

Règles et principes de sécurité et d'utilisation de l'Internet (Charte Internet)
Mettre en pratique la résolution prise par le Département le 14 février 2001
Mise à jour applicable à compter du 1^{er} juillet 2012

RÈGLES ET PRINCIPES DE SÉCURITÉ ET D'UTILISATION DE L'INTERNET **(INTERNET ACCEPTABLE USE AND SAFETY POLICY - IAUSP)**

Les règles et principes – Charte Internet

Le Département de l'Éducation de la Ville de New York (dit le « **Département** ») fournit, dans le respect des lois en vigueur, l'accès à ses infrastructures Internet, à des fins éducatives et d'échanges professionnels, à ses employés, mandataires, élèves et bénévoles, lesquels sont collectivement désignés par le terme « **utilisateurs** ». Ces règles et principes de sécurité et d'utilisation de l'Internet (« **Charte Internet** » ou *policy* en anglais) s'appliquent à tout usage, du matériel électronique et de l'accès aux systèmes Internet du Département (depuis les locaux de ce dernier ou en dehors), par les utilisateurs, y compris l'échange de courriers électroniques avec un compte e-mail du Département et l'accès à l'Internet fourni par le Département.

Les « **infrastructures Internet du Département** » englobent les appareils, la connexion à l'Internet (y compris celle qui se fait sans fil), les comptes e-mail du Département, son Intranet et toute connexion à distance à ses réseaux. On considère qu'un utilisateur se sert et accède aux infrastructures Internet du Département quand il y est actif par le biais d'un appareil électronique (appartenant ou non au Département) quel que soit le lieu où il se trouve physiquement.

On entend par « **Appareils fournis par le Département** » tout appareil électronique fourni par le Département, notamment, entre autre, les ordinateurs portables ou de bureau, les unités portatives, comme les assistants électroniques de poche (PDA), les smartphones, les i-Pads, tablettes et liseuses numériques.

L'usage, par les élèves, des infrastructures Internet du Département est soumis à cette Charte, aux règlements, dispositions réglementaires et directives du Département, aux [Règles de conduite et de mesures disciplinaires standards de la Ville \(Citywide Standards of Conduct and Uniform Disciplinary Measures](#) - « **Code de discipline** ») et aux lois applicables. L'usage, par les employés, de ces infrastructures, est soumis à cette Charte, aux règlements, dispositions réglementaires, directives, politique en matière d'emploi, conventions collectives en vigueur du Département et aux lois applicables.

En utilisant les infrastructures Internet du Département, les utilisateurs acceptent de respecter cette charte et toutes les dispositions réglementaires, politiques et directives du Département qui s'appliquent. Tous les utilisateurs sont tenus de signaler, à un enseignant, responsable ou autre membre du personnel du Département compétent, tout usage abusif du réseau ou de l'Internet, ainsi que tous les échanges qui enfreindraient cette Charte.

Principes d'un usage acceptable et sans risques de l'Internet

Généralités

La fourniture de l'accès à l'Internet et des messageries électroniques par le Département est destinée à un usage éducatif, à l'enseignement, la recherche et à faciliter la communication, la collaboration et à d'autres fins propres au Département lui-même. Les utilisateurs sont soumis aux mêmes règles que celles qui s'appliquent en classe et/ou sur leur lieu de travail.

Surveillance et protection de la vie privée

Quand ils font usage des infrastructures Internet du Département, les utilisateurs n'ont pas droit à la protection de leur vie privée. Le Département surveille et enregistre ce qu'ils font en ligne, et se réserve le droit d'accéder, d'analyser, de copier, d'archiver, ou de détruire toutes communications et fichiers électroniques. Ce principe

s'applique à tout ce qui a été sauvegardé sur les appareils fournis par le Département, fichiers, emails, cookies et historiques de navigation sur Internet.

Si les circonstances l'imposent, dans le respect des lois applicables, le Département s'octroie le droit de faire connaître, aux représentants des forces de l'ordre ou à des tiers, toute trace d'activité électronique, communications incluses. Le Département offrira sa pleine coopération aux responsables publics locaux, fédéraux ou d'État, dans le cadre de toute enquête, autorisée par la loi, sur, ou liée à, des activités illégales conduites par l'intermédiaire de ses infrastructures Internet.

Usages interdits des infrastructures Internet du Département

Les utilisateurs sont astreints à respecter l'interdiction des activités énoncée dans cette Charte Internet quand ils se servent des infrastructures Internet du Département ou y accèdent.

S'ils ont un doute sur leur droit d'avoir tel ou tel comportement, sans savoir s'il est prohibé ou non, ils sont invités à contacter un enseignant, un responsable ou un autre membre compétent du personnel du Département. Le Département se réserve le droit d'agir, sur le champ, en réaction à des actes qui (1) mettent en danger la protection et/ou la sécurité du Département, des élèves, employés, établissements scolaires, du réseau ou des ressources informatiques, ou (2) alimentent ses ressources avec des éléments dont il considère que le contenu ne se justifie pas pédagogiquement ou est sans rapport avec sa collection d'outils et documents ou ses missions, ou (3) qu'il juge impropres.

Ci-dessous figure une liste, non-exhaustive, d'exemples de comportements interdits :

1. Blessier autrui, détériorer leurs biens ou ceux du Département, en :
 - a. Ayant, publiant, diffusant des propos grossiers, obscènes, vulgaires, menaçants ou agressifs par courriers électroniques, dans des documents publiés sur les pages web du Département, ou via des sites de médias sociaux professionnels ;
 - b. Accédant à, utilisant, publiant ou diffusant des données ou supports au contenu pornographique, ou obscène, plaidant la cause d'actions illégales ou dangereuses, ou prônant la violence ou la discrimination. Les utilisateurs qui accèdent par mégarde à de tels contenus sont tenus de le signaler immédiatement selon les modalités que leur établissement scolaire ou services de direction ont définies ;
 - c. Accédant à, publiant ou diffusant des documents au contenu discriminatoire, incendiaire, haineux ou constituant une forme de harcèlement, ou en tenant des propos blessants ou mensongers sur autrui ;
 - d. Envoyant, publiant ou diffusant d'une autre manière des chaînes de lettres ou en participant à la diffusion en masse de messages non désirés (spams) ;
 - e. Dégradant, d'une façon ou d'une autre, le matériel informatique, les fichiers, données ou les infrastructures Internet du Département, notamment, entre autre, en laissant se propager des virus informatiques, en détruisant des données, logiciels ou de l'équipement, en abîmant ou rendant inutilisable le matériel électronique d'autrui, ou en ayant un comportement susceptible d'entraver ou de perturber le cadre éducatif ou professionnel du Département ;
 - f. Se servant des infrastructures Internet du Département, d'une telle façon, que l'éducation, ou les missions professionnelles, de l'utilisateur ou d'autrui en sont affectées ;
 - g. Téléchargeant, publiant, copiant, ou diffusant de la musique, des photographies, des vidéos ou d'autres œuvres, violant ainsi les lois et règlements de protection des droits de reproduction applicables. Toutes musiques, photographies, et/ou vidéos doivent être téléchargées à l'usage exclusif du Département, et non à des fins privées. Si les conditions d'utilisation d'une œuvre sont précisées, son utilisateur doit s'astreindre aux impératifs indiqués. Quand les utilisateurs ont des

doutes sur leur droit à faire usage d'une œuvre, il faut qu'ils demandent l'autorisation au propriétaire des droits de reproduction ou de la marque déposée ; ou en

- h. Faisant du plagiat. Le plagiat consiste à prendre les idées ou textes des autres et à les présenter en prétendant qu'on en est l'auteur.
2. Accéder à des infrastructures Internet du Département, ou à d'autres systèmes informatiques, sans y être autorisé, ou tenter de le faire, notamment en :
 - a. Déclarant de fausses informations à des fins malveillantes, faisant du phishing (tentative frauduleuse d'extorsion de données personnelles, par voie électronique, souvent par usurpation d'identité), ou du piratage informatique ;
 - b. Cherchant consciemment à connaître les mots de passe d'autrui ;
 - c. Divulguant, à autrui, le mot de passe d'un utilisateur permettant d'accéder aux infrastructures Internet du Département. Toutefois, les élèves sont autorisés à donner, à leurs parents, leur mot de passe pour se connecter aux réseaux et sites du Département.
 - d. Modifiant le mot de passe de quelqu'un d'autre ;
 - e. Essayant de se connecter avec le compte de quelqu'un d'autre ;
 - f. Tentant d'accéder à des documents dont l'accès est bloqué ou filtré par le Département ;
 - g. Accédant aux fichiers d'un autre utilisateur sans autorisation, en les copiant ou les modifiant ;
 - h. Dissimulant ou falsifiant l'identité d'un utilisateur ;
 - i. Usurpant le mot de passe ou l'identifiant du compte d'un autre ; ou en
 - j. Ayant un usage qui risque de bloquer l'accès des autres à leur compte ou à d'autres réseaux informatiques.
 3. Se servir des infrastructures Internet du Département à des fins commerciales, notamment en :
 - a. Utilisant les infrastructures Internet du Département pour faire des profits financiers personnels ;
 - b. Ayant une activité lucrative à caractère financier ou commercial, en faisant la promotion de ses propres activités, en participant à des échanges relatifs à des affaires d'ordre commercial, financier ou professionnel sans rapport avec le Département ;
 - c. Collectant des fonds (à moins que ce soit dans le cadre d'un des cas énumérés dans la Disposition Réglementaire A-610 du Chancelier) ; ou en
 - d. Utilisant les infrastructures Internet du Département au nom d'un élu, candidat à une fonction dirigeante, de plusieurs ou d'une liste de candidats, ou d'une organisation ou d'un comité politique.
 4. Commettre des actes illégaux voire criminels.

Filtrage

Conformément à la Loi sur la protection de l'enfance contre les dangers de l'Internet (Children's Internet Protection Act - **CIPA**), le Département bloque ou filtre l'accès à Internet pour empêcher l'affichage des contenus qu'il estime impropres pour un public mineur. Ces mesures concernent la pornographie, les documents obscènes ou qui pourraient blesser les internautes qui ne sont pas encore majeurs. Le Département peut aussi bloquer ou filtrer d'autres contenus jugés inappropriés, sans valeur éducative ou sans rapport avec les missions professionnelles, ou qui menacent le réseau. Le Département est autorisé à décider, de son propre chef, de désactiver ces filtres pour certains utilisateurs qui en ont vraiment besoin pour leurs recherches, ou à d'autres fins pédagogiques ou professionnelles licites.

Les utilisateurs n'ont pas le droit de se servir d'un site web, d'une application informatique ou d'un procédé, quels qu'ils soient, pour contourner le filtrage du réseau, ou pour commettre des actes illicites de quelque sorte.

Pour vous renseigner plus avant sur la Loi CIPA, allez sur le lien indiqué ci-dessous :

<http://www.fcc.gov/guides/childrens-internet-protection-act>

Protection des données personnelles & confidentielles

La Loi sur la protection de la vie privée et le droit à l'éducation des familles (Family Educational Rights and Privacy Act - **FERPA**) interdit aux responsables scolaires du Département de transmettre, à des tiers, des données personnelles (personally identifiable information - **PII**), tirées de dossiers scolaires des enfants scolarisés dans des établissements du Département, ou de documents, sur leur famille, sans autorisation parentale préalable. Néanmoins, peuvent s'appliquer plusieurs exceptions à cette règle générale.

Tous les utilisateurs des infrastructures Internet du Département doivent respecter la Loi FERPA et la [Disposition Réglementaire A-820 du Chancelier](#) portant sur la confidentialité et la divulgation du contenu des dossiers scolaires et sur la conservation des archives. Si vous n'êtes pas certain que telle ou telle activité n'enfreint ni la Loi FERPA ni la Disposition Réglementaire A-820 du Chancelier, veuillez contacter le Directeur général de la protection des données (Chief Information Security Officer) du Département.

La teneur des échanges, en interne, entre les services administratifs et un des avocats du Département peut aussi être confidentielle. Par conséquent, les utilisateurs ne sont pas censés faire suivre ou diffuser de telles informations sans vérifier, au préalable, que c'est possible, avec l'avocat en question. C'est aux utilisateurs de s'assurer que les emails, dont le message ou les pièces jointes contiennent des informations confidentielles, sont bien envoyés aux destinataires voulus.

Protection des élèves contre les dangers de l'Internet

1. Devoirs du Département :

- a. Le Département instruira les élèves sur le comportement, à avoir, en ligne, en expliquant notamment comment communiquer avec d'autres internautes sur les sites des réseaux sociaux et dans les salles de chat (espaces en ligne de conversations en direct), ou reconnaître et réagir contre le cyber-harcèlement.
- b. Le Département s'efforcera de garantir la protection et la sécurité des mineurs, utilisateurs de courrier électronique, des salles de chat, et d'autres formes d'échanges électroniques directs.
- c. Si les circonstances s'y prêtent, le Département donnera aux élèves, à leurs parents et au personnel, des directives et instructions pour que les élèves restent hors de danger quand ils se servent d'Internet.

2. Usage des infrastructures Internet du Département par les élèves

- a. Les élèves ne doivent pas révéler de données personnelles, sur eux-mêmes ou quelqu'un d'autre, sur les sites des réseaux sociaux, dans les salles de chat, par email, via d'autres modes de communication électroniques directs, ni sur aucun forum de la Toile. Il leur est, par exemple, défendu de donner l'adresse de leur domicile, leur numéro de téléphone fixe ou portable. Ils ne doivent pas mettre en ligne de photographies où ils figurent, ni aucune image d'autrui.

- b. Il est fortement déconseillé aux élèves de rencontrer, pour la première fois en personne, quiconque, s'ils ne connaissent cet individu que par Internet.
 - c. Les élèves doivent immédiatement dévoiler, à leur enseignant ou à un autre membre du personnel scolaire, tout message reçu ou autre agissement déplacé voire qui les met mal à l'aise.
 - d. Il est vivement demandé aux élèves de ne pas autoriser la sauvegarde de leurs mots de passe sur les ordinateurs du Département.
3. Usage des infrastructures Internet du Département, y compris des médias sociaux, par les enseignants, lors d'activités en classe
- a. Les enseignants sont fortement invités à éduquer les élèves sur le comportement, à avoir, en ligne, pour éviter de se mettre en danger, en leur expliquant notamment comment communiquer avec d'autres internautes sur les sites des réseaux sociaux et dans les salles de chat, en les sensibilisant au cyber-harcèlement et en leur montrant comment y réagir. Ils doivent se référer au [Department's Citizenship in the Digital Age guide \(guide du Département sur la citoyenneté à l'ère numérique\)](#), et aux autres ressources éducatives gratuites sur la sécurité sur Internet disponibles sur la Toile.
 - b. Médias sociaux
 - On entend par « **médias sociaux** » : tout espace de publication ou présence en ligne qui permet de communiquer de manière interactive, y compris, entre autre, les réseaux sociaux, blogs, sites web, forum en ligne et wikis (partage de connaissances en ligne). Parmi eux, on peut citer par exemple Facebook, Twitter, YouTube, Google+ et Flickr mais il y en a d'autres.
 - Pour améliorer l'éducation et l'acquisition des connaissances et savoir-faire des élèves, les établissements scolaires utilisent diverses technologies de communication interactive en ligne sur la Toile. Les sites des médias sociaux doivent n'être utilisés qu'à des fins éducatives et en rapport avec l'activité scolaire, avec les cours, les travaux et exercices à faire, et pour faciliter la communication entre élèves et enseignants.
 - Le Département limite l'accès individuel à ces sites de son personnel et des services administratifs de ses établissements scolaires. Pour faire un usage collectif d'un site de média social au sein du Département ou parmi les responsables administratifs des établissements scolaires du même Département, il faut impérativement avoir l'autorisation des parents d'élèves.
 - Dès lors que les activités scolaires sur Internet impliquent l'utilisation de médias sociaux, les enseignants doivent se référer aux [Social Media Guidelines \(Directives relatives aux médias sociaux\)](#) du Département, intégrées à cette Charte.
4. Parents d'élève(s) :
- a. Alors que la plupart du temps, les élèves seront encadrés quand ils se serviront des infrastructures Internet du Département à l'intérieur des établissements scolaires, le Département n'a pas les moyens physiques de surveiller ce qu'ils font sur l'Internet, ni de leur faire respecter le vaste ensemble de valeurs censé guider les relations sociales qu'ils ont sur la Toile. C'est aux parents que revient, en premier lieu, la tâche de transmettre leurs propres valeurs familiales à leurs enfants, de leur parler des contenus qu'ils jugent convenables et de ceux qu'ils conseillent d'éviter quand ils vont en ligne par le biais des infrastructures Internet du Département.

b. Les parents ont l'entière responsabilité de contrôler la façon dont leur(s) enfant(s) dispose(nt) d'Internet quand il(s) y accède(nt) via les réseaux et plateformes du Département, depuis leur domicile ou ailleurs en dehors d'un établissement scolaire. Le Département a le choix d'employer, ou non, un système de filtre quand il fournit l'accès à ses infrastructures Internet, depuis un domicile privé. On conseille aux parents de se renseigner auprès des établissements scolaires ou du Département.

Violation de cette Charte Internet

Le Département, notamment les services administratifs centraux et les établissements scolaires, se réserve le droit d'interdire, à tout moment, l'accès à ses infrastructures Internet - y compris à sa messagerie électronique - à tout utilisateur quel qu'il soit.

Si un élève enfreint cette Charte, on prendra les mesures disciplinaires qui s'imposent conformément au Code de discipline et aux dispositions réglementaires du Chancelier applicables. Si un élève n'est plus autorisé à accéder aux infrastructures Internet du Département, il n'a pas à être pénalisé dans la poursuite de sa scolarité. De plus, le Département fera en sorte qu'il ait toujours une véritable possibilité de participer aux cours et autres activités éducatives.

Les employés qui enfreignent cette Charte Internet feront l'objet des sanctions qui s'imposent.

Tous les utilisateurs doivent immédiatement dévoiler, à leur enseignant, leur supérieur hiérarchique, au chef de l'établissement scolaire, ou à un autre directeur, toute information reçue qui leur paraît déplacée, voire les met mal à l'aise.

Clause de limitation de responsabilité

Le Département ne donne aucune garantie sur la qualité des services fournis et n'est pas responsable en cas de réclamations, pertes, dommages, coûts, ou autres obligations, consécutifs à l'usage du réseau ou des comptes électroniques. Tous surcoûts accumulés suite à l'usage du réseau informatique du Département par un utilisateur sont à la charge de ce dernier. Le Département se dégage aussi de toute responsabilité quant à l'exactitude et à la qualité des données obtenues par l'utilisateur lors de son accès aux infrastructures Internet dudit Département. Toute déclaration, consultable sur le réseau informatique ou sur l'Internet, est considérée comme le point de vue de son auteur, et ne peut être attribuée au Département, à ses annexes ou ses employés.

Copies de cette Charte Internet et questions

Le Département se réserve le droit d'amender et/ou de réviser cette Charte à tout moment si le besoin s'en fait sentir. Il est possible de se procurer ce texte en le demandant ou de le consulter sur le site web du Département à <http://schools.nyc.gov/Offices/EnterpriseOperations/DIIT/WebServices/iaup/default.htm#preamble>.

Les questions relatives au présent ensemble de règles sont à adresser à :

NYC Department of Education
Office of Communications & Media Relations
52 Chambers Street, Room 314
New York, NY 10007
Téléphone : 212-374-5141
Fax : 212-374-5584