Charte régissant l’usage du système d’information de l’académie de Toulouse par ses utilisateurs

Rectorat de l'académie de Toulouse
CS 87703
31 077 Toulouse cedex 4

Table des matières

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 suppose le respect des dispositions législatives et règlementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte a pour objet de préciser la responsabilité de l'institution et des utilisateurs, en accord avec la législation, afin d'instaurer un usage correct des ressources informatiques du rectorat de l'académie de Toulouse. Elle précise les droits et devoirs de chacun.

Les manquements aux dispositions énoncées dans la présente charte peuvent engager la responsabilité de l'agent, au plan disciplinaire et/ou au plan pénal.

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.

La charte est accompagnée d'un guide des bonnes pratiques des outils numériques.

3. Définitions

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

Système d'information : ensemble des ressources matérielles et logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'institution et ce quel que soit le support (numérique, papier,…).

L'informatique nomade : on entend les assistants personnels, les ordinateurs portables, les téléphones portables,… C'est également un des éléments constitutifs du système d'information.

Institution : tout service de l'académie de Toulouse (rectorat, ensemble des services déconcentrés, …) et tout établissement du premier et du second degrés.

Utilisateur : tout personnel ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut. Il s'agit notamment de :

- tout agent titulaire, non titulaire ou bénéficiant d'une convention de stage

- tout prestataire ayant contracté avec l'institution ou avec une collectivité territoriale ayant compétence partagée avec l'Etat en matière d'éducation. Le contrat devra prévoir expressément l'obligation de respect de cette charte.

4. Champ d'application

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

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 contenus dans cette charte. Ils correspondent à un ou plusieurs thèmes techniques (usage de la messagerie, usage du poste de travail, conditions d'utilisation du réseau wifi,…) et ils peuvent être déclinés par unité fonctionnelle. Les guides ou les conditions d'utilisation seront élaborés en concertation avec la Direction des Systèmes d'Information (DSI) et le Responsable de la Sécurité des Systèmes d'Information (RSSI)[1].

5. Engagements de l'institution

L'institution porte à la connaissance de l'utilisateur la présente charte, après consultation des CTS.

Elle met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

Elle facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à disposition sont à usage professionnel mais l'institution est tenue de respecter la vie privée de chacun.

6. Engagements de l'utilisateur

L'utilisateur est comptable en toutes circonstances, 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 informations et des documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie[2].

Dans le cas contraire, la responsabilité de l'utilisateur pourra être engagée. Tout abus de l'utilisation des ressources mises à disposition à des fins extra-professionnelles est passible de sanctions. Par ailleurs, le chef de service, pourra, sans préjuger des poursuites ou procédures pouvant être engagées à l'encontre des personnels, limiter les usages par toute mesure conservatoire ou définitive.

Dans tous les cas, l'utilisateur reste soumis au respect de la législation en vigueur et des obligations résultant de son statut ou de son contrat.

7. Conditions d'utilisation du système d'information

7.1 Utilisation professionnelle / privée

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

[1] RSSI : personne chargée de veiller et garantir la sécurité des systèmes d'information de l'institution.
[2] Telles qu'elles résultent des droits et obligations des fonctionnaires (Loi n° 83-634 du 13 juillet 1983).

L'utilisation à des fins privées doit être résiduelle, 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.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées[3] par l'utilisateur comme relevant de sa vie privée. La mention « personnel et confidentiel » ou « personnel et privé » sera portée sur les données relevant de la vie privée. Ainsi appartient-il à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet. En l'absence de désignation explicite du caractère privé, les données sont présumées avoir un caractère professionnel et le recteur pourra y avoir accès, sous réserve du respect des secrets professionnels particuliers auxquels sont soumis certains de ses personnels.

L'utilisateur est responsable de son espace de données à caractère privé. Notamment, la sauvegarde des données à caractère privé incombera à l'utilisateur. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné, au sein de l'institution.

Dans le cadre d'une utilisation privée d'une ressource non institutionnelle, celle-ci doit répondre aux exigences de sécurité du système d'information et respecter la législation et la réglementation en vigueur.

7.2 Continuité de service : gestion des absences et des départs

Le responsable de service, en lien avec l'utilisateur, mettra en place des modalités permettant l'accès éventuel aux ressources mises spécifiquement à la disposition de l'utilisateur et ceci aux seules fins d'assurer la continuité de service.

Aussi les personnels devront, en cas d'impossibilité prolongée d'accès à leur boîte de messagerie, faire en sorte qu'en collaboration avec leur responsable hiérarchique les messages nécessaires au bon fonctionnement du service qui leur parviendraient dans leur boîte nominative, ne soient pas perdus. Ils pourront notamment utiliser la fonction de notification d'absence de la messagerie pour indiquer à leurs interlocuteurs la durée prévisible de leur absence et la boîte vers laquelle leurs messages doivent être, si besoin, émis à nouveau.

Le recteur peut imposer la mise en place de ce message d'absence, dans l'intérêt du service, et notamment pour assurer sa continuité.

Lors du 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 complet et de détruire ses seules 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 supérieur hiérarchique 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.

[3] Une dénomination « personnel et 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 (le cas échéant à distance) sur les ressources mises à disposition de l'utilisateur.

Une maintenance à distance est précédée d'une information 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 aux exigences de sécurité du système d'information ;
- 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, en conformité avec la Politique des Systèmes d'Information de l'Etat (PSSIE), la loi n°78-17 (Informatique et Libertés), et le Référentiel Général de Sécurité (RGS) en vigueur.

L'institution met en place des dispositifs permettant la formation et la sensibilisation des utilisateurs du système d'information. L'académie de Toulouse a notamment mis en place un portail de la sécurité des systèmes d'information (https://ssi.ac-toulouse.fr).

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).

Par autorisation écrite exceptionnelle, l'administration pourra accorder à un utilisateur la possibilité de déroger à ses règles de prudence, pour une mission particulière, dans l'intérêt du service.

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 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. A titre d'exemple, l'utilisateur doit penser à verrouiller son poste de travail ou son téléphone mobile professionnel.

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(s) derniers(s) 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 à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- porter à la connaissance de l'utilisateur les éléments susceptibles de lui permettre de sécuriser[4] son utilisation du système d'information ;

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 Devoir de signalement et d'information

L'utilisateur doit signaler dans les meilleurs délais tout dysfonctionnement constaté ou toute anomalie découverte lié au système d'information.

Il signale également toute possibilité d'accès à une ressource du système d'information qui ne correspond pas à son niveau d'habilitation.

Ces informations doivent être portées à la connaissance de sa hiérarchie ou du responsable de la ressource concernée ou le cas échéant au responsable de la sécurité du système d'information (RSSI) de l'institution.

8.3 Sauvegarde

La sauvegarde des données à caractère professionnel est réalisée par l'institution de façon régulière et automatique pour les fichiers des partages réseaux. La sauvegarde de données à caractère professionnel sur d'autres types de supports ne sera étudiée qu'à la demande explicite de l'utilisateur sous couvert de sa hiérarchie.

La sauvegarde des données à caractère privé incombera à l'utilisateur.

8.4 Journalisation et suivi

On entend par journalisation la conservation des événements[5] liés à un utilisateur ou à une ressource.

L'institution est dans l'obligation légale de journaliser la création des contenus des services dont elle est prestataire[6] (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 règlementaire 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 procèdera, auprès de la commission Nationale de l'Informatique et des Libertés, à une déclaration, qui mentionnera notamment la durée de mois

[4] Niveaux de risques encourus : sensibilité de l'application, des données, responsabilité particulière.
[5] Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur, …
[6] Art.6-II de la loi n° 2014-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

conservation des traces et durées de connexion, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 (Informatique et 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[7] 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.

9. Dispositions spécifiques

En complément des dispositions légales en vigueur[8] 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 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 d'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 mise à disposition par l'institution.

[7] « 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. »

[8] 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.

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 mis 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'accès à la messagerie nominative professionnelle peut s'effectuer de tout poste informatique disposant d'un accès à internet, y compris du domicile. Quel que soit le lieu et le mode d'accès à la messagerie nominative professionnelle, les règles prévues par la présente charte s'appliquent intégralement.

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[9] nominative est attribuée à un utilisateur qui la gère sous sa responsabilité. Ainsi tout relais vers une adresse personnelle d'un autre fournisseur de messagerie qui ne relèverait pas du droit français et qui viendrait à compromettre la confidentialité des messages professionnels est fortement non recommandé et serait de la responsabilité de l'utilisateur.

Les données sont protégées par le secret professionnel[10] et le transfert vers une messagerie non gérée par le rectorat peut constituer une violation du secret professionnel. La diffusion restreinte est par ailleurs incompatible avec une messagerie non professionnelle.

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 expresse.

9.1.2 Messages électroniques

Les démarches commerciales ou publicitaires, politiques ou religieuses, contraires aux principes de neutralité et de laïcité du service public de l'éducation sont interdites. De même, sont interdits les messages comportant des contenus à caractère illicite.

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[11] 1369-1 à 1369-11 du code civil.

[9] L'adresse est de la forme prenom.nom@ac-toulouse.fr
[10] http://vosdroits.service-public.fr/particuliers/F530.xhtml
[11] Issus de l'ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique.

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 constitutifs de son activité professionnelle.

Dans le cas où l'utilisateur cesse ses fonctions, de manière définitive ou pour une durée supérieure à 3 mois, **dans l'académie de Toulouse** (cas en particulier de la retraite, d'une fin de contrat, de mutations, de détachements d'un an ou de longue durée, disponibilités, mises à disposition), sa boîte aux lettres nominative professionnelle est maintenue pendant une durée de trois mois. Ce délai permet à l'utilisateur d'avertir les correspondants du changement d'interlocuteur et d'assurer la continuité de service notamment par le transfert des messages reçus au titre de sa fonction précédente.

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 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 réservé à un usage professionnel (administratif et pédagogique) et, à titre résiduel, à un usage privé tel que défini en section 7.1 dans le respect de la législation en vigueur, en dehors du temps de service.

9.2.1 Publication sur les sites Internet et Intranet de l'institution

Toute publication de pages d'information sur les sites Internet ou Intranet de l'institution doit se conformer au respect de la charte de l'institution.

Toute publication doit être au préalable, validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé (pages privées, …) sur les ressources du système d'information de l'institution n'est autorisée.

9.2.2 Sécurité

L'institution met en place des dispositifs de sécurité pour l'accès à Internet. Le contournement de ces dispositifs de sécurité n'est pas autorisé.

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect de la règlementation en vigueur.

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 pouvant se révéler volumineux ou présenter un risque pour la sécurité du système d'information.

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.

9.2.4 Ressource collaboratives

Les ressources collaboratives[12] 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 pour celle-ci :

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

10. Respect de la propriété intellectuelle

L'institution rappelle que l'utilisation des ressources informatiques et numériques implique le respect des droits de propriété intellectuelle.

En conséquence chaque utilisateur doit :

Utiliser les logiciels dans 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 des logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou d'un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

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.

[12] Pour exemple, une ressource collaborative peut être un espace de stockage commun, un carnet d'adresses partagé, une liste de diffusion, un forum, …

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. Limitation 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 a valeur de règlement intérieur pour ce qui concerne l'usage du système d'information.

Elle entre en vigueur dans toute l'académie et pour tous les personnels à compter de sa publication sur le portail de la Sécurité des Systèmes d'Information de l'académie[13].

Fait à Toulouse, le 1er septembre 2016

Pour la ministre de l'Éducation nationale,

La rectrice de l'académie de Toulouse
Chancelière des universités

Hélène Bernard

[13] https://ssi.ac-toulouse.fr