La charte d'utilisation des systèmes d'information et de communication

Révision d'avril 2021

Yvelines
Le Département

yvelines.fr

Sommaire

1. Les raisons, l'intérêt et la portée d'une charte TIC

- Parce qu'il entend respecter et faire respecter les lois et règlements qui encadrent les activités informatiques ;
- Parce qu'il se doit de sauvegarder l'intégrité de son système informatique, son bon fonctionnement et le respect de la confidentialité des données détenues dans ses services ;
- Parce qu'il veut organiser la sécurité juridique, eu égard aux éventuels recours liés à des dommages causés par les agents dans l'accomplissement de leurs missions ;
- Parce qu'il souhaite promouvoir largement l'usage d'outils informatiques modernes et efficaces sur une base de confiance et de responsabilité partagées ;

Le Département des Yvelines :

- Décide que la présente charte s'impose à tous les utilisateurs (cf lexique, page 23) ;
- Rappelle à tous les utilisateurs de ses systèmes d'information que certains usages sont pénalement répréhensibles, que d'autres peuvent nuire au bon fonctionnement du réseau ou sont susceptibles d'engager la responsabilité personnelle de l'utilisateur ou celle de la collectivité ;
- Fixe par la présente charte les conditions générales et particulières d'utilisation des moyens et ressources informatiques et de télécommunication mis à disposition par la collectivité ;
- Porte en parfaite transparence à la connaissance des utilisateurs les dispositifs mis en place pour garantir la sécurité des systèmes et des données.

Cette charte réglemente l'utilisation des systèmes d'information et de télécommunication. Elle comprend les obligations tant des utilisateurs internes ou extérieurs au Département des Yvelines que des administrateurs des systèmes d'information.

Les marchés ou contrats conclus entre la collectivité et tout tiers ayant pour but ou pour conséquence de donner accès aux ressources de la collectivité, devront stipuler que ces tiers utilisateurs s'engagent à prendre connaissance de la présente charte et à la respecter scrupuleusement. Ils sont placés sous la responsabilité d'un agent du Département.

Conformément à l'article 33 de la loi n°84-53 du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale, la charte a été soumise à l'avis du comité technique (CT). Elle est applicable depuis le 15 septembre 2014.

Cette charte est disponible sur l'intranet du Département accompagnée des documents pratiques complémentaires. Elle est également annexée au Règlement Intérieur du Département, ce qui lui confère un caractère contraignant.

La présente charte répond à des impératifs de :

- **Confidentialité** : de par ses compétences légales dans plusieurs domaines sensibles, la collectivité a mis en place des serveurs informatiques qui hébergent des informations confidentielles sur des personnes, des entreprises et des institutions. Elle serait tenue pour responsable au cas où cette confidentialité n'était pas rigoureusement préservée. Cette obligation de confidentialité nécessite de la part des utilisateurs, une grande prudence et des usages adaptés.
- **Légalité :** certains usages de la messagerie et d'Internet sont pénalement répréhensibles, en particulier, ceux qui seraient contraires à la dignité humaine, à l'ordre public et aux bonnes mœurs, ou constitueraient une incitation à la pédophilie, à la haine raciale, à la discrimination à caractère sexiste, au meurtre, au terrorisme, au proxénétisme, au trafic de stupéfiants, à la contrefaçon, au piratage informatique ou seraient susceptibles de constituer une atteinte à la sécurité nationale.
- **Efficacité** : l'usage professionnel des solutions informatiques et de communication est encouragé afin d'améliorer la productivité, la qualité, le confort et la rapidité du travail des agents.
- **Sécurité** : nombreux sont les virus et autres comportements hostiles qui peuvent infecter le système informatique de la collectivité. Afin d'en assurer le bon fonctionnement, la collectivité organise la protection de son système d'information. Elle doit le faire vis à vis des agressions extérieures, mais aussi en proscrivant les usages internes qui peuvent faciliter la compromission du système.

La charte d'utilisation des systèmes d'information et de communication fait l'objet d'un plan de communication et est portée à la connaissance des agents par tous les moyens adaptés.

Un comité de suivi, animé par le Responsable de la Sécurité du Système d'Information (RSSI), veille à la mise en œuvre, au suivi et à l'évolution de la charte.

Ce comité est notamment composé du Directeur des Systèmes d'Information, du Directeur des Ressources Humaines, du Directeur des Affaires Juridiques et des Assemblées, du Directeur de la Commande Publique Unifiée, du Délégué à la protection des données ou d'un des représentants de chacun. Il se réunit en cas de nécessité.

Ayant un rôle de conseil, de recommandation et d'alerte, le RSSI est le correspondant privilégié pour toute question relative à la mise en application des dispositions de la charte d'utilisation des systèmes d'information et de communication. Il peut être directement contacté à l'adresse électronique suivante : rssi@yvelines.fr

2. L'utilisateur au sein du Département

2.1 Ma responsabilité et mon obligation de vigilance

Comme tout utilisateur, je suis responsable de l'usage rationnel et loyal des ressources informatiques et du réseau auxquels j'ai accès et contribue à leur sécurité.

À ce titre, **je m'engage à** prendre soin des matériels et des installations informatiques mis à ma disposition. Je signale tout dysfonctionnement ou anomalie que je constate, toute erreur d'utilisation pouvant entraîner des conséquences dommageables : je contacte sans délai la Direction des systèmes d'information (DSI) au 88 88 ou sur MonPortailDSI (https://monportaildsi.yvelines.fr/s/dsi) et/ou le Délégué à la protection des données par mail : dpo@yvelines.fr

Exemple :

- perte d'une clef USB non sécurisée contenant des fichiers des usagers du Département ;
- transmission accidentelle d'un fichier contenant des données personnelles au mauvais destinataire ;
- accès non autorisé à des données personnelles ;
- violation ou tentative de violation suspectée d'un compte informatique ;
- publication involontaire de données sur internet ;
- etc.

Je m'engage à ne jamais utiliser (ou communiquer) mes identifiant et mot de passe professionnels pour accéder à un réseau, un service ou une application qui serait étranger au Département des Yvelines.

2.2 Mes conditions d'accès au système d'information

Le droit d'accès aux ressources informatiques et de télécommunication de la collectivité est conditionné au respect des termes de cette charte.

Les accès informatiques sont personnels, uniques, incessibles et temporaires. Ils cessent avec la disparition des raisons qui ont motivé leur attribution.

Par ailleurs, l'étendue des ressources informatiques auxquelles j'ai accès peut être limitée en fonction des besoins réels et des contraintes imposées par le partage de ces ressources avec d'autres utilisateurs.

Le droit d'accès peut être suspendu, par mesure conservatoire de l'autorité hiérarchique ou par la DSI si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

Les accès sont strictement personnels et confidentiels. Ainsi je prends bonne note des points suivants :

- quand l'utilisation d'un système informatique implique l'ouverture d'un compte nominatif, l'utilisateur ne doit pas se servir, pour y accéder, d'un autre compte que celui qui lui a été attribué par l'administrateur habilité. Il ne doit pas chercher à masquer sa véritable identité ;
- tout besoin d'autorisation nouvelle doit faire l'objet d'une demande à la hiérarchie habilitée et ne peut justifier l'usurpation de l'identité informatique d'autrui, avec ou sans son consentement ;
- l'utilisateur s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux applications ou au réseau, à travers un poste de travail professionnel dont il a l'usage.

2.3 La confidentialité de mes données, de celles auxquelles j'accède ou que j'échange

Chaque utilisateur accède au réseau par un nom de compte unique (identifiant) auquel est associé un mot de passe confidentiel, dont il est propriétaire.

Toutes les connexions réalisées à l'aide du compte de l'utilisateur engagent sa responsabilité. Il lui appartient donc de ne communiquer son mot de passe à aucune tierce personne, ni même à un agent de la DSI.

Cette pratique est d'autant nécessaire que des outils de synchronisation des identifiants ont été mis en place. Ces outils permettent de donner des accès à la messagerie, à Internet, à des applications (intranet, messagerie, etc…) ou des fichiers avec une identification unique. Dès lors, si je confie mon mot de passe à une personne, celle-ci pourra accéder à l'ensemble de mon dossier personnel et utiliser potentiellement mon identité numérique.

Je m'engage expressément à :

- ne pas masquer ma véritable identité ;
- ne pas usurper l'identité d'autrui ;
- ne pas quitter mon poste en laissant une session en cours non verrouillée ;
- ne jamais « prêter » mon mot de passe ;
- changer immédiatement de mot de passe en cas de doute sur son intégrité ;
- signaler à la DSI toute anomalie constatée.

Pour des raisons de sécurité, l'administrateur de la DSI impose un changement régulier de ce mot de passe.

Des mises en veille automatiques ont été paramétrées sur les postes de travail, protégées par un mot de passe. Ces mises en veille automatiques ne doivent pas être supprimées pour des raisons de sécurité.

Au cours de son activité professionnelle, chaque utilisateur est amené à accéder à des données à caractère personnel et à respecter la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du Règlement général sur la protection des données, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage pendant toute la durée de mes fonctions et après la cessation de celles-ci, quelle qu'en soit la cause à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

2.4 Le matériel qui m'est confié

Je sais que l'utilisateur est responsable du matériel qui lui est confié pour accomplir ses missions. Ce matériel ne constitue en aucun cas un équipement ou un espace privé.

Je m'engage donc à ne pas effectuer les opérations suivantes qui pourraient avoir des conséquences directes sur le matériel mis à ma disposition :

- modifier le fonctionnement, le paramétrage et les caractéristiques de mon poste de travail informatique (installation de nouveaux matériels, de logiciels même gratuits, modification de fichiers systèmes, systèmes de cryptage autres que ceux fournis par la DSI,…) ;
- modifier des éléments de configuration tels que veilles animées, curseurs animés, fonds d'écrans dans des limites portant atteinte aux performances de mon poste de travail ;
- accéder ou essayer d'accéder à des informations privées d'autres utilisateurs du réseau. Il est expressément rappelé que l'accès à des informations privées d'autres utilisateurs, leur éventuelle destruction ou modification sont des agissements pénalement sanctionnés.

Lors d'une absence prolongée (nuit, week-end), il est demandé, pour terminer proprement mes sessions, d'éteindre mon poste de travail. Ce geste procède également d'une démarche écocitoyenne (réduction de la consommation électrique).

Les postes non affectés spécifiquement à un agent sont dits en libre-service. Ils sont destinés à permettre à plusieurs personnes (sur un même équipement et pour un créneau horaire réservé) de disposer d'un accès partagé au système d'information. Sur ces postes, les utilisateurs adaptent leur temps de consultation à la nécessité de mutualiser ces équipements. Les mêmes droits et devoirs sont applicables aux utilisateurs de ces postes.

Les utilisateurs qui ont recours à des matériels de mobilité tels que téléphones (mobiles ou smartphones), tablettes ou ordinateurs portables s'engagent à sécuriser d'une part l'accès physique à leurs matériels (par exemple en utilisant le câble antivol) et l'accès aux données qu'ils contiennent par le respect des consignes de sécurité en matière de mot de passe et de mise en veille notamment. Ils sont responsables de la sauvegarde des données présentes sur leur terminal.

Les cybercafés, les hôtels, les lieux publics n'offrent pas de garantie de confidentialité, il convient donc de rester prudent dans les échanges de données réalisés en ces lieux. Lors d'un voyage à l'étranger, il est demandé de ne pas partir avec des données sensibles ou bien alors de chiffrer ces données ou les protéger par un mot de passe.

En cas de perte, de vol ou de détérioration d'équipement informatique ou de télécommunication appartenant à la collectivité, **je m'engage à** :

- en cas de vol : établir une déclaration auprès du commissariat de police ou de gendarmerie le plus proche, la transmettre à la DSI (par le portail https://monportaildsi.yvelines.fr/s/dsi) ;
- en cas de perte : établir une déclaration sur l'honneur de perte validée par le responsable hiérarchique et la transmettre à la DSI (par le portail https://monportaildsi.yvelines.fr/s/dsi) ;
- en cas de détérioration : établir un rapport circonstancié relatant les faits, validé par le responsable hiérarchique et le transmettre à la DSI ;
- avertir sans délai la DSI et le responsable hiérarchique ;
- demander à la DSI de modifier immédiatement le mot de passe ;
- alerter le supérieur hiérarchique si l'équipement contenait des données sensibles, confidentielles ou pouvant porter atteinte aux intérêts du Département en cas de diffusion : la DSI préviendra le Délégué à la protection des données et pourra, selon l'équipement concerné, effacer les données à distance sur le terminal volé ou perdu.

2.5 Les logiciels qui sont mis à ma disposition

L'utilisateur n'est habilité à installer aucun logiciel ou jeu sur ses équipements (poste de travail, tablette, smartphone...), qu'il soit payant ou gratuit, de quelque origine qu'il soit. Cette installation est réalisée par la DSI sous réserve d'une validation préalable d'opportunité formalisée par le responsable hiérarchique auquel l'agent est rattaché.

L'utilisateur n'est pas davantage autorisé à utiliser à titre professionnel des services applicatifs gratuits ou des réseaux sociaux qui n'auraient préalablement pas été évalués et validés par le Département.

Cette validation technique et sécuritaire revient à la DSI qui apprécie :

- leur conformité à la Réglementation générale européenne sur la protection des données (RGPD) et à la Loi « Informatique et Libertés » de 1978 modifiée en vigueur ainsi que les recommandations liées à la protection des données personnelles,
- la robustesse technique de ces solutions alternatives,
- leur capacité à garantir et préserver la confidentialité, l'intégrité et la disponibilité de données transmises.

Aucune copie de logiciels n'est autorisée en dehors des copies de sauvegarde. L'utilisateur est informé que l'usage et la diffusion de logiciels piratés constituent un délit passible d'amende et d'emprisonnement. Leur diffusion correspond à du recel. La DSI se réserve la possibilité d'interdire techniquement l'installation de logiciels directement par les utilisateurs, voire de les désinstaller.

Je m'engage à ne pas chercher à contourner, désactiver ou désinstaller les logiciels de protection et de filtrage.

2.6 Les données et fichiers auxquels j'accède

L'ensemble des données saisies et mises en forme par l'utilisateur dans le cadre de ses missions appartient à la collectivité (hors répertoire désigné ou incluant le mot « Privé », « Personnel » ou « Droit syndical »).

Tous les fichiers de l'utilisateur (hors ceux dans les dossiers décrits supra) doivent être partagés dans le cadre de l'organisation de la collectivité afin d'assurer la continuité du service public. Les fichiers électroniques doivent faire l'objet d'un archivage électronique suivant les mêmes règles de conservation que les documents « papier » de même nature. Les fichiers sur serveurs partagés doivent être triés et organisés.

L'utilisateur est responsable de la sauvegarde des données présentes sur son poste de travail en les déposant sur les ressources gérées par la DSI (arborescence de fichiers, gestion électronique de documents SharePoint) qui bénéficient d'une sauvegarde automatisée.

La création de fichiers contenant des données personnelles (ou d'un traitement de données personnelles papier ou informatisé) doit être portée à la connaissance du Délégué à la protection des données de la collectivité (à l'adresse mail suivant : rgpd@yvelines.fr) qui instruira la demande, accompagnera l'utilisateur et effectuera les formalités nécessaires à la mise en œuvre des traitements de données personnelles (cf. Annexe 2.3). Le Délégué à la protection des données doit être saisi au début du projet et avant toute mise en place du fichier ou de tout traitement de données personnelles.

Lorsqu'ils contiennent des données personnelles, les documents bureautiques, stockés sur des serveurs de fichiers, tels que les arborescences, ou dans une solution de gestion électronique de documents telle que SharePoint, sont considérés comme des prolongements du système d'information dont ils sont les sous-produits, et doivent répondre aux mêmes exigences en termes de protection des données à caractère personnel que le système d'information concerné (pertinence et finalité des données, durée limitée de conservation, sécurité et confidentialité, transparence, respect du droit des personnes).

2.7 Ma communication écrite

2.7.1 Ma messagerie électronique

2.7.1.1 Comportements interdits

Il est interdit aux utilisateurs de stocker, transférer ou diffuser des courriels professionnels ou privés comprenant :

- des éléments de nature offensante, diffamatoire, injurieuse, à connotation pornographique, sexiste ou raciste,
- des incitations à des diffusions en chaîne ou pyramidale.

2.7.1.2 Conservation des messages

Comme l'ensemble des documents produits dans le cadre des activités des agents du Département (papiers et électroniques), les messages envoyés ou reçus doivent faire l'objet d'opérations

d'archivage. Les documents engageants pour la collectivité font l'objet d'une attention toute particulière et doivent être enregistrés dans les dossiers correspondants sur le réseau.

Pour des raisons de fonctionnement (restauration de messages supprimés accidentellement), il existe une sauvegarde des messages échangés. Cette sauvegarde permet de récupérer des messages jusqu'à deux mois maximum.

Une logique de quota peut permettre de contenir l'augmentation régulière des tailles de boîtes aux lettres et d'améliorer la gestion individuelle de la messagerie.

2.7.1.3 Sécurité

La messagerie est devenue le premier vecteur de propagation des virus. Des outils ont été mis en place pour se prémunir contre ce type d'attaque. Tout message infecté détecté par le système de protection est éradiqué par nettoyage ou traité par le système antispam.

Toutefois, il est impossible de garantir un niveau de sécurité total. Il est donc nécessaire de respecter les précautions simples décrites ci-après :

- les messages suspects (ayant un objet douteux, un émetteur inconnu, une pièce jointe étrange ou de type « .exe », …) ne doivent pas être ouverts mais supprimés ou directement transférés à la DSI pour analyse ;
- afin d'assurer un niveau de sécurité maximum, il est strictement interdit de désactiver les systèmes de protection du poste de travail installés par la DSI.

Par ailleurs, les exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau conduisent la DSI à mettre en place des outils de mesure de la fréquence et de la taille des fichiers transmis en pièce jointe aux messages électroniques.

2.7.1.4 Le mot de passe de la messagerie

Il n'existe pas de définition universelle d'un bon mot de passe, mais sa complexité et sa longueur permettent de diminuer le risque de réussite d'une attaque informatique qui consisterait à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères.

Selon les recommandations de l'Agence national de la sécurité des systèmes d'information (ANSSI) et la Commission Nationale de l'Informatique et des Libertés (CNIL), « *« Un bon mot de passe contient 12 caractères d'au moins quatre types différents : majuscule, minuscule, chiffre et caractères spéciaux.* »(Cf. Annexe 3, page 32)

2.7.1.5 Utilisation de la messagerie électronique à des fins personnelles

Il est considéré que tout message reçu ou envoyé à partir du poste de travail mis à disposition de l'utilisateur revêt par principe un caractère professionnel.

L'utilisation de la messagerie à des fins personnelles, lorsqu'elle est rendue nécessaire par les impératifs de la vie courante et familiale, est tolérée si elle est mesurée. Dans ce cas, doit être supprimée toute mention relative au Département (telle que la signature automatique) ou tout autre indication laissant à penser que le message est rédigé dans le cadre de l'exercice de ses fonctions.

Le message qui comporte en objet la mention « Privé », « Personnel » ou « Droit syndical » bénéficie du droit au respect de la vie privée et du secret des correspondances.

Tout message qui n'est pas identifié comme tel est réputé être professionnel. Cependant, des messages professionnels ne peuvent pas être transformés en correspondance privée permettant ainsi à les communiquer à des personnes extérieures non autorisées.

L'utilisateur est informé que, pour des raisons de sécurité, d'organisation ou de gestion de l'encombrement du réseau, la DSI peut mettre en place des dispositifs d'analyse de messages ou des dispositifs visant à limiter la taille des messages échangés. La mise en place de ces dispositifs n'ayant pas pour objet le contrôle individuel des utilisateurs, la confidentialité des messages sera respectée.

Cette protection édictée ici n'existe plus si une enquête judiciaire est en cours (par exemple, si vous êtes accusé de transmettre des informations confidentielles à des tiers) ou si votre employeur a obtenu une décision d'un juge l'autorisant à accéder à ces messages. Votre employeur peut ainsi demander au juge de faire appel à un huissier qui pourra prendre connaissance de vos messages.

- je pense à consulter mes messages au moins une fois par demi-journée ;
- je privilégie la relation directe à l'échange de mails ;
- je ne mets en copie que les personnes qui ont réellement besoin de l'être ;
- j'utilise l'option « Répondre à tous » avec grande modération ;
- je prends le temps de réfléchir avant de répondre à un message ;
- je respecte les usages de politesse et savoir-vivre.

Je clique ici pour découvrir tous les conseils d'utilisation qu'a réunis pour moi la DSI

2.7.2 Ma présence sur les réseaux sociaux

Le droit d'expression directe et collective des salariés vise à définir les actions à mettre en œuvre pour améliorer l'organisation et les conditions de travail, ainsi que la qualité du travail réalisée au sein de l'équipe, du site ou de la collectivité.

Les outils numériques disponibles au sein du Département peuvent être utilisés pour favoriser ce droit d'expression. Il en est ainsi notamment :

- des outils comme les réseaux sociaux de la collectivité ou les forums,
- pour des échanges en direct : des outils de visioconférence ou de messagerie instantanée avec vidéo,
- d'autres modalités de recueil d'expression comme les baromètres sociaux.

Les réseaux sociaux internes et externes sont devenus de nouveaux outils de partage et de communication. Ils entrent dans le cadre de la présente charte et sont astreints aux mêmes règles, bonnes pratiques et obligations que les autres systèmes informatiques.

Pour les réseaux sociaux internes (blogs, forums, fils de discussion, tchats, …) :

- **valeur ajoutée** : ne contribuer que si l'intervention apporte une valeur ajoutée au thème concerné,
- **responsabilité :** être responsable de ses contributions, respecter la discrétion et la confidentialité professionnelles associées aux sujets abordés,
- **tonalité :** être professionnel sur le fond et rester courtois dans les échanges,
- **contribution :** adapter sa réactivité et ses contributions à son rôle dans les thèmes concernés, ne pas négliger ses autres obligations professionnelles,
- **respect :** ne pas publier des jugements et considérations sur d'autres personnes.

Pour les réseaux sociaux externes (blogs, Facebook, LinkedIn, Twitter, tchats …) :

- ne pas utiliser ses login et mot de passe professionnels,
- ne pas porter atteinte aux intérêts de la collectivité,
- être responsable de ses actions et parler à la première personne,
- ne jamais utiliser une fausse identité,
- ne pas publier des contenus répréhensibles par la loi,
- ne jamais divulguer une information confidentielle.

L'attention des agents est attirée sur le caractère public des propos tenus sur les blogs, et sur les risques de porter ainsi atteinte à leurs obligations.

En outre, les juridictions administratives et judiciaires considèrent qu'en fonction des « paramétrages » effectués par son utilisateur, un réseau social peut constituer soit un espace privé, soit un espace public.

À titre d'illustration, pour savoir si la page Facebook est un espace privé ou un espace public, les paramètres de confidentialité sont pris en compte de la manière suivante :

- si le compte est ouvert à toutes les personnes se connectant sur Facebook : c'est un espace public,
- si le compte est ouvert aux amis et à leurs amis : c'est un espace public,
- si le compte reste limité au cercle fermé d'amis dûment listés : c'est un espace privé.

2.8 Mon utilisation d'Internet

Seuls ont vocation à être consultés les sites Internet ayant un lien direct et nécessaire à l'activité professionnelle et présentant une utilité au regard des missions et fonctions à exercer.

Une consultation ponctuelle et mesurée des sites Internet est admise dès lors que leur contenu :

- n'est pas contraire à l'ordre public,
- ne met pas en cause les intérêts et les règles éthiques et déontologiques de la collectivité,
- ne constitue pas une incitation à transmettre des données personnelles (par exemple : données personnelles de type professionnel (adresse électronique de l'agent, par exemple) ou confidentielles (données qui seraient la production et la propriété du Département).

Le Département sanctionnera toute utilisation abusive, notamment pour le téléchargement de fichiers audio ou vidéo, etc.

Je m'engage en conséquence à respecter expressément les lois et règlements en vigueur sur le territoire français, et notamment de manière non limitative ceux régissant le fonctionnement des services en ligne, le commerce, la vente à distance, la protection des mineurs, le respect de la personne humaine et de la vie privée, la protection intellectuelle.

Je m'interdis de consulter, télécharger, stocker, diffuser ou rendre accessible, de quelque façon que ce soit, tout site ou message dont le contenu serait de caractère diffamatoire, injurieux, obscène, xénophobe, pornographique ou contraire notamment à la dignité humaine, à l'ordre public et aux bonnes mœurs, ou constituant une incitation à toute forme d'intolérance ou de malveillance, à la haine raciale, au meurtre, au terrorisme, au proxénétisme, au trafic de stupéfiants, à la contrefaçon, au piratage informatique ou susceptible de constituer une atteinte à la sécurité nationale.

Dans la mesure où des utilisations contrevenant aux règles ci-avant énoncées sont susceptibles d'engager la responsabilité civile et/ou pénale du Département, outre bien évidemment la mienne, l'administrateur de la DSI, de par la loi, est tenu à exercer un droit de regard sur l'usage de l'Internet par le personnel et une traçabilité de tous les accès Internet.

2.9 Mon utilisation des téléphones fixe et mobile

L'utilisation de la téléphonie fixe du Département (au travers d'un poste téléphonique ou d'un « softphone », logiciel de téléphonie installé sur un ordinateur) et mobile est également réservée à des fins professionnelles. Néanmoins, un usage ponctuel de la téléphonie fixe et mobile pour des communications personnelles, hors numéros à tarifs spéciaux et appels vers l'étranger, est toléré à condition que cela n'entrave pas l'activité professionnelle.

Les agents sont invités à protéger leur messagerie téléphonique par un mot de passe, dont ils assureront la confidentialité. En cas d'absence, le poste doit être renvoyé soit sur celui d'un collègue, soit sur la messagerie téléphonique.

Il faut noter que, pour tout appel téléphonique émis depuis les lignes fixes de la collectivité, les six premiers chiffres sont conservés avec le numéro du poste appelant et la durée de communication pendant douze mois courant à la date de l'exigibilité des sommes dues en paiement des prestations des services de téléphonie (délai prévu à l'article L. 34-2 du code des postes et des communications électroniques).

Les agents dotés d'un terminal de téléphonie mobile (ou « smartphone ») sont responsables du matériel (son maintien en bon état de fonctionnement, sa protection contre toute détérioration, sa surveillance en situation de déplacement) et de l'usage qui en est fait (nombre, nature, durée des appels, volume des téléchargements ou échanges de données).

A tout téléphone mobile est associé un contrat qui lie le Département à un opérateur. Ce contrat permet à chaque agent de bénéficier pour une somme forfaitaire définie dans notre marché d'un ensemble de services (voix, SMS, data) s'inscrivant dans un ensemble de contraintes (notamment liées au numéro appelé, au lieu d'émission de l'appel, au volume des data chargées…).

L'agent doté d'un téléphone mobile doit avoir pris connaissance des limites d'utilisation associées au contrat opérateur, qu'il se trouve au bureau, chez lui, en déplacement ou bien à l'étranger.

Les responsables hiérarchiques sont destinataires de l'état des consommations individuelles de téléphonie fixe et mobile. Ils ne peuvent accéder aux relevés individuels des numéros de téléphone appelés ou des services de téléphonie utilisés que de façon exceptionnelle, notamment en cas

d'utilisation manifestement anormale de ces services au regard de l'utilisation moyenne constatée au sein de la collectivité.

- je pense à protéger mon téléphone mobile par un code d'accès qui m'est personnel ;
- j'enregistre une annonce personnalisée conviant mon interlocuteur à laisser un message ;
- je préfère paramétrer le mode vibreur plutôt qu'une sonnerie qui pourrait gêner mes voisins quand je travaille dans un espace partagé ;
- je passe mes appels depuis un espace-bulle ou un couloir ;
- je ne parle pas trop fort si je ne suis pas seul…

Je clique ici pour découvrir les conseils d'utilisation que la DSI a réunis pour moi

2.10 Mon utilisation des dispositifs d'impression

L'utilisation des dispositifs d'impression est réservée à des fins professionnelles. Néanmoins, un usage personnel ponctuel est toléré à condition que cela n'entrave pas l'activité professionnelle.

Il est à noter que, dans le cadre de l'utilisation d'un dispositif d'impression équipé d'un moyen d'identification de l'agent, des informations sont enregistrées par le système d'information dans un journal électronique. Aucune trace du document imprimé n'est conservée, seules les informations suivantes sont enregistrées : le jour, l'heure, le lieu, l'identité de l'agent, le nom et le type de document imprimé, le nombre de pages et le mode d'impression (noir et blanc, couleur, recto-verso).

Les responsables hiérarchiques peuvent être destinataires du journal d'utilisation des dispositifs d'impression pour la partie qui intéresse leurs collaborateurs. Ainsi peuvent-ils être en mesure d'identifier une utilisation manifestement anormale de ces dispositifs et en droit de demander une explication à leurs collaborateurs.

- Je fais appel au service de reprographie pour imprimer de manière écoresponsable mes documents de plus de 50 pages ou en plusieurs exemplaires ;
- J'imprime de préférence mes documents de moins de 50 pages en Noir & Blanc et en Recto / Verso.

Je clique ici pour découvrir les conseils d'utilisation que la DSI a réunis pour moi

2.11 Mon droit à la déconnexion

L'article 55 de la loi N° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels introduit dans le code du travail la notion de « droit à la déconnexion » et enjoint les employeurs à mettre en place « des dispositifs de régulation

de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos et de congé ainsi que de la vie personnelle et familiale. »

Le droit à la déconnexion peut donc être entendu comme le droit de chaque salarié de ne pas répondre aux courriels et autres messages en dehors des heures de travail, afin de garantir l'équilibre entre vie professionnelle et vie privée, les temps de repos et de récupération, de réguler la charge mentale et réduire les risques d'épuisement professionnel (« burn-out »).

Le développement des outils numériques permet de contacter de plus en plus facilement et rapidement ses interlocuteurs, de consulter ses messages à tout moment. Cette possibilité ne doit cependant pas aboutir à des excès et implique de fixer certaines règles.

Les emails et SMS constituent aujourd'hui des outils importants de communication professionnelle, au même titre que les réunions ou les échanges téléphoniques. S'ils sont vecteurs de gain de temps, ces outils peuvent aussi et paradoxalement engendrer des pertes de temps ou d'efficacité et des surcharges de travail, lorsque leur usage est inadapté.

Les appels téléphoniques ou l'envoi de SMS se font normalement en direction de téléphones professionnels, sauf urgence ou situation exceptionnelle, et pendant les horaires de service. Concernant les emails, l'envoi est à éviter en semaine entre 20 h et 8 h, le week-end et les jours fériés.

Il n'est pas attendu de réponse aux messages sur ces mêmes créneaux. Ce principe est modulé en fonction des cycles de travail pour les agents en horaires décalés ou d'astreinte et ne s'applique pas, bien entendu, en cas de gestion de crise.

Le droit à la déconnexion s'exerce également lors de la participation à une réunion de travail : l'utilisation d'appareils connectés, que ce soit pour consulter ses messages ou en envoyer, ne doit pas détourner l'attention des participants, ni pouvoir être interprétée comme une marque de désintérêt à l'égard des autres participants. Une consultation discrète doit être envisagée.

- j'évite de lire ou d'envoyer mes messages entre 20h et 8h ;
- j'évite de répondre à un mail durant mes congés puisque j'ai déjà rédigé un message d'absence annonçant ma date de retour et que j'ai précisé qui suivait mes dossiers ;
- en réunion, je me déconnecte et reste attentif au propos de mes interlocuteurs, je participe aux échanges, je m'implique dans les décisions qui sont prises.

Je clique ici pour découvrir les conseils d'utilisation que la DSI a réunis pour moi

2.12 En mon absence

2.12.1 Cas de l'absence planifiée

Dans le souci d'assurer la continuité de l'activité, l'agent doit en cas d'absence :

- renvoyer ses lignes téléphoniques (fixe et mobile) vers un collègue ou enregistrer un message d'absence ;

- créer dans sa messagerie électronique un message automatique de réponse, dans lequel il informe l'expéditeur de sa date de retour et lui propose d'adresser sa demande à l'un de ses collaborateurs ou collègues.

A défaut, le responsable de service peut demander à la DSI d'habiliter un mandataire provisoire pour accéder aux ressources individuelles informatiques ou téléphoniques de l'agent.

Il aura préalablement communiqué (ou tenté de communiquer) cette intention à l'agent de manière officielle par tous moyens compatibles avec l'urgence de la situation.

La personne désignée provisoirement mandataire de ces accès est tenue à une obligation de réserve et n'est autorisée à ne prendre connaissance que des contenus strictement professionnels de l'agent absent.

Pareille procédure exclut tout accès aux répertoires et/ou boîtes aux lettres expressément signalés par les agents comme lieu de stockage de données personnelles ou syndicales (identifiés par « Privé », « Personnel » ou « Droit syndical »).

Ces démarches permettent d'avoir accès aux données et documents nécessaires à l'activité du service, contenus par exemple sur la messagerie, le répondeur vocal, les fichiers sur le réseau ou les outils collaboratifs.

Les messages identifiés comme personnels ou privés, émis ou reçus par le collaborateur depuis son poste de travail professionnel, ainsi que les fichiers identifiés comme tels et contenus sur le disque dur du collaborateur ne peuvent être ouverts (et seront donc supprimés) par l'employeur, sans l'accord de la personne concernée.

En revanche, les messages professionnels émis ou reçus par le salarié ainsi que les fichiers professionnels contenus sur le disque dur de celui-ci peuvent être librement consultés par l'employeur.

Par conséquent, si le fichier ou le dossier n'est pas notifié comme étant personnel ou relevant du droit syndical, il doit être présumé, par défaut, comme étant professionnel.

2.12.2 Cas de l'absence soudaine et imposée (force majeure)

Dans le cas d'un arrêt non planifié où l'agent ne serait pas en mesure de paramétrer ses lignes téléphoniques ou sa messagerie électronique, le Département désigne un collaborateur ou collègue mandataire et l'habilite à accéder à la messagerie électronique afin de créer le message automatique de réponse susmentionné ou d'accéder aux messages professionnels utiles à la continuité du service et à renvoyer les lignes de l'agent absent sur celles d'un collègue. Le Département informe l'agent concerné par courrier en motivant l'intervention par la nécessité de continuité du service.

La personne désignée provisoirement mandataire de ces accès est tenue à une obligation de réserve et n'est autorisée à ne prendre connaissance que des contenus strictement professionnels de l'agent absent.

Cette procédure exclut tout accès aux répertoires et/ou boîtes aux lettres expressément signalés par les agents comme lieu de stockage de données personnelles ou syndicales (identifiés par « Privé », « Personnel » ou « Droit syndical »).

Ces démarches permettent d'avoir accès aux données et documents nécessaires à l'activité du service, contenus par exemple sur la messagerie, les fichiers sur le réseau ou les outils collaboratifs,

à l'exclusion du répondeur vocal (puisqu'il est impossible d'en distinguer le contenu professionnel / personnel sans prendre connaissance des messages enregistrés).

2.13 Le droit syndical

L'utilisation de la messagerie, de l'intranet et d'Internet est autorisée aux organisations syndicales représentatives des personnels sous réserve du respect des règles de la présente charte.

En outre, l'utilisation de la messagerie leur est autorisée à condition :

- de ne diffuser que des informations et des données d'intérêt général et à caractère syndical,
- de s'engager à ne pas utiliser la messagerie pour des diffusions de tracts et de mots d'ordre,
- de s'abstenir de toute mise en cause personnelle et de ne pas s'adresser à un responsable sur le mode de l'interpellation.

Les organisations syndicales représentatives des personnels peuvent en revanche transmettre par ce canal des messages personnels à leurs adhérents ou à des groupes de contacts pourvu qu'il soit offert aux destinataires la possibilité de se désabonner et ne plus recevoir aucun message. Les destinataires doivent être clairement et préalablement informés de cette pratique afin de pouvoir manifester leur accord ou leur opposition à l'envoi de tout message syndical sur leur messagerie professionnelle.

Enfin, la mise en place de ces outils de communication sera effective, sous réserve de l'engagement formel des organisations syndicales représentatives des personnels auprès du Président du Conseil départemental, de respecter les dispositions précitées.

En cas de manquement à ces règles, le Président du Conseil départemental, garant du respect de l'application de la présente charte, se réserve le droit de suspendre l'accès à la messagerie, à l'intranet et l'Internet aux organisations syndicales représentatives.

Tous les fichiers présents dans un dossier « Droit syndical » bénéficient de la protection liée au droit syndical. Il en est de même de tout message qui comportera la mention « Droit syndical » en objet.

3. L'administrateur du système d'information et de communication

Le responsable des systèmes d'information, dénommé « administrateur », assure la direction de toutes les activités liées à la production, au transport et au stockage des données informatiques (Direction des systèmes d'information du Département, DSI).

Il a accès à toutes les données qui s'échangent tant sur le réseau interne qu'avec l'extérieur. Il est tenu à un strict respect du secret professionnel.

3.1 Le fonctionnement du système

L'administrateur est responsable du bon fonctionnement du système informatique :

- il dimensionne les installations et les réseaux aussi bien que les volumes des fichiers transmis et les durées de connexions ;
- il alloue à chaque utilisateur les ressources nécessaires à l'exercice de ses fonctions.

3.2 Le devoir de protection

L'administrateur est responsable de l'intégrité du système. Il met en place les outils nécessaires à protéger les réseaux de toute intrusion, pollution ou acte hostile.

3.3 La nécessité de surveillance

À la fois pour assurer un bon fonctionnement et une protection du réseau, l'administrateur doit veiller au bon usage des ressources par les utilisateurs.

3.4 L'analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau informatique sont analysés et contrôlés dans le respect de la législation applicable et notamment du RGPD.

L'administrateur vérifie que les matériels et logiciels des utilisateurs sont conformes aux besoins définis par leur hiérarchie ainsi qu'aux politiques d'urbanisation et de sécurité définies par la DSI.

Concernant leur usage, il comptabilise les temps de connexion, les sites visités, les volumes téléchargés ainsi que toutes activités relatives à l'usage des ordinateurs et serveurs, de la messagerie électronique, d'intranet et d'Internet. Il réalise des rapports périodiques non personnalisés, transmissibles par voie hiérarchique, et en particulier, un rapport trimestriel non nominatif des sites les plus visités pouvant être remis à la Direction générale des services.

En cas de détection de comportements non conformes à la charte, l'administrateur peut, après en avoir informé personnellement et par écrit l'utilisateur, réaliser une surveillance personnelle dont les résultats sont communiqués à l'autorité territoriale.

Dans tous les cas l'administrateur se garde le droit

- d'effacer, de comprimer ou d'isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques ;
- de suspendre à tout moment, et sans avertissement, l'accès aux systèmes d'information (sites Internet notamment), en cas d'inobservation des présentes règles par l'utilisateur ;
- de bloquer à tout moment, sans avertissement préalable, l'accès aux sites dont le contenu est jugé illégal ou offensant.

3.5 Le respect de la vie privée

Toute personne a droit au respect de sa vie privée et intime. Ce principe a une valeur constitutionnelle et est affirmé par l'article 9 du Code civil. La vie privée relève notamment de l'identité, de la vie familiale, sexuelle et sentimentale, de l'image, du domicile, de la santé, de la situation financière, de la religion ou encore, des convictions politiques.

L'administrateur est donc tenu à un strict respect du secret professionnel. La surveillance de l'administrateur ne s'exerce pas sur les dossiers informatiques nommés « Privé », « Personnel » ou « Droit syndical ».

Néanmoins, si dans le cadre de son activité professionnelle, l'administrateur est amené à constater des faits graves préjudiciables au Département, il pourra en informer sa hiérarchie sans divulguer le contenu des faits suspects.

3.6 Le respect de la légalité des usages des TIC

Sans préjudice de la confidentialité des correspondances, l'administrateur est tenu de dénoncer au Procureur de la République les usages illégaux (tels que pédophilie, incitation à la haine raciale, terrorisme) qu'il constaterait dans l'usage des outils TIC.

4. Les procédures conservatoires et contentieuses

En cas de présomptions sérieuses et concordantes d'infraction aux règles de la présente charte, la DSI peut, sans prise de connaissance du contenu des lecteurs, répertoires et fichiers personnels, décider des mesures conservatoires nécessaires à l'établissement de la preuve. La mise en œuvre de cette mesure s'accompagne de l'information du Directeur fonctionnel, de la Direction générale et de l'agent concerné.

Dans le cas où le Département souhaite prendre connaissance, puis faire état devant les tribunaux, du contenu de fichiers ou messages privés considérés comme abusifs, dangereux ou illicites, il devra préalablement demander par requête au tribunal compétent l'autorisation de faire procéder de manière contradictoire à leur lecture et éventuellement à leur saisie.

L'utilisateur qui ne respecterait pas les règles applicables à ses activités, notamment les règles définies dans la présente charte, encourt sur le plan administratif la suspension de tout ou partie de son droit d'accès au système d'information et de télécommunication. Un entretien formel avec le responsable hiérarchique direct et donnant lieu à compte rendu écrit constituera la première phase avant application éventuelle de sanctions disciplinaires, selon une échelle proportionnelle à la gravité de la faute commise.

L'utilisateur pourra être poursuivi pénalement ou civilement, si le Directeur général des services estime que la gravité de la faute le justifie.

5. Le lexique

- **Accountability :** ce terme désigne l'obligation pour les collectivités territoriales et les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données personnelles.
- **Administrateurs des systèmes d'information et de télécommunication** : les agents de la DSI dont la mission est de contrôler le bon fonctionnement et le bon usage des outils informatiques et des moyens de télécommunication. Ces administrateurs sont assujettis au devoir de réserve et sont tenus de respecter la confidentialité des informations auxquelles ils pourraient avoir accès dans le strict cadre de leur mission.
- **Archivage :** l'archivage de contenus électroniques est l'ensemble des actions, outils et méthodes mis en œuvre pour réunir, identifier, sélectionner, classer et conserver des contenus électroniques, sur un support sécurisé, dans le but de les exploiter et de les rendre accessibles dans le temps, que ce soit à titre de preuve (en cas d'obligations légales notamment ou de litiges) ou à titre informatif. La durée de l'archivage est fonction de la valeur du contenu et porte le plus souvent sur du moyen ou long terme.
- **Commission Nationale de l'Informatique et des Libertés** (CNIL). La Commission Nationale de l'Informatique et des Libertés (CNIL) est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.
- **Contributeur** : toute personne qui collabore à un travail collectif, notamment dans le cadre de réseaux sociaux tels que blogs, forums, tchats, …
- **Data Protection Officer (DPO) / Délégué à la Protection des Données (DPD) :** il est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données personnelles au sein de l'organisme qui l'a désigné, s'agissant de l'ensemble des traitements mis en œuvre par cet organisme. On le joint à l'adresse dpo@yvelines.fr
- **Données personnelles :** Une donnée personnelle désigne toute information se rapportant à une personne physique identifiée ou identifiable, laquelle doit conserver la maîtrise de cette information. Une personne physique peut être identifiée :
  - directement (exemple : nom et prénom) ;
  - indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

  L'identification d'une personne physique peut être réalisée :
  - à partir d'une seule donnée (exemple : nom) ;
  - à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association) :

  Par contre, des coordonnées de personnes morales, telles que les entreprises ou les collectivités territoriales (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont pas, en principe, des données personnelles.

- **Données sensibles** : Les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :
    - si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
    - si les informations sont manifestement rendues publiques par la personne concernée ;
    - si elles sont nécessaires à la sauvegarde de la vie humaine ;
    - si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;
    - si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

- **Données de santé :** le règlement européen sur la protection des données personnelles, entré en application le 25 mai 2018, définit ainsi les données de santé : « Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne. ». Ces données sont considérées sensibles. Leur traitement et leur collecte sont par principe interdits. Les données de santé ne peuvent être utilisées et communiquées à titre dérogatoire que dans des conditions strictement déterminées par la loi et dans l'intérêt des patients (assurer le suivi médical, faciliter sa prise en charge par l'assurance maladie…) ou pour les besoins de la santé publique.

- **Loi Informatique et Libertés de 1978 modifiée** : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (en vigueur).

- **Registre des activités de traitement :** Le registre des activités de traitement permet de recenser les traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles. Il permet notamment d'identifier :
    - les parties prenantes ;
    - les catégories de données traitées ;
    - ce à quoi servent ces données, qui y accède et à qui elles sont communiquées ;
    - la durée de conservation des données personnelles ;
    - la façon dont elles sont sécurisées.

- **Règlement général sur la protection des données RGPD** : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

- **Système d'information et de télécommunication** : tous les équipements, informatiques, électroniques et téléphoniques, matériels et logiciels, de la collectivité qu'ils soient interconnectés entre eux ou non.

- **TIC** : technologies de l'information et de la télécommunication. Elles regroupent les techniques de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications (fixes / mobiles) qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre l'information sous toutes les formes (texte, musique, son, image, vidéo).

- **Traitement de données personnelles** : Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement). Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions. Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation. Exemples de traitements : tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines, etc.

- **Travail à distance** : toutes formes de travail exécutées en dehors du bureau de l'agent (ex. : espace de co-working, télétravail à domicile, travail lors d'un déplacement professionnel…).

- **UE** : l'Union européenne est une association politico-économique de vingt-sept États européens (à date du 31 janvier 2020) qui s'étend sur un territoire de 4,2 millions de kilomètres carrés, peuplé de plus de 446 millions d'habitants. L'Union européenne est la deuxième puissance économique mondiale en termes de PIB nominal derrière les États-Unis.

- **URL** : de l'anglais Uniform Resource Locator, ce sigle désigne une chaîne de caractères utilisée pour identifier les ressources de l'Internet (une image, un son, un document, un site web). Une URL est également nommée « adresse web ». Exemple d'URL : http://www.yvelines.fr.

- **Utilisateur** : toute personne qui, ayant un lien de droit statutaire ou contractuel avec la collectivité (élu, agent titulaire, contractuel, vacataire, stagiaire, apprenti, étudiant, vacataire, employé d'un prestataire extérieur, partenaire), est amenée à utiliser les solutions informatiques et les moyens de télécommunication mis à sa disposition par le Département.

- **Utilisation mesurée à des fins personnelles** : cette utilisation est caractérisée par un usage raisonnable du système d'information et de télécommunication quantitativement (volume), qualitativement (nature) et chronologiquement (temps d'utilisation).

ANNEXES : le cadre juridique et les textes de référence

1. Les obligations des utilisateurs

Pour rappel, est désignée « utilisateur », toute personne qui, ayant un lien de droit statutaire ou contractuel avec la collectivité (élu, agent titulaire, contractuel, vacataire, stagiaire, apprenti, étudiant, vacataire, employé d'un prestataire extérieur, partenaire), est amenée à utiliser les solutions informatiques et les moyens de télécommunication mis à sa disposition par le Département.

1.1 Le respect des règles fixées dans la charte

Le non-respect des règles figurant dans la présente charte engage la responsabilité personnelle de l'utilisateur, agent du Département, dès lors qu'il est prouvé que la faute lui est personnellement imputable et l'expose à des sanctions disciplinaires définies par la loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale et le décret n°88-145 du 15 février 1988 pris pour l'application de l'article 136 de la loi du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale et relatif aux agents non titulaires de la fonction publique territoriale.

Tous les utilisateurs qui ne respecteraient pas les exigences de sécurité du système d'information, de confidentialité et neutralité des échanges engagent leur responsabilité personnelle et sont susceptibles de faire l'objet de poursuites pénales.

1.2 Le respect des obligations déontologiques

Les utilisateurs sont tenus au respect des obligations déontologiques issues du statut de la fonction publique territoriale à travers l'utilisation de moyens informatiques et de télécommunications mis à disposition par la collectivité sous peine de sanctions disciplinaires et pénales :

Secret professionnel

L'article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires énonce que les fonctionnaires sont tenus au secret professionnel dans le cadre des règles instituées dans le Code pénal. À ce titre, tout utilisateur doit faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont il a connaissance dans l'exercice de ses fonctions.

L'article 226-13 précise : « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. »

Le secret professionnel couvre l'ensemble des informations concernant une personne (un usager ou un collègue) et qui est parvenu à la connaissance de l'agent dans l'exercice de ses fonctions ou à l'occasion de cet exercice (informations reçues à raison de la profession, de la fonction ou de la mission). Il s'agit de tout ce que l'agent a appris, compris, constaté, vu, lu, entendu et ce qui lui a été confié dans le cadre de ses fonctions. Cela vise à protéger les intérêts matériels et moraux des particuliers.

Le secret professionnel est l'obligation faite aux agents qui y sont tenus de ne pas révéler les informations individuelles ou relatives à des intérêts privés protégés par la loi et recueillis dans l'exercice de leurs fonctions.

Les agents tenus au secret et ainsi dépositaires de renseignements relatifs ou intéressants des usagers peuvent être autorisés ou tenus par la loi de révéler les informations qu'ils détiennent (article 226-14 du Code pénal).

Les personnels professionnels de l'action sanitaire et sociale sont soumis au secret professionnel de par leur profession, leur fonction ou leur mission, conformément aux dispositions figurant dans le Code de l'action sociale et des familles et le Code de la santé publique.

Dignité

Cette obligation impose aux utilisateurs de ne pas porter atteinte à l'image de la collectivité.

Neutralité et devoir de réserve

L'obligation de neutralité impose aux utilisateurs de ne pas manifester leurs opinions politiques, philosophiques ou religieuses puis de s'exprimer, même à titre privé, avec une certaine retenue.

1.3 Le respect des règles de protection des données personnelles

Le Département des Yvelines traite de nombreuses données personnelles, que ce soit pour assurer la gestion des services publics dont il a la charge, la gestion des ressources humaines, la sécurisation des locaux, la publication de sites Internet, etc...

Respecter les règles de protection des données personnelles est une obligation légale et un gage de responsabilité pour le responsable de traitement de la collectivité. Mais, c'est aussi un facteur de transparence et de confiance à l'égard des usagers, des agents et des partenaires du Département.

Afin de respecter ces règles de protection des données et avant toute collecte de données personnelles, il est nécessaire que l'utilisateur prenne contact avec le Délégué à la protection des données (via l'adresse électronique dpo@yvelines.fr, que cet utilisateur soit chargé de la mise en œuvre du traitement de données personnelles ou qu'il agisse au nom du responsable de traitement de la collectivité.

La mise en place de tout fichier papier ou informatique comportant des données personnelles doit faire l'objet d'une instruction de la part du Délégué à la protection des données. En effet, un traitement de données personnelles n'est pas nécessairement informatisé. Les fichiers papiers sont également concernés et doivent respecter les obligations posées par les lois en matière de protection des données personnelles (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (en vigueur)) ainsi

que les recommandations des autorités en matière de protection des données personnelles. Ils doivent être protégés dans les mêmes conditions.

Les 5 grands principes des règles de protection des données personnelles qui doivent être respectés sont les suivants :

Le principe de finalité du traitement de données personnelles

La finalité d'un traitement de données personnelles est le but poursuivi par le traitement de données personnelles créé.

La finalité doit être déterminée, légitime et explicite : il est nécessaire de définir un but au traitement de données personnelles. Le but doit correspondre à l'objectif du traitement qui doit être clair et compréhensible.

La finalité doit être respectée : Cette finalité qui sera inscrite dans le registre du traitement et communiquée aux personnes concernées devra être respectée tout au long de la construction et de l'utilisation du fichier (papier ou électronique).

La détermination de la finalité permet de caractériser la pertinence des données personnelles et ainsi respecter le principe de proportionnalité et de pertinence. Enfin, elle permet également de fixer la durée de conservation des données personnelles. En effet, en fonction du but poursuivi, les données personnelles enregistrées dans le fichier (papier ou électronique) devront être conservées plus ou moins longtemps.

Le Principe de proportionnalité et de pertinence

Seules les données personnelles adéquates, pertinentes et non excessives au regard de la finalité poursuivie sont collectées.

Il faut faire attention à la collecte des données sensibles. Les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
- si les informations sont manifestement rendues publiques par la personne concernée ;
- si elles sont nécessaires à la sauvegarde de la vie humaine ;
- si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

Une attention particulière est aussi portée aux données personnelles relatives aux infractions ou condamnations. Ces données personnelles ne sont pas considérées comme des données sensibles mais elles font l'objet de la même protection.

Le principe d'une durée de conservation limitée

Les données personnelles collectées ne peuvent être conservées dans les fichiers (électroniques ou papiers) pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction

du type d'information enregistrée et de la finalité du fichier. Au-delà de la durée nécessaire à la finalité poursuivie, les données personnelles doivent être supprimées sauf pour des raisons historiques, statistiques ou scientifiques sous peine de sanction pénale (article 226-20 du Code pénal).

Les durées de conservation pourront être déterminées avec les équipes de la Direction des Archives Départementales (DAD).

Le principe de sécurité et de confidentialité

Le respect de l'intégrité et de la confidentialité des données personnelles doit être effectif afin d'empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès. Seules les personnes autorisées doivent avoir accès à ces données personnelles.

Le respect des droits des personnes concernées par les traitements

Dans tous les cas, les personnes concernées doivent être informées, lors du recueil, de l'enregistrement ou de la première communication des données :

- de l'identité et coordonnées du responsable du traitement ;
- de la finalité du traitement ;
- de la base légale du traitement ;
- du caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse ;
- des destinataires ou catégories de destinataire des données ;
- de la durée de conservation des données ;
- de leurs droits (droit d'accès et de rectification, droit d'opposition pour des motifs légitimes au traitement de ses données sauf si le traitement répond à une obligation légale, etc.) ;
- des coordonnées du Délégué à la protection des données ;
- de leur droit d'introduire une réclamation auprès de la CNIL.

Dans certains cas, les informations suivantes doivent être indiquées :

- les intérêts légitimes poursuivis par le responsable du traitement ;
- le fait que les données sont requises par la règlementation, par un contrat ou en vue de la conclusion d'un contrat ;
- l'existence d'un transfert des données vers un pays hors Union européenne (ou vers une organisation internationale), les garanties associées à ce transfert et la faculté d'accéder aux documents autorisant ce transfert (exemple : les clauses contractuelles types de la Commission européenne) ;
- l'existence d'une prise de décision automatisée ou d'un profilage, les informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que les conséquences pour la personne concernée ;
- le droit au retrait du consentement à tout moment, si la base légale du traitement est le consentement des personnes ;
- les autres droits applicables au traitement, en fonction de sa base légale : droit d'opposition et droit à la portabilité.

Informations supplémentaires à donner en cas de collecte indirecte :

- catégories de données recueillies ;
- source des données (en indiquant notamment si elles sont issues de sources accessibles au public).

Le respect de ces règles ainsi que les formalités préalables à la mise en œuvre des traitements est fait en collaboration avec le Délégué à la protection des données et le Département et ses relais dans les directions et services du Département.

En cas de manquement aux lois en matière de protection des données personnelles (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (en vigueur)) ainsi que les recommandations des autorités en matière de protection des données personnelles, la CNIL peut :

- Prononcer un rappel à l'ordre ;
- Enjoindre de mettre le traitement en conformité, y compris sous astreinte ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte ;
- Prononcer une amende administrative (Le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros).

Enfin, les atteintes au droit des personnes concernées par les traitements ainsi que les actes enfreignant les systèmes automatisés de traitements de données personnelles sont pénalement répréhensibles (article 40 et 41 de la loi n°78-17 du 6 janvier 1978 modifiée ; la section 5 du chapitre VI du titre II du livre II du code pénal ; articles R.625-10 à R.625-13 du code pénal).

1.4 La publication de documents

L'article L.312-1-2 du Code des relations entre le public et l'administration prévoit que les documents administratifs qui comportent des données personnelles ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement afin d'occulter ces mentions ou de rendre impossible l'identification des personnes qui y sont nommées.

Cette règle souffre d'exception. En effet, le Département est tenu de procéder à l'anonymisation du document, sauf en cas de disposition législative prévoyant qu'un document doit être rendu public dans son intégralité. Par exemple, constituent une disposition législative contraire au sens du deuxième alinéa de l'article L. 312-1-2 du CRPA, les dispositions des articles L. 2131-1, L. 3131-1 et L. 4141-1 du code général des collectivités territoriales en tant qu'ils prévoient une publication en intégralité des documents qu'ils énumèrent.

2. Les obligations du Département

2.1 Le respect du secret des correspondances

L'administrateur est tenu de respecter le secret des correspondances délimité par l'article 9 du Code civil et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales qui indiquent que toute personne a droit au respect de sa vie privée et de sa correspondance et la violation de ce secret des correspondances peut être sanctionnée tant sur le plan civil que pénal (article 226-15 du Code pénal).

2.2 Le contrôle de l'utilisation d'Internet et de la messagerie professionnelle

L'article 1242 alinéa 5 du Code civil prévoit la responsabilité civile de l'employeur du dommage causé par ses préposés dans les fonctions auxquelles il les a employés.
De plus, conformément à l'article 6-II de la loi n°2004-575 pour la confiance dans l'économie numérique du 21 juin 2004, tout fournisseur d'accès à Internet doit conserver les « données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services » dont il est prestataire et communiquer ces données sur réquisition judiciaire.

Ainsi, l'article L. 34-1 du Code des postes et des communications électroniques précise que ces données de connexion sont conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données et uniquement dans le seul but de permettre en tant que de besoin la mise à disposition de l'autorité judiciaire d'informations.

Conformément à la réglementation en vigueur, les données de connexion Internet à partir du réseau du Département des Yvelines sont conservées 1 an à compter du jour de l'enregistrement (article R10-13 III du Code des postes et des communications électroniques). Ces données contiennent l'identifiant de l'utilisateur, la date et l'heure de connexion, l'URL visitée et la taille des données consultées.

2.3 L'accès aux données à caractère personnel, le droit à la rectification et à l'oubli

Information sur le responsable de traitement

Le traitement relatif à la supervision du respect effectif de la présente Charte, permettant d'encadrer l'utilisation des ressources informatiques, est mis en œuvre par le Départemental des Yvelines, représenté par son Président en exercice, domicilié au 2 place André Mignot, 78000 Versailles.

Information sur la base du traitement/de la collecte de données

Les données sont collectées sur la base de l'article 6 (1) f du règlement européen 2016/679 (règlement général sur la protection des données - RGPD). En effet, ce traitement est nécessaire aux fins des intérêts légitimes poursuivis par la CNIL (fourniture des moyens numériques nécessaires à l'activité des membres et personnels de la Commission), dans le respect de sa Charte d'utilisation des ressources informatiques.

Les finalités de ce traitement sont les suivantes :

- La supervision du respect effectif de la Charte Informatique permettant d'encadrer l'utilisation des ressources informatiques ;
- La traçabilité des actions réalisées par l'ensemble des utilisateurs du système d'information permettant :
    - L'analyse des performances (données volumétriques globales ou individualisées, exploitation des différents journaux) ;
    - La résolution de dysfonctionnements techniques ;
    - La prévention et la gestion des incidents de sécurité ;
    - Le suivi de la conformité au regard des licences de logiciels.

En fonction de leurs besoins respectifs, les personnes suivantes sont destinataires de tout ou partie des données collectées :

- Les personnels en charge de la gestion des ressources informatiques et télécommunications du Département des Yvelines ;
- Les utilisateurs de ces ressources ;
- Le cas échéant, les personnels responsables de la sécurité des systèmes d'information.

Information sur les données collectées et leur origine (obligatoire en cas de collecte indirecte)

Le recueil des données est nécessaire à la gestion des ressources et moyens numériques du Département des Yvelines.

Conséquences en cas de non fourniture

Le recueil des données est nécessaire à la gestion des ressources et moyens numériques de la CNIL.

Information sur le profilage/conséquence du traitement (uniquement si cela s'applique au traitement)

Le traitement des données ne mène pas à une décision automatisée, y compris un profilage.

Information sur la durée de conservation et les éventuels destinataires

Les différents journaux (applications, équipements) sont conservés au maximum six mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques. Les données d'allocation de ressources sont conservées six mois à compter de la restitution de ces ressources par les utilisateurs concernés. Les statistiques individualisées éventuellement produites sont conservées le temps nécessaire aux opérations de vérification du respect de la Charte et à la sensibilisation des utilisateurs concernés, ou de la résolution des problèmes techniques rencontrés.

Information sur les éventuels transferts de données hors UE (uniquement si transferts hors UE)

Les données ne font pas l'objet d'un transfert de données en dehors de l'Union Européenne.

Comment les agents peuvent-ils exercer leurs droits sur les données qui les concernent ?

Les agents peuvent accéder et obtenir copie des données les concernant, s'opposer au traitement de leurs données, les faire rectifier ou les faire effacer. Ils disposent également d'un droit à la limitation du traitement de leurs données.

Le Département a nommé auprès de la CNIL une Déléguée à la protection des données, que les agents peuvent contacter à l'adresse suivante afin d'exercer leurs droits ou pour toutes questions relatives à la protection de leurs données :

- Par courrier :

  Déléguée à la protection des données (DPO)
  Hôtel du Département
  2, place André Mignot, 78012 Versailles Cedex

- Par email/courriel : dpo@yvelines.fr

Information sur la possibilité d'introduire une requête auprès de la CNIL

Si après avoir contacté le DPO, les agents estiment que leurs droits ne sont pas respectés ou que le dispositif de contrôle d'accès n'est pas conforme aux règles de protection des données, ils peuvent adresser une réclamation en ligne à la CNIL ou par voie postale.

Ils consulteront le site www.cnil.fr pour obtenir davantage d'informations sur leurs droits.

3. Recommandations de la CNIL (mot de passe)

LES MOTS DE PASSE N'ONT PLUS DE SECRET POUR VOUS !

****

UN MOT DE PASSE EN BÉTON |

Un bon mot de passe doit contenir 12 caractères, d'au moins 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux. Il peut être plus court si votre compte est équipé de sécurités complémentaires !

****

IL NE DIT RIEN SUR VOUS |

Personne ne doit deviner votre mot de passe à partir du nom de votre chien ou de votre film préféré. Idem pour le code de votre smartphone : préférez un nombre aléatoire à une année.

****

UN COMPTE, UN MOT DE PASSE |

Pour éviter les piratages en cascade, chacun de vos comptes en ligne qui présente un caractère sensible (banque, messagerie, réseau social, etc.) doit être verrouillé avec un mot de passe propre et unique.

****

NE JAMAIS L'ABANDONNER EN PLEINE NATURE |

Les post-it, les fichiers texte, votre smartphone ou votre boite de messagerie ne sont pas conçus pour sécuriser le stockage de vos mots de passe. Pensez aussi à ne jamais les enregistrer dans le navigateur d'un ordinateur partagé.

****

DEUX CADENAS VALENT MIEUX QU'UN |

Quand le service vous le propose, activez la double authentification. Si quelqu'un se connecte à votre compte depuis un terminal inconnu, le site vous prévient par SMS/e-mail. Libre à vous d'autoriser ou de refuser l'accès !

****

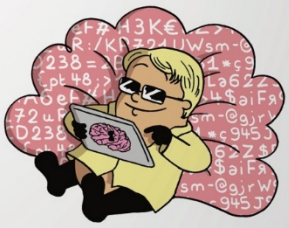
LES RETENIR SANS LES ÉCRIRE

... EN TRAVAILLANT VOS NEURONES |

Mémorisez une phrase puis utilisez la première lettre de chaque mot pour créer votre mot de passe. La phrase doit contenir des chiffres et des caractères spéciaux !

... EN REPOSANT VOS MÉNINGES |

Utilisez un gestionnaire de mots de passe ou un trousseau d'accès chiffré pour stocker vos mots de passe en toute sécurité. Vous n'aurez à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes !



****

PLUS DE CONSEILS SUR WWW.CNIL.FR

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Illustrations : Martin Vidberg

4. Les adresses de contact

Les agents sont invités à écrire :

- À rgpd@yvelines.fr pour toute question relative :
    - à l'instruction de la mise en place d'un traitement ;
    - à l'utilisation de données personnelles ou sensibles.
- À dpo@yvelines.fr pour toute question relative à leurs droits (droit d'accès, rectification, opposition, effacement, à la portabilité, à la limitation de leurs données).
- À rssi@yvelines.fr pour toute question relative à la sécurité des données ou à celle du système d'information.
- À drhdemande@yvelines.fr pour toute question relative aux droits et devoirs des agents du Département.