CHARTE D'UTILISATION DES SYSTEMES D'INFORMATION ET DE COMMUNICATION PERSONNELS ENSEIGNANTS, NON ENSEIGNANTS, BENEVOLES

PREAMBULE

L'établissement met en place une Charte d'utilisation de son système d'information dans le cadre des lois et règlementations en vigueur.

Cette Charte a pour objectif d'informer les utilisateurs sur leurs droits et leurs obligations dans le cadre d'une utilisation professionnelle et exceptionnellement, personnelle ou privée, des ressources relevant de l'informatique et de la communication de L'établissement.

La Charte a pour objectif d'instaurer la confiance dans l'utilisation du système d'information et de communication de L'établissement et de préserver l'intégrité et le bon fonctionnement de ce système, dans le respect des droits et des libertés de chacun.

ARTICLE 1 : GENERALITES

1.1 Objet de la Charte :

L'objet de la Charte est de règlementer le fonctionnement et l'utilisation du système d'information et de communication de L'établissement.

1.2 Nature juridique de la Charte :

La Charte constitue un engagement des partenaires, conformément aux dispositions de l'article L. 122-39 du Code du travail. Elle remplace et annule toutes dispositions contraires contenues dans le règlement intérieur existant, relatives au fonctionnement et à l'utilisation du système d'information de l'établissement.

Le non respect des règles figurant dans la présente Charte peut engager la responsabilité civile ou pénale de l'utilisateur s'il est prouvé que les faits fautifs lui sont personnellement imputables.

1.3 Champ d'application de la Charte :

La présente Charte s'applique à tout membre du personnel, quel que soit son statut et quelle que soit son ancienneté, et notamment aux salariés mais aussi aux enseignants, aux bénévoles, aux emplois-jeunes, intérimaires et stagiaires, ainsi qu'aux personnes mises à disposition et aux différents partenaires, prestataires et sous-traitants de l'établissement ayant accès au système d'information et de façon générale, à toute personne amenée à créer, développer, maintenir ou utiliser le système d'information et dénommé "utilisateur".

Chaque utilisateur interne ou externe à l'établissement sera informé individuellement du contenu de la Charte.

Les contrats souscrits par l'établissement et qui donnent lieu à un accès à son système d'information par des tiers devront stipuler le respect des règles de la présente Charte par ces tiers ainsi que toute autre personne salariée ou sous-traitante liée contractuellement à eux.

L'utilisation des ressources objet de la Charte, dont l'établissement dispose en tant que propriétaire ou locataire, fait l'objet d'autorisations strictement personnelles et temporaires qui ne peuvent en aucun cas être cédées, même pour une durée déterminée, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation, même à titre provisoire, de l'activité professionnelle qui l'a justifiée.

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau et des moyens de communication auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de son poste.

1.4 Responsable du système d'information :

Le Responsable du système d'information et de communication veille à la protection, à la maintenance, et au bon fonctionnement du système d'information de l'établissement.

Il respecte la présente Charte et s'assure du respect par les utilisateurs de cette dernière. Il agit en concertation avec la direction et les services compétents de l'établissement afin de garantir la conformité avec les dispositions légales, effectuer toute formalité ou déclarations, en particulier celles issues de la Loi Informatique et Libertés du 6 janvier 1978 et de la loi du 10 juillet 1991 sur le secret des correspondances.

Le Responsable a notamment accès aux serveurs de fichiers, aux serveurs de Web et aux serveurs de messagerie de l'établissement, il est donc susceptible de prendre connaissance de l'ensemble des données reçues, émises ou élaborées par les utilisateurs.

Cependant, conformément à l'obligation de confidentialité à laquelle il est soumis, le Responsable ne peut divulguer les informations dont il aurait eu connaissance dans le cadre de ses fonctions, en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs, dès lors qu'elles ne mettent en cause ni le bon fonctionnement technique des applications, ni la sécurité du système informatique, ni quelque intérêt de l'établissement.
Est assimilée au Responsable toute autre personne intervenant dans le cadre des fonctions définies par la présente charte et conformément aux règles en vigueur.
Les référents informatiques qui peuvent être des enseignants, des parents, des emplois-jeunes ou des bénévoles sont placés sous la responsabilité du Chef d'établissement.

1.5 Avis :

La présente Charte a été soumise à l'avis :
- des représentants du personnel
- du conseil d'établissement.

ARTICLE 2 : PROTECTION DU SYSTEME INFORMATIQUE

2.1 Objectifs de la protection

La protection du système d'information et de communication de L'établissement .a pour objectif :

- d'empêcher la diffusion non autorisée des informations de nature

administrative, technique, économique, juridique, financière, artistique, et plus généralement de toute autre information confidentielle, sensible ou stratégique appartenant à l'établissement ;

- de sauvegarder et de conserver la preuve de la date de création et de diffusion desdites informations ;
- de protéger l'intégrité des données et du fonctionnement du système d'information de l'établissement ;
- d'empêcher l'intrusion dans le système d'information de matériels et de logiciels, de données et de fichiers de nature à porter préjudice à l'établissement ;
- de définir les conditions d'utilisation, les mises à jour, la maintenance, la correction, la réparation des matériels et logiciels de l'établissement.

L'intrusion non autorisée dans le système d'information de l'établissement sera considérée comme une infraction pénale. Il est précisé que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est pénalement sanctionné conformément aux dispositions de la Loi n° 88-19 du 5 Janvier 1988 dite « loi Godfrain » (Article 323-1 et suivants du code pénal).

2.2 Exercice de la protection

Le Responsable peut avoir accès à l'ensemble des composants du système d'information et de communication de l'établissement à n'importe quel moment et ce afin d'effectuer tout acte de protection du système d'information qu'il juge opportun.

Afin d'être assisté dans l'accomplissement de sa mission, le Responsable du système d'information peut utiliser des logiciels de prise de main à distance pour accéder à distance à l'ensemble des données de n'importe quel poste de travail informatisé de l'établissement.
Ces interventions sont portées à la connaissance des intéressés.

En cas d'externalisation des opérations de maintenance, l'administrateur s'assure que le prestataire et ses préposés n'accèdent qu'aux données nécessaires à l'accomplissement de leur mission et qu'ils s'engagent par contrat à respecter la confidentialité sur les informations dont ils auraient eu connaissance au cours de leur prestation.

Dans le cas où un composant du système d'information ne se trouverait pas dans les locaux de l'établissement, l'utilisateur qui en a la garde s'oblige à le restituer ou le confier au Responsable à première demande de sa part.

Le Responsable peut mettre en place des outils de contrôle et de surveillance répondant strictement aux finalités de protection du système d'information et surveillance de l'activité des utilisateurs.

La Direction de l'établissement peut être saisie par toute personne intéressée, en cas d'atteinte aux droits des personnes ou aux libertés individuelles et collectives qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

2.3 Mesures techniques de protection

2.3.1 Accès sécurisé au système informatique

L'accès au système d'information et de communication de l'établissement est, sauf dérogation accordée par le Responsable, réservé aux seuls utilisateurs internes de l'établissement.

Le contrôle de l'accès au système d'information permet d'identifier toute personne utilisant un ordinateur. Cette identification permet, à chaque connexion, l'attribution de droits et de privilèges propres à chaque Utilisateur sur les ressources du système dont il a besoin pour son activité professionnelle.

Un identifiant et un mot de passe unique sont confiés à chaque utilisateur qui doit les mémoriser. L'utilisateur est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas les communiquer à un collègue ou un tiers, ni la noter sur document ou dans un fichier. Il est rappelé que le simple fait d'accéder au système d'information au moyen d'éléments d'identifications différents de ceux dont l'utilisateur est le titulaire peut être constitutif d'un accès frauduleux et d'une éventuelle usurpation d'identité pénalement sanctionnés.

En cas d'oubli de son mot de passe, seul le Responsable du système d'information de l'établissement peut en communiquer un nouveau à l'utilisateur. Un autre mot de passe peut être attribué à l'utilisateur pour accéder ou faire fonctionner sa messagerie électronique, ou pour accéder à des fichiers en partage réservé.

Chaque mot de passe est modifié selon une fréquence déterminée par le Responsable. Un mot de passe doit être composé selon les prescriptions du Responsable et conformément aux normes de sécurité en vigueur.

Il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Il est rappelé que le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est pénalement sanctionné.

2.3.2 Les sauvegardes de secours

Chaque utilisateur doit effectuer lui-même la sauvegarde de ses données figurant sur le disque dur d'un poste mis à sa disposition. Le Responsable fixe la fréquence et les modalités de ces sauvegardes pour chaque utilisateur ou groupe d'utilisateurs.
En ce qui concerne le travail en réseau, l'administrateur met en œuvre un système de sécurité comportant des dispositifs de sauvegarde des informations présentes sur le(s) serveur(s).

2.3.3 Les pare-feux

L'établissement dispose de pare-feux destinés notamment à empêcher l'intrusion de virus informatiques.

Le pare-feu contrôle l'ensemble du trafic sortant du système d'information et de communication de L'établissement, aussi bien local que distant. Il contrôle également le trafic entrant constitué notamment de la messagerie électronique, l'échange de fichiers, la navigation sur Internet.

- Il détient toutes les traces de l'activité qui transite par lui : s'agissant de la navigation sur Internet (sites visités, heures des visites, durée des visites, type, nom et volume des éléments téléchargés), s'agissant des messages envoyés et reçus (expéditeur, destinataire(s), objet, type et volume de la pièce jointe, et éventuellement texte du message).

- Il filtre et bloque les adresses des sites Internet non autorisés par le principe de la liste noire, rendant impossible la visualisation des contenus déterminés. Les sites concernés sont illicites, contraires aux bonnes mœurs ou attentatoires aux droits d'autrui comme, notamment, les sites diffusant des données de nature pornographique, pédophile, raciste, révisionniste ou incitant à la

haine raciale, la violence, etc...
Les données recueillies par le pare-feu pourront faire l'objet d'un examen ponctuel, effectué a postériori, afin de détecter d'éventuels abus, ou bien en cas de suspicion à l'égard d'un utilisateur en particulier, tout en garantissant le respect de la vie privée et les libertés fondamentales des utilisateurs sur leur lieu de travail.

2.3.4 Les antivirus

Il est impératif que chaque utilisateur procède à une vérification de la présence de l'anti-virus au moyen de l'interface du poste informatique qu'il utilise. Le Responsable informatique procède à la mise à jour régulière du ou des anti-virus, afin que le système d'information soit protégé de manière efficace.

Chaque utilisateur est tenu d'avertir sans délai le Responsable du système d'information de tout comportement suspect de tout élément matériel ou logiciel du système d'information mis à sa disposition.

ARTICLE 3 : MATÉRIELS, PROGRAMMES ET LOGICIELS

3.1 Mise à disposition

L'établissement met à la disposition des utilisateurs les matériels, programmes et logiciels nécessaires à l'exercice de leur activité professionnelle.

Les utilisateurs ayant, de par leurs fonctions, la possibilité de disposer de matériels et de logiciels à titre mobile ou nomade, doivent prendre toutes les dispositions nécessaires à fin de prévenir le vol ou la détérioration de ces matériels et de ces logiciels.

En particulier, un utilisateur qui à la possibilité de disposer de matériels et de logiciels à titre mobile ou nomade à l'extérieur des locaux de l'établissement doit être assisté par le Responsable pour mettre en œuvre le cryptage des informations traitées (choix de la méthode, du logiciel, détermination des clés, etc…).

Il est rappelé que toute limitation de l'accès à quelque contenu que ce soit (fichiers, messagerie, etc…) au moyen d'un mot de passe ou d'outils de cryptage est soumis à l'autorisation préalable du Responsable.

3.2 Règles d'utilisation

utilisation privée possible :

Les matériels, programmes et logiciels mis à la disposition des utilisateurs doivent être utilisés à titre professionnel.

Une utilisation personnelle de ces ressources est tolérée dans la mesure où celle-ci est n'entrave pas de façon significative la bonne marche du travail des utilisateurs, n'est pas contraire aux intérêts de l'établissement, reste raisonnable dans sa durée, et ne porte pas atteinte à la règlementation en vigueur.
Les fichiers créés dans le cadre d'une utilisation personnelle, laquelle doit conserver un caractère exceptionnel, doivent porter la mention "privé". Les utilisateurs sont tenus de classer ces fichiers dans un répertoire spécifique portant également les mêmes mentions afin de prévenir le Responsable du de la nature particulière s'attachant à cette catégorie de fichiers.
Même dans ce cas, un contrôle du contenu de ces fichiers pourra être effectué, en cas de risque ou évènement particulier, hors la présence de l'utilisateur concerné.

Les utilisateurs s'engagent à ne pas transformer des fichiers à caractère professionnel en fichiers personnels.
Tout fichier ne comportant pas la mention "privé", ou ne comportant pas d'éléments laissant clairement apparaitre qu'il est de nature privée est considéré comme un fichier professionnel par le Responsable. De ce fait, il est librement accessible et exploitable par ce dernier même hors la présence de l'utilisateur.

L'utilisation des matériels, programmes et logiciels doit être effectuée conformément aux recommandations et règles techniques communiquées par le Responsable dans le cadre de notes de service.
Les utilisateurs s'interdisent d'utiliser les matériels, programmes et logiciels en violation des droits de l'établissement et des tiers et, notamment au regard des lois en vigueur sur la propriété intellectuelle et la liberté d'expression.
Les utilisateurs s'interdisent également de modifier de quelque manière que ce soit les matériels, programmes et logiciels qui sont mis à leur disposition sans autorisation préalable du Responsable et de tout titulaire de droits concerné.

3.3 Introduction de nouveaux Matériels, programmes et logiciels

Seul le Responsable est autorisé à introduire ou à permettre l'introduction dans le système d'information et de communication de l'établissement tout nouvel élément (nouveaux matériels, programmes, logiciels et applications...).

Les utilisateurs s'interdisent notamment de télécharger sans autorisation tout programme ou élément de programme, application, "plugin" ou mise à jour à partir de l'extérieur du système d'information et de communication, quand bien même seraient-ils incités à le faire par l'éditeur.

Tout utilisateur doit solliciter l'autorisation préalable du Responsable pour un nouveau matériel, programme ou logiciel, avant son admission et son utilisation dans le système d'information et de communication.

En particulier, est interdite, sans autorisation, justifiée par les exigences de l'activité professionnelle, la mise en œuvre de logiciels permettant (sans que cette liste soit limitative) :
- la réception et l'émission de flux de données (streaming),
- la discussion instantanée,
- l'échange de données partagées en point à point,
- Les jeux et applications ludiques ou à caractère de loisir.

Cette interdiction s'applique à tout type de contenu, qu'il soit assimilé à une application ou un simple fichier à caractère fonctionnel et quel que soit le langage informatique employé.
Ces obligations sont expressément renforcées à l'intention des utilisateurs disposant de tout composant du système d'information à caractère mobile ou nomade, mis en œuvre en dehors des locaux de l'établissement.

Les utilisateurs s'engagent à ne pas mettre en œuvre tout programme destiné à contourner les procédures établies dans le but de garantir directement ou indirectement, de quelque manière que ce soit le niveau de sécurité des systèmes.

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle et de la licence à laquelle est soumis le logiciel. Ces copies ne peuvent être effectuées que par le Responsable ou une personne déléguée par ses soins.

Le Responsable se réserve la possibilité d'effacer toute trace de logiciels, progiciels, programmes ou fichiers créés ou introduits dans le système d'information de l'établissement, en violation des droits des tiers, notamment de propriété intellectuelle, et de dénoncer tout acte délictueux aux autorités, sans préjudice de l'application de sanctions dans le cadre du statut.

ARTICLE 4 : REGLES GENERALES D'EMPLOI DU SYSTÈME D'INFORMATION ET DE COMMUNICATION

4.1 Mise à disposition de la messagerie électronique

Une adresse …@melouvert est fournie aux enseignants par le Rectorat.

Chaque utilisateur peut disposer également d'une messagerie électronique d'Etablissement pouvant exceptionnellement et sous certaines conditions, être utilisée à titre privé.

Cette messagerie électronique est composée du prénom et/ou du nom de l'utilisateur suivi du nom de l'établissement, elle est attribuée par le Responsable qui peut en délivrer une nouvelle à la demande de l'utilisateur si la demande est bien fondée (en cas de changement de nom de l'utilisateur par exemple).

4.2 Mise à disposition d'un accès à Internet

Un accès à Internet est attribué aux utilisateurs afin de permettre la consultation des sites au nom de l'établissement.

4.3 Mise à disposition de moyens de communication

Des moyens de communication fixes ou mobiles peuvent être mis à la disposition des utilisateurs par L'établissement ... dans le cadre de l'activité.

4.4 Cessation de la mise à disposition

Lors du départ définitif ou de la cessation du lien entre un Utilisateur et l'établissement, celui-ci est tenu de restituer sans délai tout matériel mis à sa disposition dans le cadre de son activité et de garantir l'accès illimité et irrévocable par le Responsable à tout contenu relatif à son activité.

L'utilisateur s'engage à ne conserver aucun matériel ou aucune donnée quels qu'ils soient permettant d'accéder au système d'information et de communication.

Il est informé par la Direction de l'établissement et par le Responsable de l'utilisation qui sera faite des fichiers et des messages électroniques professionnels et privés.

4.5 Règles et précautions générales d'utilisation à titre privé

L'utilisation de la messagerie électronique (envoi et réception de messages) ainsi que la consultation des sites internet et enfin l'emploi des moyens de communication sont autorisées à des fins privées à titre exceptionnel, hors temps de cours pour les enseignants.

L'utilisation privée doit globalement respecter des proportions raisonnables, et plus particulièrement les conditions suivantes :
- ne pas affecter le fonctionnement du système d'information et de communication en termes, notamment, de fréquence, de volume, de taille, de format des données échangées (messages électroniques, données de visualisation des sites) ;
- ne pas entraver l'accès professionnel ;
- ne pas influer de façon significative sur la bonne marche du service ;
- ne pas influer sur la bonne exécution des tâches qui sont confiées à l'utilisateur dans le cadre de son poste ;
- ne pas porter de manière générale préjudice à l'établissement.

ARTICLE 5 : REGLES PARTICULIERES A LA MESSAGERIE

5.1 Règles et précautions d'utilisation à titre professionnel

Les règles hiérarchiques et d'organisation des pouvoirs internes de signature doivent être respectées. Ainsi, aucun message électronique ne doit être expédié par un utilisateur qui n'en a pas l'autorité.

Les utilisateurs ne doivent pas répondre à des messages électroniques répétés (spam) ni les transférer lorsque ceux-ci sont reçus à leur insu sur leur messagerie électronique professionnelle et ne présentent aucun rapport avec leurs fonctions et leurs attributions au sein de l'entreprise. Ils s'engagent dans pareil cas à les détruire immédiatement et à avertir le Responsable en cas d'abus manifeste de fréquence ou de volume.

Le message électronique pouvant être reconnu comme preuve ou commencement de preuve par écrit dans le cadre d'un contentieux, les utilisateurs doivent porter une attention toute particulière à la rédaction et à la diffusion de celui-ci, et plus particulièrement dès lors qu'il comporte un engagement, retire ou confère un droit quel qu'il soit.

Les risques liés à l'interception des messages électroniques des utilisateurs exigent de limiter l'utilisation de la messagerie électronique à destination de l'extérieur du système d'information aux informations à caractère non confidentiel et/ou non sensible. L'utilisateur doit consulter la Direction de l'établissement en cas du moindre doute.

Dès lors qu'un utilisateur est contraint de communiquer vers l'extérieur du système d'information et de communication des informations à caractère confidentiel et/ou sensible, l'autorisation préalable du Responsable est nécessaire pour la mise en œuvre de la protection de l'information.

Le Responsable du système d'information peut être éventuellement amené à :
- soit installer un outil de protection et/ou cryptage sur le matériel confié à l'utilisateur ;
- soit assurer lui-même cette transmission cryptée.

Les utilisateurs sont informés que les messages électroniques à caractère professionnel ne peuvent être couverts par le secret des correspondances.

5.2 Règles et précautions d'utilisation à titre privé

L'utilisateur qui entend utiliser la messagerie électronique de l'établissement à des fins privées doit classer ses messages électroniques à caractère personnel (reçus et envoyés) dans un répertoire spécifique portant la mention "privé" et indiquer dans l'objet même des messages électroniques envoyés la mention "privé" de manière à prévenir le Responsable de la nature particulière s'attachant à cette catégorie de messages.
Les utilisateurs s'engagent à ne pas transformer des messages électroniques professionnels en messages personnels.

Tout message électronique reçu ou envoyé ne comportant pas la mention "privé" dans son objet, ou ne comportant pas d'éléments laissant

clairement apparaitre qu'il est de nature privée est considéré comme un message professionnel par le Responsable et sera donc librement accessible et exploitable par ce dernier même hors la présence et l'autorisation de l'utilisateur.

Il est permis d'utiliser, dans le cadre exclusivement privé, les services d'un site Internet fournissant une plateforme d'échange de messagerie électronique, à condition que cette utilisation respecte strictement les mêmes conditions d'utilisation de la messagerie électronique à titre privé et de la consultation d'Internet.

5.3 Contenu des messages électroniques

Aucun message électronique, y compris relevant d'une utilisation privée, ne doit comporter d'éléments à caractère violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, pornographique ou contraire aux bonnes mœurs ou susceptible de porter atteinte au respect et à la dignité de la personne humaine et ce, tant à l'égard des autres utilisateurs que de tout tiers extérieur à l'établissement.

Aucun message électronique y compris relevant d'une utilisation privée, ne doit comporter d'éléments de nature à porter atteinte à l'image de l'établissement.

L'attention des utilisateurs est attirée en particulier sur le fait que le nom de domaine composant toute adresse de messagerie électronique mise en œuvre par l'établissement est un élément concourant à la promotion de l'image de ce dernier.

Aucun message électronique y compris relevant d'une utilisation privée, ne doit comporter d'éléments protégés par les lois en vigueur sur la propriété intellectuelle, autres que ceux expressément autorisés par l'établissement.

De manière générale, aucun message électronique y compris relevant d'une utilisation privée, ne doit comporter d'éléments de nature à porter atteinte aux droits de l'établissement et des tiers, en vigueur au moment de sa diffusion.

Les utilisateurs s'interdisent de solliciter ou d'encourager l'envoi par d'autres utilisateurs ou par des tiers de messages comportant des éléments de cette nature et s'engagent à les détruire immédiatement s'ils sont amenés à en recevoir à leur insu. En cas d'excès manifeste de réception de tels messages, les utilisateurs doivent avertir le Responsable qui peut prendre d'éventuelles mesures de blocage et de protection.

5.4 Contrôles et mesures de la messagerie

Les contrôles mis en œuvre en permanence par peuvent porter sur :
- Les fréquences et volumes globaux d'émission et de réception par utilisateur ;
- Les moyennes et extrêmes relevés au niveau de l'ensemble des utilisateurs.

Dans le cas où la Direction de l'établissement constate une utilisation manifestement anormale et/ou excessive au regard de l'utilisation moyenne de l'utilisation de la messagerie électronique, une analyse individuelle peut être effectuée à titre justificatif et de façon contradictoire avec l'utilisateur concerné.
L'analyse individuelle porte, le cas échéant, sur :
- La fréquence des messages expédiés,
- Les horaires et volumes de chacun des messages expédiés,
- La détermination du caractère professionnel ou privé de chacun des messages, sans pour autant violer caractère privé du contenu d'un message.

Les données recueillies dans le cadre de ces contrôles sont conservées pendant une durée maximale de six mois.

5.5 Format, type et taille des messages électroniques

Afin de garantir le bon fonctionnement du système d'information et de communication, sur décision de la direction de l'établissement, le Responsable peut, à l'égard d'un utilisateur, ou d'un groupe d'utilisateurs, être amené à limiter le format, le type et la taille des messages électroniques ainsi que de leurs pièces jointes envoyés et/ou reçus par l'utilisateur.

Ces limitations doivent être justifiées par l'intérêt général et proportionnelles à l'objectif recherché et les utilisateurs en sont informés au préalable par note de service.

Le Responsable peut, le cas échéant, mettre à la disposition des utilisateurs des outils de compression de fichiers, qui devront être utilisés lorsque les fichiers à adresser en pièce jointe dépassent une taille déterminée.

5.6 Durée de conservation de la messagerie

La messagerie électronique de l'utilisateur est conservée sur le serveur de l'établissement pendant une durée déterminée par le Responsable, ce délai ne dépassant toutefois pas six mois. Au delà de ce délai, les messages seront éventuellement conservés dans le cadre d'un archivage global des données contenues sur les serveurs. (article pertinent dans le cas où la messagerie est gérée par l'établissement lui-même)

ARTICLE 6 : REGLES PARTICULIERES A LA CONSULTATION D'INTERNET

6.1 Règles et précautions d'utilisation particulières à l'accès à Internet

Qu'ils agissent à titre professionnel ou privé, les utilisateurs s'interdisent de :
- Participer à des forums de discussion ou à des dialogues en direct de type "Chat" sans disposer au préalable des autorisations internes nécessaires pour s'exprimer au nom de l'établissement les propos échangés répondant aux mêmes conditions d'utilisation que la messagerie électronique ;
- Inscrire leur adresse électronique professionnelle sur des sites internet sans liens directs avec leurs fonctions et leurs attributions ;
- Participer anonymement à des discussions ou tout type d'échanges en ligne, lesquels répondent aux mêmes conditions d'utilisation que la messagerie électronique ;
- Alimenter des pages personnelles et de manière plus générale tout espace externe au système d'information et de communication sans autorisation du Responsable du système d'information,
- Produire tout contenu à caractère violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, pornographique ou contraire aux bonnes mœurs ou susceptible de porter atteinte au respect et à la dignité de la personne humaine, et d'exprimer toute opinion personnelle étrangère à son activité professionnelle susceptibles de porter préjudice et ce, tant à l'égard des autres utilisateurs que de tout tiers extérieur à l'établissement ;

- Télécharger des logiciels, progiciels, programmes ou fichiers protégés par les lois en vigueur sur la propriété intellectuelle, sans autorisation préalable du Responsable et des ayants droit ;
- Consulter et/ou de télécharger le contenu de sites à caractère pornographique, pédophile, contraires aux bonnes mœurs, raciste, révisionniste ou incitant à la haine raciale ou pouvant revêtir le caractère d'une infraction pénale.

L'établissement ne pourra être tenu pour responsable des modifications ou suppressions d'informations ainsi que des infractions pénales commises par un utilisateur qui ne se sera pas conformé à ces règles.

Le Responsable se réserve la possibilité de détruire toute trace de contenus introduits ou créés dans le système d'information et de communication, en violation des lois, règlements ou des droits de tiers et de dénoncer préalablement à la destruction tout acte illicite aux autorités, sans préjudice des sanctions en vigueur dans le cadre au statut de l'utilisateur.

Les utilisateurs doivent porter une attention toute particulière à leurs activités car leurs données et celles de l'établissement pourront être enregistrées par des tiers et analysées afin d'établir un profil pouvant être utilisé à des fins de prospection commerciale (cookies).

6.2 Contrôles et mesures de l'accès à Internet

Les contrôles mis en œuvre en permanence par le Responsable peuvent porter sur :
- Les durées globales de consultation par utilisateur,
- Les adresses des sites les plus visités par l'ensemble des utilisateurs.

Dans le cas où la Direction de l'établissement constate une utilisation manifestement anormale et/ou excessive au regard de l'utilisation moyenne de l'accès à Internet, une analyse individuelle peut être effectuée à titre justificatif et de façon contradictoire en présence de l'utilisateur concerné.

L'analyse individuelle porte, le cas échéant, sur :
- L'adresse de chaque site consulté,
- Les horaires et durées de consultation de chacun des sites,
- Le volume des données échangées

Les données de connexion recueillies dans le cadre de ces contrôles sont conservées pendant une durée maximale de six mois.

Afin de garantir le bon fonctionnement du système d'information et de communication, sur décision de la direction de l'établissement, le Responsable peut, à l'égard d'un utilisateur, ou d'un groupe d'utilisateurs, limiter la durée de consultation des sites, ainsi que la liste des adresses pouvant être consultées, imposer des configurations de sécurité du navigateur et des limites de taille au téléchargement de contenus par tout moyen technique adéquat.

Ces limitations doivent être justifiées par l'intérêt général et proportionnelles à l'objectif recherché et les utilisateurs en sont informés au préalable par note de service.

ARTICLE 7 : REGLES PARTICULIERES AUX MOYENS DE COMMUNICATION

Les données recueillies par tout système mis en œuvre par l'établissement ou qui sont communiquées par un opérateur fournissant des services de communication à l'établissement pourront faire l'objet d'un examen ponctuel, a postériori, afin de détecter d'éventuels abus, ou bien en cas de suspicion, tout en garantissant le respect de la vie privée et des libertés des utilisateurs sur leur lieu de travail.

En particulier, hormis le Responsable, aucun accès aux relevés individuels identifiant les destinataires des communications ou les services utilisés n'est autorisé, sauf de façon exceptionnelle, notamment en cas d'utilisation manifestement anormale ou abusive de ces services au regard de leur utilisation moyenne constatée au sein de l'établissement.

De tels relevés sont établis et communiqués de façon contradictoire avec l'utilisateur concerné, et les 4 derniers chiffres des numéros des destinataires sont occultés.

ARTICLE 8 : INTRANET

8.1 Mise à disposition

L'établissement peut mettre en œuvre un dispositif d'Intranet fonctionnant sous la responsabilité technique du Responsable du système d'information et sous la responsabilité éditoriale du Chef d'Etablissement.

Aucun utilisateur ne peut introduire ou tenter d'introduire d'éléments ou de contenus sur l'Intranet sans l'autorisation expresse du Responsable et de la direction de l'établissement. Les utilisateurs peuvent formuler toute suggestion à ces derniers quant au contenu ou au fonctionnement de l'Intranet de l'établissement.

8.2 Données personnelles et droit à l'image

L'utilisateur est averti préalablement à toute diffusion sur l'Intranet de données personnelles concernant et, notamment, de l'utilisation de son image.
L'utilisateur peut demander auprès du Responsable d'exercer un droit d'accès, de rectification ou de suppression de toute donnée personnelle le concernant, pour tout motif légitime.

ARTICLE 9 : INFORMATIQUE ET LIBERTÉS

Lorsque l'utilisateur est amené à constituer des traitements automatisés de données personnelles telles que définies par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi du 6 août 2004, il veillera en particulier :
- A se conformer aux règles en vigueur en matière notamment de collecte, de finalité, de durée conservation, de sécurité et de confidentialité des données ;
- A respecter les procédures obligatoires relatives à la Commission Nationale Informatique et libertés (CNIL) ou du correspondant aux données à caractère personnel ;
- A procéder à l'information préalable des personnes concernées quant à la finalité du traitement et les destinataires éventuels du traitement de ces informations ;
- A informer les personnes concernées de l'existence d'un droit d'opposition à la collecte, d'accès et de suppression des informations traitées ;
- A mettre en garde quant au risque inhérent à une éventuelle communication sur internet que des données soient utilisées dans des pays n'assurant pas un niveau de protection suffisant des données à caractère personnel.

Il est rappelé que le non respect des dispositions en matière de traitements de données personnelles peut être constitutif d'infractions pénales (article 226-16 et suivants du code Pénal) sans préjudice de

l'indemnisation des personnes concernées.

L'établissement ne pourra être tenu pour responsable du non respect des dispositions en matière de traitements de données personnelles dès lors que l'utilisateur n'aura pas informé la Direction de la création et la mise en œuvre d'un tel traitement.

ARTICLE 10 : **SANCTIONS**

Les utilisateurs qui contreviendraient aux règles précédemment définies s'exposent :

- A une limitation ou à une suppression de l'accès aux services,
- Aux poursuites disciplinaires prévues dans le cadre des règlements de l'éducation nationale ou définies dans le règlement intérieur de l'établissement,
- Aux poursuites pénales prévues par la loi.

Aucune sanction disciplinaire ne peut être infligée à l'utilisateur sans que celui-ci soit informé dans le même temps et par écrit des griefs retenus contre lui.

En cas de différend relatif à l'utilisation de tout dispositif soumis à la présente charte, l'utilisateur a la possibilité d'accéder aux données complètes relatives à son utilisation relevées par les dispositifs de surveillance mis en œuvre.
Dans le cas où des abus répétés et précisément constatés sont constitutifs d'un non respect de la charte et notamment des articles 4 à 7, la Direction de l'établissement se réserve la possibilité de mettre en place des limitations ou une interdiction de l'utilisation des outils mis à la disposition de l'utilisateur en cause, étant précisé que ces mesures ne pourront en aucun cas affecter directement ou indirectement l'exercice de son activité professionnelle par l'intéressé.

ARTICLE 10 : **INFORMATION**

En tant que partie du Règlement Intérieur de l'établissement, la Charte est été affichée conformément à l'article R. 122-12 du Code du travail le 02 juillet 2008.

Elle est accessible à partir de son espace de travail l'établissement le cas échéant. La Charte s'applique à compter du 1er septembre 2008.

SUITE A LIRE : DEFINITIONS

DEFINITIONS

1) système d'information

Il s'agit des :

- **Matériels informatiques** (entendu comme l'ensemble des éléments physiques employés pour le traitement des données, tels que les ordinateurs, fixes ou portables, et tout autre matériel informatique, connectique ou bureautique incluant les serveurs, hubs, câbles du réseau, photocopieurs, téléphones, fixes ou portables notamment), ainsi que de l'ensemble des **logiciels** contenus dans ou faisant fonctionner, inter-opérer ou protégeant en totalité ou en partie lesdits matériels informatiques, (comprenant, entre autres, les protocoles de communication TCP/IP), permettant notamment la création, la consultation, la modification, la suppression, l'échange, la circulation, la diffusion, la duplication, la reproduction et le stockage de données, fichiers, bases de données, intranet, extranet sous forme d'images, de sons, de textes ou tout autre type de contenu.

- **Moyens de communication** (entendus comme l'ensemble des éléments physiques employés pour les communications entre systèmes et machines, ou entre individus, tels que les téléphones, fixes ou mobiles, et tout autre matériel informatique, fax, télécopieurs, télex, émetteurs/récepteurs radio, talkie walkies notamment…) permettant tous flux quelconques d'information entre les utilisateurs ou avec l'extérieur.

2) Sauvegardes de secours :

Il s'agit des procédures et des matériels destinés à être utilisés dans certains cas d'anomalies de fonctionnement.

3) Pare-feux :

Dispositifs informatiques qui permettent le filtrage des flux d'information entre un réseau interne à un organisme et un réseau externe et qui ont pour objectif de neutraliser les tentatives de pénétration en provenance de l'extérieure et de maîtriser les accès vers l'extérieur, ainsi qu'assurer une surveillance de tout flux de données.

4) Messagerie électronique :

Service permettant aux utilisateurs habilités de saisir, envoyer ou consulter en différé des courriels.

5) Courriel :

Document sous format numérique contenant le plus souvent un texte auquel peuvent être joints d'autres textes, des images ou des sons, qu'un utilisateur saisit, envoie ou consulte, en différé par l'intermédiaire d'un réseau.

6) Adresse de courrier électronique :

Libellé permettant l'identification d'un utilisateur de messagerie électronique et l'acheminement des messages qui lui sont destinés.

7) Internet :

Réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement, de proche en proche, de messages découpés en paquets indépendants.

8) Intranet :

Réseau de télécommunications et de téléinformatique destiné à l'usage exclusif d'un organisme et utilisant les mêmes protocoles techniques que l'Internet.

9) Navigateur :

Logiciel permettant à l'utilisateur de rechercher et de consulter des documents, et d'exploiter les liens hypertextes qu'ils comportent.

10) Site :

Ensemble de documents et d'applications placés sous une même autorité et accessibles par Internet à partir d'une même adresse universelle.

11) Forum de discussion :

Service permettant aux utilisateurs de discuter et d'échanger sur un thème donné : chaque utilisateur peut lire à tout moment les interventions de tous les autres et apporter sa propre contribution sous forme d'articles.

12) Pièce jointe :

Document ou fichier annexé au corps d'un message électronique.

13) Téléchargement :

Transfert de programmes ou de données d'un ordinateur vers un autre.

14) Virus :

Logiciel malveillant, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un évènement donné.

15) Ver, Cheval de troie :

Logiciel malveillant indépendant qui se transmet d'ordinateur à ordinateur par l'internet ou tout autre réseau et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.

16) Répertoire :

Liste d'identificateurs, classés selon des arguments appropriés, permettant l'accès aux informations qu'ils désignent.

17) Donnée personnelle :

Il s'agit de toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (coordonnées, adresse IP, image, empreinte, etc…).