



MINISTÈRE  
DE L'ÉDUCATION NATIONALE,  
DE L'ENSEIGNEMENT SUPÉRIEUR  
ET DE LA RECHERCHE



# CHARTRE D'UTILISATION DU SYSTEME D'INFORMATION DE L'ACADEMIE DE LILLE

Document approuvé en Comité Technique Académique le 23/06/2014

Rectorat de l'Académie de Lille

Cité académique Guy Debeyre

20, rue Saint-Jacques - BP709 - 59033 Lille Cedex

Tél : 03.20.15.60.00

Fax : 03.20.15.65.90

<http://www.ac-lille.fr>

## Table des matières

<b>1. CONTEXTE.....</b>	<b>3</b>
<b>2. OBJET.....</b>	<b>3</b>
<b>3. DÉFINITIONS.....</b>	<b>3</b>
<b>4. CHAMP D'APPLICATION.....</b>	<b>3</b>
<b>5. ENGAGEMENTS DE L'INSTITUTION.....</b>	<b>4</b>
<b>6. ENGAGEMENTS DE L'UTILISATEUR.....</b>	<b>4</b>
<b>7. CONDITIONS D'UTILISATION DU SYSTÈME D'INFORMATION.....</b>	<b>4</b>
<b>7.1. Professionnelle / privée.....</b>	<b>4</b>
<b>7.2. Continuité de service : gestion des absences et des départs.....</b>	<b>4</b>
<b>7.3. Assistance et maintenance.....</b>	<b>5</b>
<b>7.4. Ressources non institutionnelles.....</b>	<b>5</b>
<b>8. DISPOSITIONS GÉNÉRALES.....</b>	<b>5</b>
<b>8.1. Moyens d'authentification.....</b>	<b>6</b>
<b>8.2. Devoirs de signalement et d'information.....</b>	<b>6</b>
<b>8.3. Sauvegarde.....</b>	<b>7</b>
<b>8.4. Journalisation et suivi.....</b>	<b>7</b>
<b>8.5. Confidentialité.....</b>	<b>7</b>
8.5.1. Administrateur informatique.....	7
8.5.2. Visibilité des flux de communication.....	7
<b>9. DISPOSITIONS SPÉCIFIQUES.....</b>	<b>8</b>
<b>9.1. Messagerie électronique.....</b>	<b>8</b>
9.1.1. Adresses électroniques.....	8
9.1.2. Messages électroniques.....	8
<b>9.2. Internet.....</b>	<b>9</b>
9.2.1. Publications sur les sites internet et intranet.....	9
9.2.2. Sécurité.....	9
9.2.3. Visibilité et communication.....	9
<b>9.3. Ressource collaborative.....</b>	<b>9</b>
<b>10. RESPECT DE LA PROPRIÉTÉ INTELLECTUELLE.....</b>	<b>9</b>
<b>11. RESPECT DE LA LOI INFORMATIQUE ET LIBERTÉS.....</b>	<b>10</b>
<b>12. LIMITATIONS DES USAGES.....</b>	<b>10</b>
<b>13. ENTRÉE EN VIGUEUR DE LA CHARTE.....</b>	<b>10</b>

## 1 CONTEXTE

---

Les informations que nous manipulons tous les jours sont des denrées précieuses et convoitées. Elles sont devenues indispensables à la réalisation de notre mission de service public. De nombreuses composantes pédagogiques, organisationnelles et techniques gravitent et évoluent autour de ces informations. Afin de veiller au bon fonctionnement de cet ensemble, il convient d'en définir un cadre commun d'utilisation.

L'académie est responsable des données qui lui sont confiées, c'est donc à chacun de nous d'en assurer leur protection.

## 2 OBJET

---

Le bon fonctionnement du système d'information implique le respect des règles visant à assurer la sécurité, la performance des traitements, la préservation des données et le respect des dispositions légales et réglementaires qui s'imposent.

La présente charte a pour objet de définir les règles, les prérogatives, les engagements et les responsabilités pour tout ce qui concerne le système d'information de l'Académie de Lille.

Elle a aussi pour vocation de sensibiliser les utilisateurs aux exigences de sécurité et d'attirer leur attention sur certains comportements pouvant porter atteinte à l'intérêt collectif du service public d'éducation.

## 3 DÉFINITIONS

---

Dans la présente charte, les termes suivants ont le sens qui leur est donné ci-dessous.

- **Institution** : tout service académique (rectorat, direction des services départementaux, ...) et tout établissement du premier et du second degrés ;
- **Ressource** : élément informationnel<sup>1</sup> ou matériel ;
- **Système d'information** : ensemble des ressources permettant de collecter, regrouper, classifier, stocker, traiter et diffuser de l'information quel que soit le support (numérique, papier, ...) ;
- **Utilisateur** : personne physique ayant accès au système d'information.
- **Ressource non institutionnelle**<sup>2</sup> : ressource mise à disposition des utilisateurs par des tiers.

## 4 CHAMP D'APPLICATION

---

La présente charte s'applique à l'institution ainsi qu'à l'ensemble des utilisateurs de son système d'information.

Dans le contexte de cette charte, les rôles suivants ont l'attribution qui leur est donnée ci-dessous.

**Institution** : Académie de Lille.

**Utilisateur** :

- Agent titulaire ou non titulaire concourant à l'exécution des missions de service public.
- Prestataire<sup>3</sup> ayant contracté avec le Ministère de l'Éducation nationale ou avec une collectivité territoriale ayant compétence partagée avec l'État en matière d'éducation.

La charte peut être complétée par des conditions d'utilisation et des guides : ceux-ci définissent les règles spécifiques et pratiques d'usage et ne peuvent pas contrevenir aux principes définis dans cette charte. Ils correspondent à un ou plusieurs thèmes techniques (usage de la messagerie, usage du poste de travail, guide du filtrage internet, ...) et ils

---

<sup>1</sup> Pour exemple, une ressource informationnelle peut être un fichier informatique, un document rédigé, ...

<sup>2</sup> Les ressources matérielles personnelles ou les services en ligne proposés par des tiers font parties des ressources non institutionnelles.

<sup>3</sup> Le contrat avec le prestataire devra prévoir expressément l'obligation de respect de la charte.

peuvent être déclinés par unité fonctionnelle. Les guides ou les conditions d'utilisation seront élaborés en concertation avec la Direction des Systèmes d'Information et le Responsable Sécurité des Systèmes d'Informations<sup>4</sup>.

## **5 ENGAGEMENTS DE L'INSTITUTION**

---

L'institution s'engage à assurer la sécurité du système d'information et la protection des utilisateurs.

L'institution facilite l'accès des utilisateurs aux ressources du système d'information.

L'institution est tenue de respecter la vie privée de chacun.

## **6 ENGAGEMENTS DE L'UTILISATEUR**

---

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des ressources auxquelles il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie<sup>5</sup>.

En tout état de cause, l'utilisateur est soumis au respect de la législation en vigueur et des obligations résultant de son statut ou de son contrat.

## **7 CONDITIONS D'UTILISATION DU SYSTEME D'INFORMATION**

---

### **7.1 Professionnelle / privée**

Les systèmes d'information mis à la disposition de l'utilisateur sont prioritairement à usage professionnel.

L'utilisation à des fins privées doit être non lucrative et raisonnable, tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service. En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard du coût global d'exploitation.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées<sup>6</sup> par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet.

Dans le cadre d'une utilisation privée d'une ressource non institutionnelle, celle-ci doit répondre aux exigences de sécurité du système d'information.

### **7.2 Continuité de service : gestion des absences et des départs**

Pour assurer la continuité de service, l'utilisateur doit informer sa hiérarchie des modalités permettant l'accès aux systèmes d'information dont il dispose.

Lors de son départ définitif du service ou de l'établissement, il appartient à l'utilisateur de veiller à laisser les ressources utilisées dans un état impersonnel et de détruire ses données à caractère privé. La responsabilité de l'institution ne pourra être engagée quant à la conservation et la confidentialité de ces données.

Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'institution. Toutes les ressources mises à disposition de l'utilisateur telle que l'adresse de messagerie ne seront plus fonctionnelles ou accessibles par l'utilisateur à l'échéance du délai défini dans ces mesures de conservation.

---

<sup>4</sup> RSSI : Personne chargée de veiller et garantir la sécurité du système d'information de l'institution.

<sup>5</sup> Tel qu'il résulte des droits et obligations des fonctionnaires (Loi n°83-634 du 13 juillet 1983).

<sup>6</sup> Une dénomination "Personnel & Privé" ne pourra pas porter à équivoque.

### 7.3 Assistance et maintenance

En cas de question relative au fonctionnement du système d'information, l'utilisateur consultera la documentation mise à sa disposition. En cas de problème relatif au fonctionnement du système d'information ou de demande spécifique, l'utilisateur se rapprochera de son service d'assistance technique.

Pour effectuer la maintenance corrective, évolutive ou à des fins de restauration, dans la mesure du possible, l'institution se réserve la possibilité de réaliser des interventions sur les ressources mises à la disposition de l'utilisateur.

### 7.4 Ressources non institutionnelles

La mise en œuvre ou l'utilisation d'une ressource non institutionnelle au sein du système d'information est définie ci-dessous dans le cadre d'une utilisation professionnelle. Bien que non recommandée, cette ressource peut être un complément ou faire partie intégrante du système d'information. De ce fait, son utilisation (et son accès) au sein du système d'information est tolérée lorsqu'elle :

- respecte la législation en vigueur ;
- est conforme avec les exigences de sécurité du système d'information ;
- correspond à un besoin de nécessité de service ou de mission de service public de l'utilisateur ;
- est adéquate, pertinente et non excessive au regard des finalités pour lesquelles elle est utilisée ;
- est interopérable fonctionnellement et techniquement avec le système d'information.

Lorsque la ressource non institutionnelle respecte ces conditions et lorsque son utilisation s'inscrit en dehors d'un cadre pédagogique, l'utilisateur ou le responsable en charge de la mise en place d'une ressource non institutionnelle veillera au préalable de son utilisation à :

- s'assurer auprès de l'institution qu'il n'existe pas d'équivalent institutionnel pouvant répondre à ses besoins ;
- informer la direction des systèmes d'information sur l'utilisation, le changement ou l'abandon d'une ressource non institutionnelle.

En dehors du cadre pédagogique, l'utilisation d'une ressource non institutionnelle peut être refusée par le responsable hiérarchique.

L'institution ne peut garantir la prise en charge de l'assistance pour les ressources non institutionnelles. La maintenance de ressources non institutionnelles personnelles ne peut être imputée à l'institution. De ce fait, elle ne pourra être tenue pour responsable des dysfonctionnements d'interopérabilité fonctionnelle et technique avec le système d'information.

## 8 DISPOSITIONS GÉNÉRALES

---

L'institution met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs. Elle met en place des dispositifs permettant la formation et la sensibilisation des utilisateurs au système d'information.

Toute ressource qui comporte un risque de sécurité, qui limite ou qui bloque le bon fonctionnement du système d'information pourra être isolée, voire supprimée. Dans la mesure du possible, l'utilisateur en sera informé au préalable.

Afin d'assurer la sécurité et le bon fonctionnement du système d'information, l'utilisateur prendra les précautions suivantes :

- ne pas relier, créer, installer, copier, télécharger ou utiliser sur le système d'information des ressources autres que celles mises à disposition par l'institution ;
- ne pas modifier, réinitialiser ou supprimer les ressources permettant l'accès ou l'utilisation du système d'information de l'institution sans être expressément habilité ;

- se conformer aux dispositifs mis en place par l'institution pour lutter contre les menaces et les attaques sur le système d'information ;
- veiller à limiter la diffusion ou la publication d'une ressource au strict nécessaire ;
- vérifier lors de la fin d'usage d'une ressource si elle doit être détruite ou conservée. Si la ressource doit être conservée, il est possible que cette opération soit déjà prise en charge par l'institution (académie, établissement scolaire, ...). Dans tous les cas, prendre les dispositions en conséquence ;
- s'assurer lors de la destruction d'une ressource qu'elle ne soit plus exploitable (en particulier pour les ressources sensibles).

D'une manière générale, une autorisation exceptionnelle, accordée à un utilisateur et sortant du cadre de sa mission habituelle, n'est opposable que si elle est formelle et consignée.

## **8.1 Moyens d'authentification**

L'utilisateur est informé que les moyens d'authentification permettant l'accès au système d'information constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux ressources protégées un caractère privé.

Les droits d'accès et les habilitations accordés à l'utilisateur sont définis en fonction de sa mission et de son niveau d'exercice.

La sécurité des systèmes d'information mis à la disposition de l'utilisateur lui impose de respecter les consignes et les règles de sécurité relatives à la gestion de l'authentification et à la gestion des accès. Il doit notamment :

- garder strictement confidentiel(s) son (ou ses) moyen(s) d'authentification et ne pas le(s) dévoiler à un tiers ;
- ne pas utiliser les noms et moyens d'authentification d'un autre utilisateur, ni chercher à les connaître ;
- veiller à ne pas garder un accès ouvert à une ressource sans surveillance.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son ou ses moyens d'authentification, il devra procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur. Le bénéficiaire de la communication du moyen d'authentification veillera à s'assurer de garder une trace de cette communication. Il ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle à l'origine de la communication.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions de la part de l'institution :

- veiller techniquement à ce que les ressources ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité de service mises en place par la hiérarchie (cf. section 7.2) ;
  - limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- et de la part de l'utilisateur :
- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite.

## **8.2 Devoirs de signalement et d'information**

L'institution doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

L'utilisateur doit signaler dans les meilleurs délais tout dysfonctionnement constaté ou toute anomalie découverte lié au système d'information. Cette information doit être portée à la connaissance de sa hiérarchie ou du responsable de la ressource concernée.

Il signale également toute possibilité d'accès à une ressource du système d'information qui ne correspond pas à son habilitation. Cette information est portée à la connaissance de la personne responsable de la ressource concernée ou le cas échéant au RSSI de l'institution.

### **8.3 Sauvegarde**

La sauvegarde des données à caractère professionnel par l'institution ne sera réalisée qu'à la demande explicite de l'utilisateur. La sauvegarde des données à caractère privé incombera à l'utilisateur.

### **8.4 Journalisation et suivi**

On entend par journalisation la conservation des événements liés à un utilisateur ou à une ressource.

L'institution est dans l'obligation légale de journaliser la création de contenus des services dont elle est prestataire<sup>7</sup> (hébergement, messagerie, ...). En complément, l'institution se réserve le droit d'élargir le dispositif de journalisation à l'ensemble du système d'information.

Une exploitation de la journalisation du système d'information peut être réalisée uniquement à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, techniques, de sécurité ou de détection des abus, dans le respect de la législation applicable. Préalablement à cette mise en place, l'institution procédera, auprès de la Commission Nationale de l'Informatique et des Libertés, à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

L'institution assurera l'intégrité de l'horodatage des événements journalisés.

### **8.5 Confidentialité**

L'utilisateur a une obligation générale et permanente de confidentialité et de discrétion attachée à l'utilisation des informations disponibles sur le système d'information.

#### **8.5.1 Administrateur informatique**

Les administrateurs du système d'information, utilisateurs chargés de la conception puis de la conduite opérationnelle des systèmes d'information, ne peuvent en aucun cas divulguer les informations couvertes par le secret des correspondances ou identifiées comme relevant de la vie privée de l'utilisateur.

Cependant, ils doivent informer les personnes compétentes et prendre les mesures adaptées et définies dans le cadre de leurs fonctions, lorsque ces informations :

- peuvent mettre en cause le bon fonctionnement technique du système d'information et sa sécurité ;
- tombent dans le champ de l'article<sup>8</sup> 40 alinéa 2 du code de procédure pénale.

#### **8.5.2 Visibilité des flux de communication**

Afin de veiller à la confidentialité des données, l'institution doit contrôler la légitimité de la nature des flux de communication entrant et sortant de son système d'information.

Uniquement à des fins de protection du système d'information et dans le plus strict respect de la vie privée des utilisateurs, elle peut notamment être amenée à bloquer, interdire ou déchiffrer des flux de communication chiffrés.

---

<sup>7</sup> Art.6-II de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

<sup>8</sup> « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »

## 9 DISPOSITIONS SPÉCIFIQUES

---

En complément des dispositions légales en vigueur<sup>9</sup> et au regard de la mission éducative de l'institution, l'accès, le téléchargement, la production et la consultation volontaire de contenus à caractère pornographique, raciste et pédopornographique depuis les locaux ou avec les ressources mises à la disposition par l'institution, est interdite.

### 9.1 Messagerie électronique

L'utilisation de la messagerie électronique constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'institution.

Les communications professionnelles par message électronique se feront uniquement via les messageries et les adresses électroniques professionnelles nominatives, fonctionnelles ou organisationnelles mises à disposition par l'institution.

Pour préserver la sécurité et le bon fonctionnement du système d'information, des filtres et des limitations techniques sur l'utilisation de la messagerie peuvent être mises en place.

#### 9.1.1 Adresses électroniques

L'institution s'engage à mettre à la disposition de l'utilisateur une adresse de messagerie électronique professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

L'aspect nominatif de cette adresse électronique ne retire en rien le caractère professionnel de celle-ci. Elle peut cependant constituer le support d'une communication privée telle que définie en section 7.1 dans le respect de la législation en vigueur. L'adresse électronique<sup>10</sup> nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'institution. La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'«utilisateurs», relève de la responsabilité exclusive de l'institution : ces adresses ne peuvent être utilisées sans autorisation explicite.

#### 9.1.2 Messages électroniques

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages. Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie électronique ainsi qu'une dégradation du service.

L'utilisateur doit être vigilant sur la nature des messages qu'il échange au même titre que pour les courriers traditionnels. Les messages échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles<sup>11</sup> 1369-1 à 1369-11 du code civil.

L'utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques.

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

---

<sup>9</sup> On retrouve entre autre la législation liée aux contenus pédopornographiques, racistes, d'incitation à la haine raciale, aux messages à caractère violent susceptibles d'être vus ou perçus par un mineur.

<sup>10</sup> L'adresse est de la forme prenom.nom@ac-lille.fr

<sup>11</sup> Issus de l'ordonnance n°2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique.



## 9.2 Internet

Il est rappelé qu'internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques). Il peut constituer le support d'une communication privée telle que définie en section 7.1 dans le respect de la législation en vigueur.

### 9.2.1 Publications sur les sites internet et intranet

Toute publication sur les sites internet ou intranet de l'institution doit se conformer au respect de la charte sur l'hébergement.

### 9.2.2 Sécurité

L'accès à internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution. En complément des dispositions légales en vigueur, l'institution se réserve le droit de limiter, sélectionner ou restreindre l'accès à certains contenus ou services internet.

### 9.2.3 Visibilité et communication

L'utilisateur signale, dans les meilleurs délais, les éventuels abus perpétrés à l'encontre de l'institution et des personnels sur internet. Cette information doit être portée à la connaissance du RSSI.

Seules les personnes habilitées peuvent communiquer au sujet et au nom de l'institution.

## 9.3 Ressource collaborative

Les ressources collaboratives<sup>12</sup> sont des outils de travail. Elles doivent être utilisées dans un souci de partage de l'information et afin de faciliter les échanges dans le cadre de la vie professionnelle, culturelle et associative.

Une ressource collaborative est sous la responsabilité d'au moins un utilisateur. Il est l'interlocuteur privilégié des autres utilisateurs pour tous les problèmes de gestion et d'utilisation. Il appartient à l'utilisateur responsable d'une ressource collaborative de s'assurer :

- de la transmission de sa responsabilité en cas de départ ou d'arrêt de participation à la ressource collaborative ;
- que les accès à la ressource collaborative soient strictement réservés aux utilisateurs habilités ;
- que chaque utilisateur accédant à la ressource collaborative ait un rôle défini ;
- de veiller à la bonne tenue et organisation de la ressource collaborative ;
- de s'assurer de la sauvegarde et de la fin d'usage de la ressource collaborative.

## 10 RESPECT DE LA PROPRIÉTÉ INTELLECTUELLE

---

L'institution rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- veiller à respecter les conditions des licences souscrites ou s'assurer de respecter les dispositions légales liées à l'exception pédagogique ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

---

<sup>12</sup> Pour exemple, une ressource collaborative peut être un espace de stockage commun, un carnet d'adresses partagé, une liste de diffusion, un forum, ...

## **11 RESPECT DE LA LOI INFORMATIQUE ET LIBERTÉS**

---

Conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'Information.

Ce droit s'exerce auprès du responsable hiérarchique du service ou de l'établissement dont il dépend.

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à cette loi.

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés ».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement les services compétents qui prendront les mesures nécessaires au respect des dispositions légales.

## **12 LIMITATIONS DES USAGES**

---

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les différents guides d'utilisation, la « personne juridiquement responsable » pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Par « personne juridiquement responsable », on entend : toute personne ayant la capacité de représenter l'institution (recteur, directeur académique des services de l'éducation nationale) ou un établissement d'enseignement scolaire, supérieur et de recherche (président d'université, chef d'établissement, directeur d'établissement, ...).

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est passible de sanctions.

## **13 ENTRÉE EN VIGUEUR DE LA CHARTE**

---

La présente charte entre en vigueur dès son approbation en Comité Technique Académique.

Toutes les règles relatives à l'utilisation des systèmes d'information entrant en conflit avec les présentes règles sont annulées et remplacées par celles-ci.