressent au serveur mandataire afin d'accéder à l'Internet et ne peuvent accéder au contenu que par son intermédiaire. L'accès aux ressources de l'Internet par d'autres moyens (changement de port, utilisation d'un serveur mandataire extérieur,…) devrait, dans la mesure du possible être interdit afin de garantir un niveau de sécurité optimal.

En tant qu'intermédiaire, le serveur mandataire peut donc décider si l'accès aux ressources demandées

doit être accepté. L'ensemble des contenus, qu'ils s'agissent d'une page web, d'un site de bavardage, d'un site de courrier électronique, etc. sont analysés.

Une action a été engagée par le Ministère afin de développer et de généraliser de tels dispositifs dans les établissements et les écoles, notamment à travers le projet S2I2E. C'est la solution qui permet d'avoir le contrôle le plus fin sur l'ensemble des contenus, elle est donc à retenir en priorité.

UTILISATION DE LOGICIELS SUR LE POSTE CLIENT

Il existe sur le marché des logiciels de filtrage autonomes, au niveau du poste de l'utilisateur et qui ne se basent pas sur le système PICS.

Ces produits de filtrage reposent sur des listes de sites à filtrer, et des critères de filtrage par mots clés.

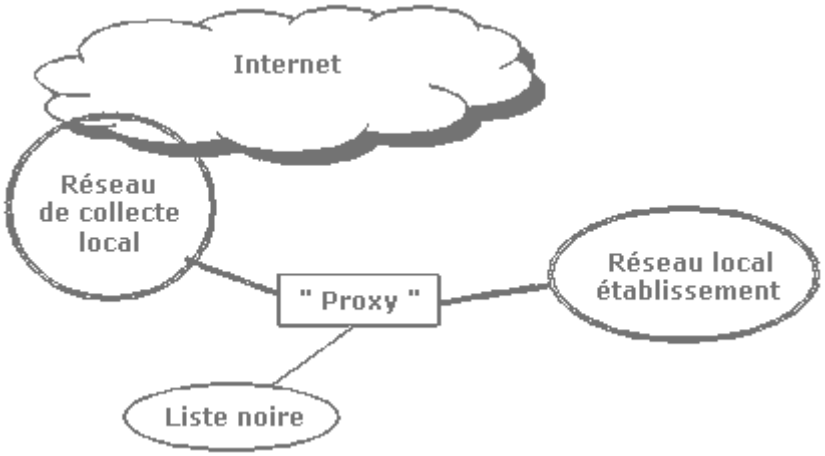
Ces listes peuvent être des listes de sites interdits (« liste noire »), des listes de sites autorisés (« liste blanche ») ou une combinaison des deux.

Ce type de logiciel ne demande donc pas d'évaluation du site par le concepteur, mais ce sont directement les éditeurs du logiciel de filtrage qui peuvent fournir une liste de sites à interdire. Ce sont aussi les administrateurs du poste de travail qui peuvent sélectionner cette liste.

Le procédé de filtrage par mots clés permet de se passer d'une classification des pages a priori en utilisant une analyse du site à la volée. Il n'y a donc pas besoin de répertorier les sites.

Architectures proposées et solutions logicielles

SOLUTION AU NIVEAU DU SERVEUR MANDATAIRE : ADAPTÉ À UNE ARCHITECTURE MULTIPOSTE OU MUTUALISÉE



Le serveur mandataire est le passage obligé de toute connexion. Il n'y a donc pas de contournement possible, toutes les pages et tous les contenus seront analysés par le dispositif.

<< Architecture type

Serveurs mandataires disponibles avec dispositif de filtrage intégré

Parmi les serveurs mandataires disponibles, à la fois dans le domaine du logiciel commercial que dans le domaine du logiciel libre, certains proposent des fonctionnalités de filtrage.

Ces serveurs mandataires permettent d'interdire l'accès à certaines pages web, en redirigeant les requêtes vers une page déterminée. Ils permettent donc de réaliser un contrôle a priori des informations consultées. Ces serveurs sont aussi utilisable pour réaliser le contrôle a posteriori : à partir d'une liste de sites inappropriés, ils permettent d'enregistrer tous les accès à ces sites associés à une identification.

Le logiciel Squidguard

Ce logiciel libre est intégré dans plusieurs projets soutenus par l'Education Nationale : EOLE, SLIS, pingoo, linuxedu, etc.

Il s'agit d'un greffon (« plugin ») destiné à Squid qui est un serveur mandataire libre très utilisé. Ce greffon apporte les fonctionnalités de filtrage.

Il permet entre autre fonctionnalités de :

- Bloquer l'accès à un ensemble de sites définis par une liste noire pour certaines catégories d'utilisateurs
- Rediriger un accès à une page interdite vers une autre page
- Limiter l'accès à l'Internet dans le temps en définissant des plages horaires d'accès selon les profils
- Autoriser l'accès à un nombre limité de pages web en proposant des fonctionnalités de type liste blanche
- Le serveur mandataire Squid permet l'authentification de l'utilisateur

De plus amples renseignements techniques sont disponibles sur le site de Fabrice Prigent à l'Université de Toulouse 1, http://cri.univ-tlse1.fr/documentations/cache/squidguard.html ou sur le site du logiciel http://www.squidguard.org (en anglais).

Le logiciel Dansguadrian

Dansguardian est un logiciel disponible sous une licence libre pour toute utilisation non commerciale. Il s'agit d'un greffon pour le serveur mandataire Squid, qui apporte des fonctions de filtrage multiples.

En complément des fonctionnalités de SquidGuard et de Squid, il permet de :

- Examiner le contenu des pages pour détecter les contenus inappropriés, en analysant les structures de phrases, des éléments de pagination et le vocabulaire type utilisé.
- Limiter la quantité de données transmise du réseau interne de l'école vers le serveur de la page web, par exemple pour limiter l'utilisation de pièces jointes dans les courriers électroniques.

Dansguardian utilise le même format de données que Squidguard pour définir les listes noires. Ces deux logiciels peuvent donc avoir une liste noire commune. Cependant, Dansguardian n'est pas directement intégré dans les projets nationaux.

Les logiciels commerciaux

Des logiciels commerciaux proposant les mêmes types de fonctionnalités sont disponibles. Voici une liste non exhaustive :

CheckPoint

I-Gear

WebSense (http://www.websense.com)

Bess (http://www.n2h2.com/products/bess_home.php)

Surfcontrol (http://www.surfcontrol.com)

Les listes disponibles

Les listes noires permettent de définir un ensemble de sites interdits par l'intermédiaire de domaines interdits, d'URL interdites, de fichiers interdits et de motifs généraux dans les adresses internet. On peut par exemple imaginer que dans ces listes noires seront présent les adresses de sites pornographiques, de sites racistes, etc. Ces listes noires peuvent aussi fournir des motifs génériques indiquant des sites à proscrire : par exemple, on peut interdire les fichiers MP3, des fichiers exécutables, etc.

Différents niveaux de listes noires sont à prévoir, afin de pouvoir adapter le filtrage aux situations pédagogiques :

- Des sites illégaux
- Des sites inappropriés
- Autres sites

Les sites illégaux ne pourront pas être consultés, quel que soit le profil de l'utilisateur ou la situation pédagogiques. Les sites inappropriés sont définis relativement à une tranche d'âges, une situation pédagogique, un profil d'utilisateurs, etc.

Les listes noires permettent de créer un Internet où tout est autorisé sauf la consultation de quelques sites. On garde donc la possibilité de naviguer librement d'un site à un autre, tout en restreignant les risques d'accéder à un site inapproprié. La spécificité de l'Internet reste conservée. Cependant, une liste noire ne peut jamais être exhaustive : le nombre de sites disponibles sur l'Internet augmente de jour en jour, il n'est pas possible de prendre en compte la totalité des sites. Une liste noire répertorie un maximum de sites, et non la totalité. La participation de chacun, par l'intermédiaire de la remontée d'informations, permet de compléter cette liste et d'augmenter les performances des listes noires.

Les listes blanches permettent d'autoriser des sites. Ce type de liste peut être utile dans le cadre d'un travail en autonomie complète, sans contrôle de l'enseignant. Dans ce cas la recherche d'informations se rapproche d'une recherche dans une documentation.

Une structure nationale au niveau interministériel est mise en place afin de coordonner et de centraliser l'offre de liste noire. Les partenaires (Ministère de l'Intérieur, délégation à la famille, MJENR, etc.) contribueront dans leur domaine respectif à améliorer et pérenniser cette liste ainsi que la structure et le suivi institutionnel. Un site de référence (site sur educnet) a été créé afin de regrouper l'ensemble des informations et des moyens mis en place par cette structure.

A l'heure actuelle, une liste « noire » est librement téléchargeable à l'adresse (site sur educnet). Les procédures d'utilisation sont détaillées à l'adresse (site sur educnet). Cette liste est une liste au format texte pur, adaptable facilement à un ensemble de format, dont le format des listes SquidGuard.

Des procédures automatisées de mise à jour des listes sont mises en place afin de pouvoir prendre en compte rapidement les ajouts et suppression proposés par les équipes locales.

Par ailleurs, des listes internationales sont disponibles sur le site de SquidGuard http://www.squidguard.org/blacklist/ (site en anglais).

Installation et configuration

Le logiciel Squidguard est intégré dans les solutions suivantes :

SLIS (http://slis.ac-grenoble.fr/),

EOLE (http://eole.orion.education.fr/),

Pingoo (http://www.pingoo.org/),

AbulEdu (http://www.abuledu.org/).

Des instructions d'installation sont disponibles sur les sites de chacun de ces projets. En particulier, ces projets permettent d'automatiser la mise à jour de la liste « noire » utilisée. On est alors sûr d'utiliser la dernière version de la liste noire disponible.

Annuaire et identification

Les projets globaux SLIS, EOLE, Pingoo proposent la gestion de comptes utilisateurs par l'intermédiaire d'un annuaire LDAP. Ce dernier est installé automatiquement à l'installation, à partir de la base de données de l'établissement, et permet d'assurer l'identification de l'utilisateur lors de la navigation sur l'Internet par l'intermédiaire du serveur mandataire.

Cette identification de l'utilisateur peut être conservée dans les traces relatives aux connexions.

Informations à conserver

Afin de pouvoir gérer d'éventuels incidents et de pouvoir perfectionner les listes noires disponibles, il est indispensable de conserver les informations de connexions (« logs ») des usagers. Les informations de connexion doivent le groupe d'usagers ainsi que la personne qui accède à chaque ressource sur l'Internet.

La durée de conservation doit être suffisante pour permettre de traiter un incident découvert tardivement, c'est à dire une durée de 3 à 6 mois. La conservation de ces informations peut être réalisée de différentes manières : une conservation locale ou une conservation extérieure à l'établissement.

Les traces devront être analysées régulièrement, afin de garantir l'efficacité du dispositif de filtrage. Les informations extraites de ces fichiers, par exemple lors d'incident ou d'accès à des contenus inappropriés

seront transmises, via la chaîne de remontée des incidents, au RSSI qui est le référent unique en matière de sécurité et de filtrage au niveau académique.

Les traces pourront être analysées à l'aide de programmes de type scripts, afin de systématiser et d'améliorer l'efficacité de cette analyse. Des scripts d'analyse peuvent par exemple être trouvés sur la page http://cri.univ-tlse1.fr/documentations/cache/squidguard.html, afin de détecter les pages inappropriées non filtrées par la liste noire.

SOLUTION SUR LE POSTE CLIENT : ADAPTÉ À UNE ARCHITECTURE MONO-POSTE

Les petites structure, en particulier les petites écoles ne possèdent parfois qu'un seul poste relié directement à l'Internet, sans réseau local interne à l'école ou à l'établissement.

Dans ce cas précis, la solution du serveur mandataire n'est peut-être pas la mieux adaptée, notamment pour des raisons de moyens. L'utilisation d'un logiciel de filtrage sur le poste client, au niveau du poste unique, semble plus pertinente, bien que moins performante.

Les magazines « 60 millions de consommateurs » et « le point » ont testé des logiciels proposant ces fonctionnalités. Les résultats sont consultables sur le site de ces éditeurs, aux adresses suivantes :

http://www.lepoint.fr/pointcom/document.html?did=137005
http://www.60millions-mag.com/images_publications/349_logiciels_filtrages-ok.pdf

La formation et la sensibilisation

Le filtrage logiciel des accès à l'Internet est nécessaire et permet de canaliser les accès. Cependant la voie de la responsabilisation et de la sensibilisation est indispensable et elle doit s'inscrire dans le cadre plus général de l'éducation à la citoyenneté.

Les utilisateurs, personnels de l'Éducation et élèves, doivent être mis en garde contre les dangers et abus possibles liés à l'Internet. Aussi, des actions de formation et de sensibilisation, dont les modalités sont à définir par les académies, à destination de l'ensemble des établissements scolaires et écoles doivent être mises en place. Elles pourraient revêtir les formes suivantes :

- Formation des chefs d'établissement et des directeurs d'école
- Répercussion auprès de l'équipe pédagogique par l'équipe dirigeante.

La sensibilisation des personnels doit être fait au plus proche de l'établissement ou de l'école. Les chefs d'établissement ou les directeurs d'école sont en relation permanente avec les membres de la communauté éducative et en collaboration avec les ressources académiques, en particulier le CTICE aidé par le RSSI, ils pourraient être chargés de répercuter à l'ensemble des personnels la formation et la sensibilisation à l'utilisation de l'Internet qu'ils ont reçus.

La sensibilisation des élèves peut entre autre avoir lieu selon deux axes :

- La mise en place d'une charte d'utilisation des ressources de l'Internet, détaillée ci dessous.
- Le B2I, Brevet Informatique et Internet, est un cadre parfaitement adapté à la transmission des problématiques liées à l'Internet et à une sensibilisation à l'usage des ressources. Le B2I est en voie de généralisation dans les écoles, collèges et lycées, ce qui permet de s'adresser à l'ensemble des élèves concernés.

Les chartes

MISE EN ŒUVRE

Une charte d'utilisation des ressources TIC doit être établie dans chaque établissement. Elle doit être jointe au règlement intérieur. Afin d'avoir une valeur de contrat entre l'élève et l'établissement, elle devra être signée par les élèves et les parents, pour les élèves mineurs.

Cette charte précisera les activités autorisées selon les personnes, selon les séquences pédagogiques, et devra préciser les sanctions associées à une utilisation inappropriée.

La charte de l'établissement doit être expliquée et détaillée aux élèves par l'équipe pédagogique, au même titre que le règlement intérieur. Les discussions associées contribuent à la formation civique et citoyenne

des élèves. Elles font donc partie intégrante du dispositif éducatif.

Exemple de chartes

L'Education Nationale a mis au point une charte nationale type à destination de élèves. Elle est disponible à l'adresse suivante http://www.educnet.education.fr/chrgt/charteproj.pdf .

Cette charte est à adapter aux spécificités de chaque établissement ou école.

Parallèlement, il est important que les personnels de l'éducation nationale signent aussi une charte d'utilisation des ressources de l'Internet. Une charte est en cours de validation dans le cadre du Schéma Directeur de la Sécurité.

La « netiquette »

Associée à une charte de l'établissement, la « netiquette » est une définition des bonnes manières et des bonnes pratiques sur l'Internet. En particulier, la « netiquette » définit des règles de bonne conduite à suivre dans le courrier électronique, le transfert de fichier, les forums de discussion, etc. La netiquette est adoptée par l'Association de Fournisseurs d'Accès à l'Internet. Elle est disponible à l'adresse : http://netiquette.afa-france.com/ .

La netiquette peut constituer une des bases de la sensibilisation des élèves à l'Internet. Des décisions de justice récentes, notamment vis à vis des courriers électroniques non sollicités, ont apporté une légitimité à ce texte de bonnes conduites.

Responsabilités et procédures d'urgence

Le Schéma Directeur de la Sécurité définit précisément les responsabilités de chacun des acteurs. Il définit en particulier la notion de Personne Juridiquement Responsable.

Responsabilité du recteur

Le recteur est chargé au niveau académique de la mise en place des solutions dans les établissements ainsi que de la sensibilisation et de la formations des usagers.

Les services du rectorat, en particulier le CTICE et son équipe, sont chargés d'organiser la formation et la sensibilisation au niveau académique. Le CTICE et son équipe peuvent conseiller les chefs d'établissement et directeurs d'école dans le choix et la mise en place de dispositifs d'aide à l'établissement.

Le chef d'établissement, point d'entrée dans l'établissement

Les modalités de mise en œuvre du dispositif de filtrage sont définies sous la direction du chef d'établissement (ou directeur d'école). Il prend la décision de retenir une solution technique adaptée à son établissement ou son école, sous les conseils des ressources académiques, et met en place un dispositif de formation/sensibilisation à destination de l'équipe pédagogique et des élèves.

Un site web est mis en place à l'adresse http://aiedu.orion.education.fr , afin de permettre à chaque chef d'établissement ou directeur d'école d'indiquer l'avancement de la mise en place du dispositif.

En cas d'incident, le chef d'établissement doit être le passage obligé entre la communauté éducative et les services académiques. Il transmet ensuite l'ensemble des informations nécessaires à la cellule académique constituée autour du CTICE et du RSSI.

Le RSSI coordinateur et correspondant académique sécurité

Il centralise les remontées d'informations, en estime la gravité, effectue une remontée au niveau nationale si besoin, grâce à la chaîne de gestion des urgences.

Cette chaîne s'organise comme suit :

1. Au sein de chaque établissement ou école, les membres de l'équipe pédagogiques informent le chef d'établissement ou le directeur d'école des incidents constatés.

2. La cellule académique constituée autour du RSSI et du CTICE est informé des incidents se produisant dans les établissements et écoles par le chef d'établissement ou le directeur d'école. Si localement l'incident n'a pu être résolu, les ressources académiques telles que les psychologues, les techniciens sécurité, conseillers juridiques des rectorats et inspections académiques pourront être sollicités. Ces structures devraient pouvoir traiter la plupart des incidents.

3. Cette cellule académique informe la cellule nationale de coordination par l'intermédiaire des dispositifs d'assistance mis à disposition (interface web et numéro de téléphone). Au besoin, le haut fonctionnaire de défense est informé par la chaîne d'alerte définie dans le schéma directeur de la sécurité. Si l'incident n'a pu être résolu au niveau académique, des ressources spécialisées, notamment dans les domaines psychologique, judiciaire et liés à la sécurité seront sollicitées.

La circulation de l'information par cette chaîne d'alerte est le moyen le plus efficace d'améliorer la liste noire nationale. En effet le site (site web de remontée d'infos sur la liste) permet d'indiquer à la cellule responsable de la gestion de la liste noire, des sites inappropriés pour l'instant non répertoriés par la liste noire. La contribution de tous les acteurs permettra d'obtenir une liste de plus en plus complète et qui remplira d'autant mieux son rôle.

Pour chaque incident constaté, le RSSI doit conserver les traces informatiques (« logs ») et mettre à jour une base de données comprenant :

- La description de l'événement
- Les circonstances de l'évènement
- Les conséquences de l'événement
- Les décisions et les mesures prises dans le cadre de cet incident

LA CELLULE NATIONALE DE COORDINATION

La cellule de coordination remplit plusieurs missions :

- Coordonner la remontée d'informations des académies vers le niveau national
- Être l'interlocuteur unique en cas de problème non résolu au niveau local ou académique
- Orienter vers une cellule d'aide psychologique les cas n'ayant pu être traités au niveau local ou académique
- Assurer la gestion de la « liste noire » nationale
- Assurer une veille technologique permanente afin d'assurer une pérennité technologique des outils utilisés

La sous cellule de gestion de la liste noire :

Cette cellule est chargée d'assurer la mise à jour et la mise à disposition de la « liste noire » nationale et d'assurer sa pérennité. Un site web, ainsi qu'une adresse de courrier électronique sont mis en place afin d'assurer la remontée de l'information.

La sous cellule d'aide psychologique :

A travers une adresse de courrier électronique et un numéro de téléphone, cette cellule peut être jointe pour traiter les cas grave nécessitant une assistance psychologique non disponible au niveau local ou académique.

Procédures à mettre en œuvre en cas d'incident : rappels et précisions

Dans la circulaire n° 2004-035 du 18-2-2004 parue au Bulletin officiel de l'Éducation nationale du 26 février 2004, le ministre indique la mise en place d'une chaîne d'information qui doit être utilisée en cas d'incidents

liés à l'usage des TIC dans le cadre pédagogique.

Cette chaîne d'information est constituée comme suit :

- au sein de chaque établissement ou école, les membres de l'équipe pédagogique informent le chef d'établissement ou le directeur d'école des incidents constatés ;

- la cellule académique constituée autour du CTICE, avec l'appui du RSSI, est informée des incidents se produisant dans les établissements et écoles par le chef d'établissement ou le directeur d'école ;

- en cas de besoin, cette cellule académique informe la cellule nationale de coordination par l'intermédiaire des dispositifs d'assistance mis à disposition (interface web et courrier électronique). Au besoin, le haut fonctionnaire de défense est informé.

Dans tous les cas, la non résolution d'un incident à un niveau doit entraîner la transmission de l'information au niveau supérieur. Toutes les informations relatives aux incidents devront être conservées (en particulier les " journaux " de connexions ou *logs*).

L'utilisation de cette chaîne d'information doit avoir lieu dans les situations suivantes :

1. découverte d'un site Internet inapproprié dans le cadre pédagogique et non bloqué par le dispositif de sélection ou de contrôle mis en œuvre par l'établissement ou l'école

Deux cas peuvent se présenter selon la solution retenue par l'établissement ou l'école :

- si cette solution est basée sur la " liste noire " nationale, ce site doit être signalé à la cellule qui gère cette liste. Pour cela il suffit de compléter le formulaire disponible à l'adresse http://bd.educnet.education.fr/cgi-bin/squidguard_modify.cgi ; un moteur d'analyse étudiera la page et décidera de son ajout ;

- si cette solution est basée sur une solution d'un éditeur, il faut alors utiliser les moyens mis à disposition par l'éditeur. Le site peut aussi être signalé à la cellule de gestion de la liste noire par le formulaire http://bd.educnet.education.fr/cgi-bin/squidguard_modify.cgi afin de l'ajouter à la " liste noire " nationale.

Dans l'attente de l'ajout à la liste noire du site signalé, il peut être possible de supprimer localement l'accès à ce site par l'intermédiaire de la solution technique mise en œuvre. Il suffit pour cela de se reporter aux fonctionnalités du produit.

Dans tous les cas, il est important de transmettre au chef d'établissement ou au directeur d'école toute demande d'ajout de sites à la " liste noire ". Le chef d'établissement pourra alors prendre la responsabilité de supprimer l'accès à un site.

2. découverte d'un site Internet approprié dans le cadre pédagogique et injustement bloqué ;

Deux cas peuvent se présenter selon la solution retenue par l'établissement ou l'école :

- si cette solution se base sur la " liste noire " nationale, ce site doit être signalé à la cellule qui gère cette liste. Pour cela il suffit de compléter le formulaire disponible à l'adresse http://bd.educnet.education.fr/cgi-bin/squidguard_modify.cgi ; un moteur d'analyse étudiera la page et décidera de son retrait ;

- si cette solution se base sur une solution d'un éditeur, il faut alors utiliser les moyens mis à disposition par l'éditeur.

Dans l'attente de la suppression du site signalé de la " liste noire ", il peut être possible de supprimer localement l'interdiction d'accès à ce site par l'intermédiaire de la solution technique mise en œuvre (ajout du site sur une " liste blanche " locale par exemple). Il suffit pour cela de se reporter aux fonctionnalités du produit.

Dans tous les cas, il est important de transmettre au chef d'établissement ou au directeur d'école toute demande de suppression de sites de la " liste noire ". Le chef d'établissement pourra alors prendre la responsabilité d'autoriser l'accès à un site.

3. consultation par un ou plusieurs élèves de sites Internet inappropriés dans le cadre pédagogique ;

Au cours d'un séquence, des élèves peuvent accéder à des sites inappropriés. Si de tels sites sont consultés, la procédure à suivre est la suivante :

- signaler, comme prévu dans le point 1. les sites inappropriés consultés ;
- avertir le chef d'établissement ou le directeur d'école de l'incident ;
- selon le degré de gravité et l'évolution de la situation, le chef d'établissement pourra prévenir la cellule académique chargée de cet aspect, pour une prise en charge par les services académiques.

4. demande de la part des médias d'explication en cas d'incident ;

Dans le cas d'une demande des médias en cas d'incident, le chef d'établissement ou le directeur d'école devra s'adresser à la cellule académique chargée de la sécurité dans le cadre de l'usage pédagogique de l'Internet.
La cellule académique devra s'appuyer sur les services de communication pour transmettre des éléments de réponses aux médias.
En cas de crise dépassant le cadre académique, la cellule nationale devra être prévenue à travers le site http://www.educnet.education.fr/aiedu/contact.html.

5. découverte d'un site Internet illégal au regard de la loi française ;

La loi oblige tout citoyen à signaler tout site Internet découvert. Si une telle découverte a lieu dans le cadre pédagogique, la procédure à suivre est la suivante :

- le site manifestement illégal doit être signalé le plus tôt possible aux autorités compétentes. Ce signalement Ce signalement peut avoir lieu en ligne à l'adresse http://www.internet-mineurs.gouv.fr rubrique " signalement " ;
- signaler, comme prévu dans le point 1. le site afin d'en limiter l'accès ;
- prévenir le chef d'établissement ou le directeur d'école de la procédure engagée ;
- le chef d'établissement et le directeur d'école prévient alors la cellule académique compétente des procédures engagées.