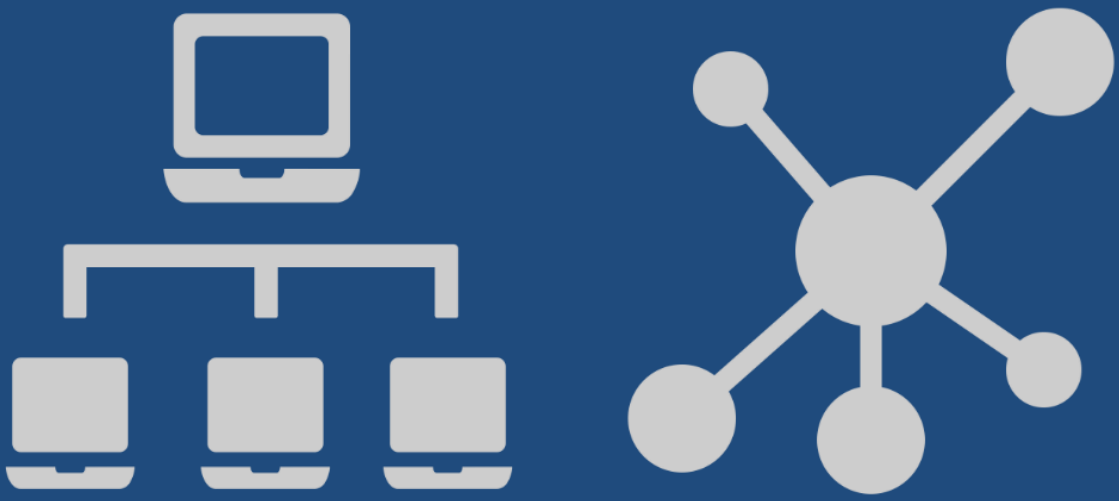
CHARTE D'UTILISATION DU SYSTEME D'INFORMATION



académie Amiens

RÉGION ACADÉMIQUE
HAUTS-DE-FRANCE

MINISTÈRE
DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Table des Matières

I INTRODUCTION 3
I.1 Contexte 3
I.2 Objet 3
I.3 Définitions 3
II CONDITIONS D'UTILISATION 4
II.1 Engagements de l'institution 4
II.2 Engagements de l'utilisateur 4
II.2.1 Utilisation professionnelle et utilisation privée 4
II.2.2 Continuité de service : gestion des absences et des départs 4
II.3 Ressources non institutionnelles 5
II.4 Dispositions générales 5
II.4.1 Moyens d'authentification 6
II.4.2 Devoirs de signalement et d'information 7
II.4.3 Sauvegarde 7
II.4.4 Journalisation et suivi 7
II.4.5 Confidentialité 7
II.4.6 Assistance et maintenance 8
II.5 Dispositions spécifiques 8
II.5.1 Messagerie électronique 8
II.5.2 Internet 9
II.5.3 Ressource collaborative 10
II.6 LES SPÉCIFICITÉS DÉCOULANT DE LA MISSION ÉDUCATIVE 10
II.7 Respect de la propriété intellectuelle 10
II.8 Protection des données à caractère personnel – RGPD et LIL 11
II.9 Limitation des accès 11
II.10 Entrée en vigueur de la charte 11

I INTRODUCTION

I.1 Contexte

- Les informations que nous manipulons tous les jours sont des données 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. Chacun de nous doit en assurer la protection.

I.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 d'Amiens.
- 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 leur intérêt et/ou à l'intérêt collectif du service public 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 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 du Numérique et le Responsable Sécurité des Systèmes d'Information[1].
- La présente charte dans sa version actualisée est disponible sur le site de l'académie d'Amiens.

I.3 Définitions

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

- **Institution** : Elle gère, possède ou met en œuvre le système d'information.
- **Ressource** : élément informationnel[2] 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,
  Agent titulaire ou non titulaire concourant à l'exécution des missions de service public d'éducation.
  Prestataire ayant contracté avec le Ministère de l'Éducation Nationale ou avec une collectivité territoriale ayant compétence partagée avec l'État en matière d'éducation.
- **Ressource non institutionnelle**[3] : ressource mise à disposition des utilisateurs par des tiers.

[1] RSSI : Personne chargée de veiller et garantir la sécurité du système d'information de l'institution.

[2] Les ressources matérielles personnelles ou les services en ligne proposés par des tiers sont des ressources non institutionnelles

[3]. Pour exemple, une ressource informationnelle peut être un fichier informatique, un document rédigé, …

II CONDITIONS D'UTILISATION

II.1 Engagements de l'institution

- L'institution s'engage à :
  - assurer la sécurité du système d'information et la protection des utilisateurs ;
  - faciliter l'accès des utilisateurs aux ressources du système d'information ;
  - respecter la vie privée de chacun.

II.2 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 éthiques et déontologiques professionnelles.
- 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.

II.2.1 Utilisation professionnelle et utilisation privée

- Les systèmes d'information mis à la disposition de l'utilisateur sont essentiellement à usage professionnel.
- Il n'est pas interdit d'utiliser les services ou équipements numériques dans la sphère privée à la condition que cette utilisation reste raisonnable, tant dans la fréquence que dans la durée, qu'elle ne nuise pas à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service et que cela n'engendre pas de surcoût au regard du coût global d'exploitation.
- Par contre il est strictement interdit d'en faire un usage à but lucratif ou d'utiliser, à des fins personnelles, toutes données à caractère personnel auxquelles l'utilisateur a accès dans le cadre professionnel.
- Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Les messages personnels et privés devront être identifiés par un sujet commençant par la mention « PERSONNEL » et les documents stockés dans un dossier nommé « Personnel et privé »[4]
- Dans le cadre d'une utilisation privée d'une ressource non institutionnelle, celle-ci doit répondre aux exigences de sécurité du système d'information.

II.2.2 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. Toutes les ressources mises à disposition de l'utilisateur ne seront plus accessibles.

[4] Une dénomination "Personnel et Privé" ne pourra pas porter à équivoque.

- Lors du départ définitif de l'académie, la messagerie personnelle sera supprimée après une période de six mois suivant la date de fin d'activité. L'utilisateur a la possibilité de demander une prolongation d'usage, à renouveler chaque année, ou une fermeture anticipée.
- Pour les besoins de continuité de service en cas d'absence ou d'indisponibilité d'un agent, l'institution pourra accéder aux données d'un poste professionnel de l'agent dans les conditions suivantes :
    - Le demandeur souhaitant accéder aux données, après avoir obtenu l'accord écrit (courriel, lettre manuscrite, SMS…) du détenteur des données, sollicite l'accès aux documents auprès de l'administrateur du système d'information ;
    - Si l'agent est injoignable ou refuse l'accès, la demande devra être portée par le responsable hiérarchique du demandeur pour solliciter l'administrateur du système d'information. L'administrateur accordera alors cet accès au supérieur hiérarchique. L'agent sera obligatoirement informé de l'accès.

  Quelles que soient les conditions, seront exclus de cet accès les messages et documents personnels et privés identifiés comme tels.

II.3 Ressources non institutionnelles

- La mise en œuvre ou l'utilisation d'un service ou d'une ressource numérique non institutionnelle (réseaux sociaux, services en lignes, éditeurs privés…) 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 ou 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. Le cas échéant, il informera le délégué à la protection des données et la direction des systèmes d'information et du numérique 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.

II.4 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 et 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.

II.4.1 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.
- Les identifiants sont strictement personnels. L'agent ne doit jamais les communiquer.
- La sécurité des systèmes d'information impose de respecter les consignes et les règles de sécurité relatives à la gestion de l'authentification et à la gestion des accès. L'utilisateur se doit notamment de :
    - garder strictement confidentiel(s) son (ou ses) moyens(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.
- 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 II.2.2) ;
- limiter l'accès aux 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.
- Tout équipement utilisé dans un cadre professionnel ou manipulant des données professionnelles (poste de travail, ordinateur ou téléphone portable, …) doit être protégé par un dispositif de sécurité (mot de passe, empreinte, code PIN, …) et doit être verrouillé ou se verrouiller automatiquement à la fin de son utilisation.
- Sauf consignes explicites ou considérations techniques particulières, un mot de passe doit :
  - Être constitué a minima de 8 caractères mixant minuscules, majuscules, chiffres et caractères spéciaux en évitant les caractères accentués, ç et € qui pourraient occasionner des difficultés avec certains claviers ou équipements mobiles ;
  - Être modifié au moins une fois par an.

II.4.2 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 et au DPD de l'institution.

II.4.3 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.

II.4.4 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 (hébergement, messagerie, …) dont elle est prestataire. En complément, l'institution se réserve le droit d'élargir le dispositif de journalisation à l'ensemble du système d'information dans le respect de la réglementation applicable (RGPD).
- Une exploitation de la journalisation du système d'information peut être réalisée à des fins statistiques, de traçabilités réglementaires, fonctionnelles ou techniques, de sécurité ou de détection des abus.
- L'institution assurera l'intégrité de l'horodatage des événements journalisés.

- Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel.

II.4.5 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.

4.5.1 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 ou sa sécurité ;
  - tombent dans le champ de l'article[5] 40 alinéa 2 du code de procédure pénale.

4.5.2 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.

II.4.6 Assistance et maintenance

- En cas de question relative au fonctionnement du système d'information, l'utilisateur consultera en priorité la documentation mise à sa disposition. En cas de problème ou de demande spécifique, l'utilisateur se rapprochera de la plate-forme d'assistance académique. Les modalités d'accès sont consultables sur le site internet de l'académie.
- Pour effectuer la maintenance corrective, évolutive ou à des fins de restauration, l'institution se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à la disposition de l'utilisateur.
- Dans la mesure du possible, les interventions à distance seront précédées d'une information de l'utilisateur.

II.5 Dispositions spécifiques

II.5.1 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.

[5] « 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. »

- 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 mis en place.

5.1.1 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 II.2.1 dans le respect de la législation en vigueur. L'adresse électronique[6] nominative est attribuée à un utilisateur qui l'utilise 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. Les propriétaires ou modérateurs de ces listes de diffusion doivent en assurer leur mise à jour a minima une fois par an ou lors d'un changement de propriétaire.

5.1.2 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 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.
- En cas d'utilisation abusive en nombre, en volume ou en espace de stockage, l'institution pourra être amenée à appliquer des limitations techniques (quotas) afin de garantir une efficacité et une disponibilité optimale du service de messagerie à tous les usagers.
- Par ailleurs, pour des raisons de capacité technique et pour les espaces de messagerie électroniques professionnelles nominatives et fonctionnelles, une suppression automatique sera effectuée :
    - pour les messages placés dans les corbeilles depuis plus de 30 jours ;
    - les messages de plus de 365 jours pour les messageries n'ayant eu aucune connexion depuis au moins 2 ans.

[6] L'adresse est de la forme prenom.nom@ac-amiens.fr

Si l'utilisateur souhaite conserver exceptionnellement ses messages au-delà de ces délais, Il lui appartient de prendre contact avec la DSIN pour étudier les mesures d'archivage nécessaires.

5.1.3 Activation du transfert automatique de messagerie

- La fonctionnalité de transfert automatique de messagerie permet à l'utilisateur de renvoyer tous les courriers qu'il reçoit vers un autre compte de messagerie.
- L'activation de cette fonctionnalité n'est pas recommandée et ne peut se faire que par l'utilisateur et sous sa responsabilité. Cette fonctionnalité pourra être désactivée en cas de modification de la politique nationale décidée au niveau ministériel.
- En aucun cas, ce transfert ne devra être effectué par la communication ou l'enregistrement des identifiants académiques à un fournisseur extérieur à l'académie.
- Que ce soit pour une adresse professionnelle ou fonctionnelle, il appartient à l'utilisateur, avant l'activation, de s'assurer que la destination de ce transfert de courrier soit conforme aux exigences de confidentialité et de protection des données à caractère personnel.

II.5.2 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 II.2.1 dans le respect de la réglementation en vigueur.

5.2.1 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.

5.2.2 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.

5.2.3 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 et du DPD si cela concerne des données à caractère personnel.
- Seules les personnes habilitées peuvent communiquer au sujet et au nom de l'institution.

II.5.3 Ressource collaborative

- Les ressources collaboratives[7] 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 :

[7] Pour exemple, une ressource collaborative peut être un environnement numérique de travail (ENT), un espace de stockage commun, un carnet d'adresses partagé, une liste de diffusion, un forum, …

- 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 concernés ;
- 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.

II.6 Les spécificités découlant de la mission éducative

- L'attention est attirée tout particulièrement sur les spécificités de la mission éducative de l'Éducation nationale. Outre les autres comportements ou usages pénalement sanctionnés, il est rappelé notamment que l'accès, le téléchargement, la production et la consultation volontaire de contenus à caractère pornographique ou raciste depuis les locaux ou avec les ressources mises à la disposition par l'institution, est strictement interdite.

II.7 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.

II.8 Protection des données à caractère personnel – RGPD

- 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.
- L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel.
- 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 à des règles particulières de protection. En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement son délégué à la protection des données (DPD) qui prendra les mesures nécessaires dans le but d'assurer le respect des dispositions légales.
- Conformément à la réglementation, chaque utilisateur dispose d'un renforcement de ses droits afin de mieux protéger ses données personnelles. Ces droits s'exercent directement auprès du délégué à la protection des données de l'établissement dont il dépend.

II.9 Limitation des accès

- En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les différents guides d'utilisation, l'institution pourra, sans préjuger des poursuites pénales ou disciplinaires, limiter les usages par mesure conservatoire.
- Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est passible de sanctions.

III ENTREE EN VIGUEUR DE LA CHARTE

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