Département des Hautes-Pyrénées

Règlement des usages du Système d'Information départemental

V 2.0.2

SOMMAIRE

Table des matières

1 Préambule

La Collectivité, **le Département des Hautes Pyrénées (CD65),** met à disposition un ensemble de moyens informatiques et de communication nécessaires à l'exercice des missions de ses agents.

L'utilisation de tout système informatique relié à un réseau suppose la mise en place de règles dont le rôle est d'assurer la sécurité des données et les performances des traitements, dans le respect de l'organisation interne et des législations applicables.

Le raccordement d'un système informatique à un réseau public tel qu'Internet rend le respect de ces règles impératif.

La préservation et le bon usage du Système d'Information départemental est primordial pour la continuité d'exercice des missions du CD65.

1.1 Objet du règlement

Ce règlement a pour but de rassembler les consignes à appliquer et les conseils de bons usages.

Il définit les conditions d'accès et les règles d'utilisation des moyens informatiques.

Il a également pour objet de sensibiliser les Utilisateurs aux risques d'utilisation de ces moyens. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un Utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile ou pénale ainsi que celle de la Collectivité.

1.2 Champ d'application

Le règlement concerne TOUS les agents de la Collectivité ainsi que l'ensemble des personnes habilitées par l'autorité territoriale, qui utilisent les moyens informatiques et de communication (organismes associés et services extérieurs, élus, partenaires, élèves stagiaires, prestataires, etc.).

Le terme « Utilisateur » sera employé de manière générique dans l'ensemble du règlement. Celui-ci s'applique à tout Utilisateur dans l'exercice de ses missions.

On entend par :

- Collectivité : Structure administrative qui assiste les élus du conseil départemental dans la réalisation des missions qui sont à leur charge.
- Organismes associés : Structure ayant une convention de mise à disposition de moyens la liant à la collectivité.
- Prestataires : personne physique ou morale, y compris un organisme public, qui offre des services à la Collectivité.

1.3 Glossaire

Administrateur : Un administrateur est un Utilisateur qui dispose de privilèges (ou droits) étendus sur le SI et en supporte la responsabilité inhérente. Pour cela il est doté de compétences reconnues dans les domaines, réseaux, systèmes, téléphonie, ...
L'administrateur applicatif agit sur les paramétrages et le droit des utilisateurs. L'administrateur système et infrastructure agit sur les équipements informatiques ou sur les bases de données.
Les prestataires ou stagiaires peuvent être compris dans cette catégorie.

BYOD : Acronyme de « Bring Your Own Device » qui signifie « Apportez votre propre matériel ». Consiste à intégrer les appareils personnels des Utilisateurs dans le système d'information au moyen d'une solution de gestion des terminaux mobiles.

Chiffrement : Opération consistant à transformer un message en clair en un message chiffré compréhensible seulement par la personne disposant de la clé de déchiffrement.

Cloud public : Espace de stockage ou application, disponible au grand public par Internet, proposé par un fournisseur de service.

Compression : Opération visant à réduire la taille d'un fichier ou d'un groupe de fichiers. Elle s'effectue au moyen d'un logiciel de compression (7Zip, WinZip, WinRar…) dont le rôle est de coder les informations numériques sous une forme plus compacte.

Compromission : Un élément du système d'information est dit compromis lorsque son contrôle a été perdu, qu'il a subi des dégâts ou que l'information supportée a été révélée en contradiction avec son niveau de confidentialité.

Donnée à Caractère Personnel : Toute information relative à une personne physique susceptible de l'identifier, directement ou indirectement (article 4 du RGPD). Exemples : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, …

Équipements nomades : Matériels et logiciels permettant à l'Utilisateur d'exercer son activité en dehors de son lieu de travail habituel.

L'e-réputation : Il s'agit de la réputation d'une entité (marque, personne morale ou physique, particulier, personne publique) réelle (représentée par un nom ou un pseudonyme) ou fictive, l'opinion commune la concernant (informations, avis, échanges, commentaires, rumeurs…) sur les réseaux.

Filtrage (ou proxy filtrant) : Logiciel permettant de contrôler l'accès à Internet en fonction de certains paramètres (catégories, mots-clés, adresses IP…).

Logiciel malveillant (Malware) : Catégorie de programmes qui ont pour objectif de nuire, dont font partie les virus, les vers, les chevaux de Troie, les bombes logiques, les logiciels de rançon, les logiciels de publicité intempestive. Un logiciel malveillant peut combiner plusieurs attributs parmi ceux décrits.

Message indésirable (ou SPAM) : Messages non sollicités reçus par e-mail. Ces messages peuvent être, soit commercial, soit une escroquerie, soit une attaque informatique sous forme de pièce jointe ou de manipulation.

Moyens d'authentification : Ce sont les moyens que l'utilisateur utilise pour prouver son identité. On les catégorise dans trois groupes :

- Ce que je sais : Un mot de passe
- Ce que je suis : Une empreinte digitale, la biométrie en général
- Ce que je possède : Un smartphone enrôlé, une carte à puce, un jeton d'authentification.

Moyens informatiques : Ensemble de ressources informatiques, matérielles et logicielles. Ils comprennent : les ordinateurs et leurs périphériques (écran, clavier, souris, scanner, imprimante, ...), les serveurs, les applications métiers, les systèmes d'exploitation et les logiciels installés, les réseaux informatiques, les outils et services de messagerie électronique, des outils et services d'accès aux réseaux informatiques internes et externes, des outils et services de téléphonie.

Poste de travail : Ensemble de matériels et logiciels mis à disposition de l'Utilisateur dans le cadre de son activité.
Le poste de travail peut comprendre :

- L'ordinateur : unité centrale, écran, clavier, souris, casque
- Les équipements nomades (voir définition)
- Les moyens d'impression

Rétention : Se dit du temps maximum de conservation des données lorsqu'une sauvegarde est mise en place. Elle va de quelques heures à plusieurs années en fonction des données.

Sécurité des données : Consiste à protéger les informations contre l'indisponibilité, l'altération des données (intégrité) ou perte de confidentialité.

Système d'information : Comprend l'ensemble des moyens informatiques, les processus, le personnel et l'organisation, permettant le traitement des données de la Collectivité.

Traitement : « Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...) » (article 6 du RGPD).

Virus : Une caractéristique de certains logiciels malveillants. Ce terme est souvent utilisé par abus de langage pour désigner tous les logiciels malveillants. Un virus est défini par une capacité d'autoreproduction et une résistance à la suppression.

1.4 Principaux textes réglementaires applicables

Les principaux textes réglementaires applicables sont les suivants :

- Le Code pénal : et notamment les articles 323-1 à 323-8 et 226-16 à 226-24 ;
- la Loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- Le Règlement Général européen sur la Protection des Données.

- La faute disciplinaire
  - Loi 83-634 du 13 juillet 1983 art.29
  - Loi 84-16 du 11 janvier 1984
  - Décret n° 84-961 du 25 octobre 1984

2 Les interlocuteurs

Direction des ressources humaines

La direction des ressources humaines est garante avec la direction métier de l'adéquation des moyens informatiques (ordinateur, logiciels, accessoires, …) mis à la disposition de l'Utilisateur avec la mission à réaliser via les fiches de nouvel arrivant, mouvement, départ.

Le directeur des ressources humaines garantit à la direction générale les éléments de gestion individuelle des agents concourant à la mise en application effective du présent règlement.

Direction des Systèmes d'Informations et du Numérique

La DSIN a pour vocation de mettre à la disposition des Utilisateurs un ensemble de moyens techniques permettant d'utiliser au mieux les nouvelles technologies de traitement de l'information.

Ils veillent à ce que ce système d'information soit cohérent, pérenne, sécurisé, disponible et évolutif. Le responsable de ces entités répond à la direction générale des éléments techniques concourant à la mise en application du présent règlement. Les services informatiques participent aux évolutions du présent règlement.

Le support informatique

Le support informatique, spécialiste de l'informatique et de la téléphonie, a en charge le support à l'Utilisateur, les dépannages, qu'il s'agisse de problèmes de matériels ou de logiciels. Il peut également apporter conseil, assistance et formation. Le point d'entrée du support informatique est matérialisé par l'équipe « Assistance Utilisateur ».

L'Utilisateur prend contact avec le support informatique lorsqu'il fait face à un problème, un incident ou une demande particulière. Ceci garantit qu'il soit répertorié, tracé et que les actions de correction ou d'évolution seront engagées.

Le support informatique, le cas échéant relayé par un autre administrateur des services informatiques, peut utiliser un logiciel de contrôle à distance. L'utilisation de cet outil requiert l'autorisation de l'Utilisateur concerné. Lors de la prise en main, l'Utilisateur doit valider qu'il autorise ou non l'accès.

Les administrateurs fonctionnels

Les administrateurs fonctionnels des applications sont en charge de l'attribution des droits aux Utilisateurs quand cette opération n'est pas effectuée au sein de la DSIN. L'attribution des droits doit être réalisée de manière cohérente avec les missions qui sont confiées aux Utilisateurs.

La hiérarchie

Avant toute demande de moyens informatiques, l'Utilisateur fait valider par sa hiérarchie l'adéquation entre les exigences de sa mission et les moyens sollicités.

Le Délégué à la protection des données (DPO)

Au sein de la collectivité le délégué à la protection des données veille, de manière indépendante, au respect du cadre légal en matière de protection des données à caractère personnel recueillies et traitées par les services du Département. Il développe

une politique de protection des données, en lien étroit avec le responsable des traitements, en direction des services et des usagers du Département dont il garantit les droits en la matière.

Le responsable sécurité des systèmes d'information (RSSI)

Le **RSSI** est chargé de la définition et de la mise en œuvre de la politique de sécurité de la collectivité. Il possède en outre un rôle stratégique d'information, de conseil et d'alerte de la direction générale sur les risques en matière de sécurité informatique.

Le responsable des traitements

Le responsable d'un traitement de données à caractère personnel est la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement.

Les utilisateurs

Toutes personnes physiques ou morales ayant accès au Système d'Information (SI) de la collectivité.

3 Responsabilité des Utilisateurs

L'Utilisateur est un des acteurs de la sécurité. Ses droits s'accompagnent de devoirs. Les règles suivantes s'appliquent à l'ensemble des documents, créés, consultés, modifiés et transmis par l'Utilisateur. (Voir 1.2 Champ d'application)

Les sociétés sous-traitantes s'engagent à faire respecter le présent règlement à leurs salariés et leurs sous-traitants. Il sera systématiquement et de manière contractuelle porté à leur connaissance pour mise en œuvre.

3.1 Protection des données

L'Utilisateur a l'obligation de protéger les informations et documents qu'il manipule ainsi que ceux disponibles sur le système d'information de la Collectivité auxquels il a accès.

3.1.1 Disponibilité

L'Utilisateur s'engage à ne pas interrompre ou à contribuer à l'interruption de l'accès aux données. L'Utilisateur stocke les données qu'il exploite, qu'il crée ou qu'il transforme sur les espaces réseau dédiés.

L'Utilisateur peut stocker des données sur son poste de travail, il en assume la responsabilité et met en œuvre les moyens nécessaires afin de garantir la continuité du service. En cas de perte, ces données ne pourront être restaurées par la DSIN.

Seules les données stockées sur les espaces réseau accessibles par l'Utilisateur sont sauvegardées et peuvent être restaurées durant la période de rétention.

3.1.2 Intégrité

L'Utilisateur doit s'assurer que la modification ou destruction de fichiers et documents ne porte aucun préjudice à la Collectivité.

3.1.3 Confidentialité

L'Utilisateur a une obligation de discrétion et de confidentialité envers les données internes de la Collectivité.

L'Utilisateur évitera de conserver des documents confidentiels ou sensibles sur un ordinateur portable ou, mettra en œuvre les mesures de protection appropriées proposées par la DSIN pour préserver la confidentialité et l'intégrité des informations stockées.

L'Utilisateur libère son bureau de tout document (notes, post-it, etc.) pouvant contenir des informations sensibles en dehors de sa séance de travail.
L'Utilisateur veille particulièrement à protéger les informations confidentielles, sensibles, ou à caractère personnel des regards externes lors d'une session de travail et quand il quitte momentanément son poste de travail, ceci afin de réduire le risque de vol, de fraude, de fuite de données.

L'Utilisateur s'assure que les supports informatiques ou tout autre support contenant des informations ou des données confidentielles sont conservés en lieu sûr.
L'Utilisateur est encouragé à réduire son utilisation de papier en numérisant les documents, pour en faciliter la recherche, et potentiellement réduire le risque de vols.

Le chapitre 9 Données à caractère personnel est consacré aux lois et règlementations sur la protection des données personnelles.

3.2 Éthique et Déontologie

L'Utilisateur doit respecter les règles d'éthique et de déontologie liées à sa fonction et ne pas abuser des privilèges dont il dispose pour en tirer un profit personnel.

3.3 E-Réputation

Les Utilisateurs de la Collectivité bénéficient comme tous les citoyens d'un droit d'expression. En application du principe de loyauté et du devoir de réserve du fonctionnaire, un agent ne doit pas compromettre la réputation de la Collectivité.

Cette obligation va au-delà des locaux et des horaires de travail. Elle est permanente et s'applique de fait sur Internet et en particulier sur l'ensemble des réseaux sociaux, mais aussi aux échanges oraux.

3.4 Devoir de signalement

Par ailleurs, l'Utilisateur est tenu d'avertir le support informatique par l'intermédiaire du pôle assistance de :

- Toute violation ou tentative de violation suspectée de ses accès,
- Toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation,
- Tout dysfonctionnement logique et technique constaté,
- Toutes anomalies découvertes (intrusion dans le réseau, vol/perte de matériel, etc.),

- Et de manière générale, de tout comportement anormal du poste de travail.

Il signale au Délégué à la Protection des Données de la Collectivité toute atteinte aux données à caractère personnel qu'il constate.

4 Droits d'accès et Mots de passe

L'accès au système d'information est soumis à autorisation préalable, et à l'acceptation entière des termes du présent règlement. L'accès aux moyens informatiques est contrôlé par les services informatiques qui délivrent les moyens d'authentification propres à chaque Utilisateur (identifiant et mot de passe).

Des droits sont définis au sein de chaque application en lien avec la fonction de l'Utilisateur.
Ils sont définis en respectant le principe de moindres privilèges. Cela implique de restreindre les droits d'accès afin que l'utilisateur ne dispose que des droits strictement nécessaires à l'exercice de ses missions.

Les accès sont personnels, confidentiels et incessibles. Ils cessent avec la disparition des raisons qui ont motivé leur attribution. L'accès est limité aux activités professionnelles définies dans le cadre de la mission de l'Utilisateur.

Il convient de rappeler que les visiteurs / prestataires / partenaires ne peuvent pas avoir accès au système d'information de la Collectivité sans l'accord préalable des services informatiques.

L'Utilisateur possède un « compte utilisateur », caractérisé par un identifiant et accompagné d'un mot de passe, qui lui est propre. L'usage de comptes non nominatifs et partagés entre plusieurs Utilisateurs est prohibé. Cela est valable également pour les Administrateurs techniques.

Toutes les connexions réalisées à l'aide de ces codes d'authentification engagent la responsabilité de son propriétaire. En conséquence de quoi, il convient de respecter les règles de sécurité suivantes :

- L'Utilisateur devra modifier le mot de passe confié par les services informatiques lors de sa première connexion.
- L'Utilisateur devra choisir un mot de passe respectant les règles de complexité définies dans ce chapitre.
- L'Utilisateur ne doit pas stocker son mot de passe ni sur support papier ou électronique non chiffré.
- L'Utilisateur ne doit jamais confier son identifiant/mot de passe, même à son collègue, son supérieur hiérarchique ou un technicien du support informatique.
- L'Utilisateur ne doit jamais demander l'identifiant/mot de passe d'un autre utilisateur.
- L'Utilisateur ne doit pas tenter d'utiliser les moyens d'authentification autres que les siens ou masquer sa véritable identité.
- Les membres du service informatique ne doivent pas demander le mot de passe d'un utilisateur, mais doivent l'inviter à le saisir.

- Dans le cas d'une intervention imposant au service informatique une connexion en lieu et place de l'utilisateur, un mot de passe temporaire sera utilisé par les techniciens avec l'autorisation expresse de l'utilisateur.

- Le mot de passe professionnel ne doit pas être en lien avec la vie personnelle de l'Utilisateur (nom d'un membre de la famille ou d'un animal, dates de naissance, activités pratiquées).

- Il est fortement recommandé d'avoir un mot de passe professionnel différent de ses mots de passe privés.

Le mot de passe Utilisateur doit obligatoirement suivre les règles suivantes :

- Avoir une longueur minimale de 8 caractères.

- Comporter un mélange de minuscules, majuscules, chiffres et caractères spéciaux.

- Etre renouvelé à une fréquence de 6 mois.

Les moyens techniques automatisés nécessaires seront mis en œuvre par la DSIN afin d'obliger le respect de ces règles et du changement de mot de passe. Ceci sera progressivement déployé à l'ensemble de la collectivité.

Lors du départ d'un Utilisateur ou d'un changement de fonction, les droits d'accès attribués seront supprimés ou modifiés selon la procédure en vigueur.

5 Sauvegarde

La Collectivité sécurise les données manipulées ou créées par l'Utilisateur, grâce à des sauvegardes automatisées. L'Utilisateur a en charge de déposer les documents professionnels sur les espaces de stockage réseau dédiés. La période de rétention des données est d'une durée de 20 jours.

Les données non-professionnelles ou sauvegardées sur tous autres supports que les espaces réseau sont exclues du processus de sauvegarde automatisé de la DSIN.

En cas d'incident l'Utilisateur prend contact avec le support informatique, pour enclencher une procédure de restauration dans le délai de rétention.

La Collectivité dégage toute responsabilité en cas de perte de données privées de l'Utilisateur sur son SI.

6 Poste de travail

Les matériels sont mis à disposition par les services informatiques en fonction des besoins et des impératifs de mission. Ils demeurent la propriété de la Collectivité.

L'Utilisateur s'engage à prendre soin du matériel confié. Il le restitue selon les procédures en vigueur en cas de mobilité interne ou de départ.

L'Utilisateur du réseau informatique s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- D'altérer, voir interrompre, même temporairement, le fonctionnement normal du réseau ou de l'un des systèmes connectés au réseau.

- D'accéder à des informations privées d'autres Utilisateurs du réseau, sans leur autorisation expresse.

- De modifier ou de détruire des informations communes sur un des systèmes connectés au réseau.

- De modifier le fonctionnement, le paramétrage et les caractéristiques de son poste de travail.

L'Utilisateur ne doit pas connecter au réseau ou à son poste de travail d'autres équipements que ceux fournis par les services informatiques (exemple : clé USB, clavier, etc…). Si besoin, l'Utilisateur formule une demande de dérogation auprès des services informatiques et s'assure que l'équipement est exempt de logiciel malveillant en utilisant un scan antiviral.

L'Utilisateur est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements.

7 Nomadisme

7.1 Définition

On entend par « équipements nomades » les moyens informatiques mobiles.

Cela comprend :

- Les ordinateurs portables,

- Les téléphones mobiles dit « simples » aux fonctionnalités limitées,

- Les téléphones mobiles « intelligents », également appelés smartphones, sur lesquels il est possible d'installer des applications pour étendre les fonctionnalités,

- Les tablettes, équivalents grands formats des téléphones intelligents,

- Les supports de stockage de fichiers (Disque dur externe, clé USB),

- Les moyens d'authentification physique (badge, carte à puce, application d'authentification sur le smartphone de l'Utilisateur),

- Les objets connectés.

Ces moyens informatiques sont délivrés par les services informatiques de la Collectivité. Les badges de pointages sont eux distribués par la direction des ressources humaines.

Ils font partie du poste de travail de l'Utilisateur et sont soumis aux règles du chapitre 6 Poste de travail, quel que soit l'endroit où ces équipements sont utilisés.

A noter que le nomadisme inclut également tous les documents professionnels sur supports papier.

7.2 Règles générales

Ces règles s'appliquent lors de déplacements, d'astreintes, de télétravail.

L'Utilisateur porte les responsabilités définies au chapitre 3, dans le cadre de l'utilisation nomade.

L'Utilisateur doit conserver les équipements nomades en lieu sûr. Lors de ses déplacements, il veille à ne pas les laisser apparents dans un véhicule, ou tout autre lieu.

L'utilisation des équipements délivrés par la Collectivité doit être avant tout professionnelle, l'usage à titre privé reste exceptionnel.

L'Utilisateur, lors d'une connexion à la Collectivité, via l'extranet, se conforme aux règles d'accès depuis les locaux.

L'Utilisateur évite dans la mesure du possible de se connecter avec un équipement nomade via un réseau inconnu ou partagé tel que celui des aéroports, gares, trains, restaurants ou fast-foods, et dont la sécurisation n'est pas garantie. L'utilisateur doté d'un smartphone professionnel (connexion 3G / 4G) privilégiera le partage de connexion depuis ce périphérique.

En cas de perte ou de vol d'un équipement nomade, l'Utilisateur prévient le plus rapidement possible le support informatique. La désactivation des accès doit se faire au plus vite.
Il effectue une déclaration auprès du commissariat de police le plus proche. Il adresse une copie de cette déclaration au Service Contentieux / Assurance de la Collectivité ainsi qu'au responsable de la sécurité du système d'information.

Toute fausse déclaration volontaire est passible de sanctions disciplinaires ou pénales.

7.3 Ordinateurs portables

7.3.1 Ordinateurs portables de prêt

Des ordinateurs portables de prêts peuvent être mis à disposition selon les besoins de l'Utilisateur.

L'Utilisateur veille à supprimer les fichiers enregistrés sur le disque dur des portables lors de son usage avant de retourner le matériel au support informatique.
À défaut, le support informatique supprime les données stockées sur les ordinateurs avant de proposer ce matériel à nouveau.

7.4 Téléphones portables

Le support informatique fournit des téléphones portables aux Utilisateurs habilités lorsque cela est nécessaire à leur fonction.

Ces téléphones sont intégrés dans l'outil de gestion des terminaux mobiles, ou « MDM », de la collectivité.

Lors de la perte ou du vol d'un téléphone portable, l'abonnement téléphonique de l'Utilisateur doit être suspendu.

La capture d'images, de vidéos ou de fichiers audio n'est pas recommandée en dehors du cadre professionnel. La responsabilité de l'Utilisateur est engagée dans cette situation.

L'Utilisateur doit se servir du téléphone portable dans des conditions de discrétion garantissant la confidentialité des échanges (ne pas échanger d'informations confidentielles dans un lieu public).

L'Utilisateur doit garder confidentiel le code PIN de sa carte SIM, ainsi que le code déverrouillage de son équipement.

L'utilisateur s'engage à modifier les paramètres par défaut de l'appareil, c'est-à-dire :

- Le code PIN et le schéma de verrouillage,
- Le verrouillage automatique.

L'Utilisateur doit verrouiller son téléphone dès qu'il ne s'en sert plus. Il est recommandé d'activer le mécanisme de verrouillage automatique pour qu'il s'actionne au bout de 60 secondes d'inactivité.

Lorsque le téléphone est équipé de Bluetooth, il est recommandé de désactiver cette fonctionnalité entre chaque utilisation, de manière à diminuer les risques d'une attaque par ce biais. Si l'Utilisateur utilise le Bluetooth pour se connecter à une voiture partagée (location, autopartage, etc.), il doit s'assurer de supprimer les données résiduelles sur le véhicule comme l'historique des appels ou le carnet de contact avant de rendre le véhicule.

7.5 Smartphones et tablettes

L'Utilisateur utilise son smartphone ou sa tablette, dans le même cadre que celui des téléphones portables.
Ces règles sont étendues aux services proposés par les applications mobiles. Leur utilisation engage la responsabilité de l'Utilisateur.

8 Logiciels

Seules les personnes habilitées sont autorisées à installer des logiciels sur les postes de travail. L'Utilisateur s'engage à ne pas télécharger ni installer de logiciels gratuits disponibles sur Internet : cela peut constituer une atteinte à la sécurité du système d'information.

L'Utilisateur réduit au strict nécessaire l'utilisation de code Visual Basic ou de Macro de la suite Office.

Si l'Utilisateur a besoin d'un logiciel propriétaire ou libre, il en fait la demande au support utilisateur de la DSIN.

L'Utilisateur s'engage à ne pas utiliser, ni diffuser de logiciels piratés, ce qui constitue un délit passible d'amende et d'emprisonnement. À noter que sa diffusion correspond à du recel.

L'Utilisateur ne doit pas tenter de désactiver ou désinstaller tout dispositif de sécurité (antivirus, pare-feu, etc.) mis en place par les services informatiques.

L'Utilisateur s'engage à ne pas installer, ni utiliser d'outils permettant d'effectuer des attaques informatiques (scan réseau, programmes malveillants, surveillance).
Seuls, les administrateurs techniques et personnes habilitées peuvent faire l'objet d'exceptions décrites dans une procédure validée par la Direction.

9 Données à caractère personnel

La définition des données à caractère personnel est précisée au §1.3 du présent règlement.

Les données à caractère personnel peuvent exister sous plusieurs formes :

- Numériques : c'est en général à ces données là qu'on pense en premier ;
- Physiques : les données sous format papier (par exemple des listes de personnes) sont également des données à caractère personnel soumises à la règlementation sur la protection des données à caractère personnel et au présent règlement.

9.1 Les règles à respecter par les agents / utilisateurs

Dans le cadre d'une mission de service public, les Utilisateurs manipulent des données à caractère personnel concernant les administrés, les partenaires, les agents, …. On entend par données à caractère personnel, toute information relative à une personne physique susceptible de l'identifier, directement ou indirectement.

Le Règlement Général européen pour la Protection des Données (dit RGPD) et la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ont pour objet de protéger les personnes contre les dangers d'une utilisation abusive de fichiers contenant des données à caractère personnel. Ils définissent les conditions dans lesquelles les données à caractère personnel peuvent être recueillies et faire l'objet d'un traitement.

La Collectivité a désigné un délégué à la protection des données à caractère personnel (Data Protection Officer, DPO), celui-ci est obligatoirement consulté par le(s) responsable(s) des traitements préalablement à leur création. Ils recensent dans un registre les traitements de données à caractère personnel de la Collectivité dès leur mise en œuvre. Le DPO de la collectivité peut être contacté à l'adresse de messagerie delegue.donnees@ha-py.fr.

Le DPO veille au respect de l'exercice des droits des personnes et des usages de leurs informations.
En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le DPO. Elles pourront saisir un tribunal pour faire valoir l'absence de respects des droits sur ces données (article 21 du RGPD)

Pour rappel la liste des droits des personnes concernées par les données à caractère personnel :

- Droit à l'information
- Droit d'accès
- Droit de rectification
- Droit d'effacement
- Obligation de notification de ses droits et sur les traitements des données personnelles

- Droit à la portabilité des données
- Droit d'opposition
- Droit à ne pas être profilé (article 22 RGPD)

De ce fait, chaque Utilisateur se doit de n'accéder qu'aux informations et documents, qui lui sont propres, publics ou partagés.

Si, dans l'exercice de ses missions il manipule des données à caractère personnel, il est tenu :

- D'observer un devoir de discrétion et de confidentialité de ces données, tant dans le cadre professionnel que dans sa vie privée.

- De ne collecter que les données nécessaires au traitement.

- D'être transparent avec l'administré sur l'usage qui en est fait, et rappeler le soin apporté aux données.

- De transmettre au responsable de traitements, dans les meilleurs délais, les demandes d'activation de ses droits par la personne.

- De signaler au responsable de traitements toute atteinte aux données à caractère personnel constatée.

Si dans l'accomplissement de son travail, un Utilisateur est amené à constituer des fichiers contenant des données à caractère personnel, il doit se référer au DPO de la Collectivité qui prendra les mesures associées.

9.2 Engagements des agents / utilisateurs

Chaque utilisateur étant amené à accéder à des données à caractère personnel, déclare reconnaître la confidentialité des dites données.

Par conséquent, chaque utilisateur s'engage à prendre toutes précautions conformes aux usages et à l'état de l'art (articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016) dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Chaque utilisateur s'engage en particulier à :

- Ne pas utiliser les données auxquelles il/elle peut accéder à des fins autres que celles prévues par ses 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 ses fonctions ;

- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses 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 ;

- S'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;

- En cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée des fonctions, de l'utilisateur demeurera effectif, sans limitation de durée après la cessation de ses fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

Chaque utilisateur est informé que toute violation du présent engagement l'expose à des sanctions disciplinaires et pénales conformément à la règlementation en vigueur, précisées au §20 du présent règlement.

9.3 Engagements de la collectivité vis-à-vis de ses agents / utilisateurs

Dans le cadre de l'exercice de ses missions, la collectivité met en œuvre des traitements de données à caractère personnel nécessitant une collecte de données de ses agents/utilisateurs.

Le Département en tant qu'employeur prend des engagements pour garantir la protection des données à caractère personnel de ses agents.

L'objectif de ce paragraphe est d'informer les agents du Département concernant les traitements dont ils font l'objet par leur employeur, ainsi que des mesures de sécurité mises en œuvre et des modalités d'exercice de leurs droits.

9.3.1 Traitements de données de ses agents mise en œuvre par le Département

Ces traitements sont les suivants :

- Dans le domaine des Ressources Humaines :
  - Carrière et paye ;
  - Temps de travail et absences ;
  - Formations et compétences ;
  - Recrutements ;
  - Dotations individuelles ;
  - Frais de déplacements ;
  - Elections professionnelles ;
  - Gestion de l'action sociale pour les agents
  - Médecine du travail (y compris gestion des absences médicales et psychologue du travail) ;
  - Gestion des indemnités chômage ;
  - Gestion des dossiers agents ;
  - Risques professionnels et document unique ;

- Budget et masse salariale ;
- Déclaration Sociale Nominative ;
- Communication et affichage RH ;
- Echanges de données avec les organisations syndicales ;
- Gestion des postes et effectifs ;

- Dans le domaine du Système d'Information :
  - Attribution et gestion des droits d'accès aux ressources informatiques de la collectivité
  - Gestion de la sécurité du SI par la traçabilité des actions (Cf. §11.1 et 18 du présent règlement)
  - Traçabilité de la navigation internet ;
  - Téléphonie
- Dans le domaine de la sécurité des bâtiments :
  - Contrôle d'accès aux bâtiments ;
  - Vidéosurveillance ;
- Dans le domaine de l'information interne :
  - Organigrammes et annuaires ;
  - Intranet (commentaires des agents) et communication interne

9.3.2 Description des traitements

Chaque traitement fait l'objet d'une fiche du registre des traitements conformément à l'article 30 du RGPD. Cette fiche vise à décrire précisément le traitement et à en définir les modalités de sécurité adaptées.

Le registre des traitements est tenu par le délégué à la protection des données du Département.

Le responsable des traitements au sens du RGPD est le Président du Conseil Départemental des Hautes-Pyrénées. Chaque traitement est mis en œuvre sous la responsabilité des directions.

En annexe du présent règlement sont précisées pour chaque traitement les informations suivantes :

- Les finalités – à quoi sert le traitement de données ;
- La licéité – quel est le fondement juridique du traitement ;
- Les catégories de données collectées ;
- La durée de conservation de ces données.

Ces informations sont présentées en annexe du règlement pour en faciliter la mise à jour régulière en fonction des évolutions des traitements, sans nécessiter la revalidation complète du présent règlement. En cas de modification, une information sera présentée au Comité Technique.

9.3.3 Mesures de sécurité visant à la protection des données à caractère personnel

Chaque traitement peut faire l'objet de mesures de sécurité spécifiques.

Le Département met également en œuvre une politique globale de sécurité du Système d'Information, ces mesures s'appliquant à l'ensemble des traitements de données à caractère personnel :

- Pour les données numériques :
  - La confidentialité est assurée par un contrôle d'accès. Chaque utilisateur, pour accéder à ces données doit s'identifier et s'authentifier avec son compte personnel et son mot de passe confidentiel ;
  - La sauvegarde des données stockées dans les logiciels et sur le réseau est également réalisée pour assurer l'intégrité des données, garantir une continuité et une récupération en cas d'incident ;
  - Une protection globale du réseau et des postes informatiques est également mise en œuvre avec plusieurs outils techniques : mise à jour des logiciels et des matériels, système anti-intrusion, antivirus et antispam.
- Pour les données sur support physique / papier :
  - Un contrôle d'accès aux bâtiments est également une mesure de sécurité qui vise à garantir la confidentialité pour l'accès aux locaux. Seules les personnes habilitées doivent pouvoir accéder aux locaux contenant des données à caractère personnel.
- Pour l'ensemble des données quel sur soit le support :
  - Le présent règlement est un outil qui définit un cadre permettant à tous les agents de participer à la sécurisation de ces données.

9.3.4 Droits des personnes concernées / des agents

Les agents du Département peuvent exercer leurs droits concernant leurs données directement auprès des services concernés.

Ils peuvent également contacter le DPO par mail (delegue.donnees@ha-py.fr) ou par le formulaire du site internet (« Contacter le Délégué à la Protection des Données (DPO) »).

Ils peuvent également porter réclamation directement auprès de la CNIL : www.cnil.fr.

Une rubrique « RGPD / protection des données » est également à leur disposition :

- sur l'Intranet : « Projets Transverses > RPGD protection des données » ;
- et sur le site internet du Département « Protection des données ».

10 Usage à des fins privées

La Collectivité fournit à l'Utilisateur des moyens informatiques et de télécommunications dans le cadre de son activité professionnelle. Si l'Utilisateur en fait un usage personnel, il en assume la pleine et entière responsabilité ainsi que les conséquences juridiques.

L'Utilisateur n'est pas autorisé à se servir de son poste de travail, de son téléphone professionnel fixe ou portable à des fins privées sauf à titre occasionnel et si cela n'entraine aucune surfacturation ou perturbation du fonctionnement normal du système d'information.

La consultation des sites Internet à des fins personnelles est une simple tolérance. Sa consultation ne doit pas perturber le bon fonctionnement du service tant que la durée et le volume de connexion restent raisonnables.

Dans ce cadre personnel, la consultation doit se limiter à des sites Internet dont le contenu n'est pas contraire à l'ordre public, aux bonnes mœurs et aux missions de services publics. Il est notamment interdit :

- De rechercher, visualiser télécharger, transmettre ou conserver des contenus à caractère pornographique, pédophile, raciste, xénophobe, diffamatoire, portant atteinte au respect de la personne humaine et à sa dignité, incitant à l'accomplissement d'un délit ou d'un crime, contraire à l'ordre public ou aux bonnes mœurs, attentatoires à l'image interne ou externe de la Collectivité. L'Utilisateur ne peut être tenu pour responsable s'il reçoit, à son insu, de tels documents. Il est tenu d'en informer son supérieur hiérarchique puis de les supprimer. Il ne doit pas inciter un tiers à lui adresser de tels documents. Il doit s'abstenir de participer à des groupes de discussion ou de consulter des sites dont le caractère est proscrit (forums, news groups, tchats, etc.)

- De télécharger des logiciels ou des œuvres protégées, sans autorisation des ayants droit — Les administrateurs réseaux se réservent la possibilité d'effacer du système d'information toute trace de ces logiciels et œuvres introduites dans le Système, en violation des droits de propriété intellectuelle d'autrui,

- De consulter des sites susceptibles de comporter un risque pour le système d'information de la Collectivité, encombrer ou saturer le réseau,

- D'utiliser des dispositifs / sites web / logiciels permettant de contourner les dispositifs de protection technique ou de porter atteinte à la confidentialité des informations,

- De créer ou de mettre à jour, au moyen de l'accès à l'Internet fourni par la Collectivité, tout site Internet (notamment, page personnelle, journal personnel en ligne, etc.) en dehors du cadre professionnel autorisé**.**

L'utilisation des réseaux sociaux à des fins privées est une simple tolérance, ayant un caractère nécessairement exceptionnel, et sous réserve que cet usage ne perturbe pas le bon fonctionnement du service.

Les données privées (répertoires/données et e-mails) doivent être identifiées comme telles et classées dans un dossier nommé « PERSONNEL » ou « PRIVE ». Cela concerne les notes, les documents produits, mais aussi les fichiers et les messages électroniques.

Ce marquage n'empêche pas la Collectivité d'avoir accès à ces données. La Collectivité peut y accéder en présence de l'agent et en cas de nécessité ou de suspicion de non-respect des règles ci-dessus.

L'Utilisateur ne doit pas déposer sur les espaces de stockage réseaux ses données privées/personnelles. Les espaces de stockage réseau doivent faire l'objet d'un usage strictement professionnel.
L'Utilisateur supprime les données privées / personnelles (documents et e-mails) de son poste de travail à son départ de la Collectivité. Dans le cas contraire il s'expose à une éventuelle divulgation de ses données privées / personnelles.

11 Internet

L'Utilisateur identifié par les services informatiques dispose d'un accès à Internet, dans le cadre d'une autorisation.

L'Utilisateur engage sa responsabilité dans l'usage qu'il en fait, particulièrement du point de vue du droit de reproduction, d'utilisation, de détournement des informations manipulées.

La collectivité dispose d'un proxy qui permet la restriction des accès à certains sites ou la mise en place de quota horaire. Ce dernier permet aussi de conserver les traces de consultations des sites internet par les agents. Les traces sont conservées pour une année conformément à la législation.

11.1 Conditions d'utilisation

La consultation des sites Internet se fait dans le cadre strictement professionnel. L'usage à des fins privées est décrit dans le chapitre 10 « Usage à des fins privées ».
De manière générale, l'utilisation des services Internet à des fins commerciales, ludiques ou illicites est interdite.

En cas d'abus, pour des raisons de sauvegarde et de sécurité du système d'information, la DSIN a la faculté de supprimer ou de restreindre ponctuellement la connexion à Internet.
Elle peut être également mandatée pour cette action par une direction métier.

L'Utilisateur est informé que des dispositifs et procédures de contrôle pourront être mis en place par la Collectivité et s'appliquer à l'ensemble de la navigation sur l'Internet.

En parallèle de ces dispositifs de contrôle, des règles de filtrage et de blocage des sites Internet sont mises en œuvre. Si un site Internet se trouve bloqué par les services informatiques et que l'Utilisateur a, pour des raisons professionnelles, l'obligation d'accéder à ce site, il dépose une demande visée par son supérieur hiérarchique au service assistance de la DSIN afin de débloquer le site Internet.

En cas de procédure judiciaire pour une infraction présumée aux dispositions énoncées ci-dessus, la collectivité pourrait être tenue de communiquer à l'autorité judiciaire l'ensemble des informations demandées.

11.2 Forums, Réseaux sociaux et Sites collaboratifs

L'Utilisateur est informé des risques liés à l'utilisation de ces modes de communication :

- D'une part, au regard des risques d'encombrement, d'engorgement et de ralentissement des connexions,

- D'autre part, au regard de la responsabilité de l'Utilisateur, vis-à-vis de la Collectivité et des tiers, sur les propos émis. Pour rappel, ceci est également valable avec une connexion internet personnelle.

Dans le cadre de sa participation, l'Utilisateur respecte les règles du présent règlement, et en particulier au titre de la confidentialité : le respect de l'obligation de réserve et du secret professionnel.

11.3 Service dans le nuage (cloud)

L'utilisation de cloud public sort du périmètre de responsabilité de la Direction des Systèmes d'Information et du Numérique de la Collectivité.
Les données transmises sur ces plateformes peuvent être réutilisées, copiées, falsifiées, voire supprimées, engendrant un risque pour la Collectivité.
L'Utilisateur doit faire valider à la DSIN l'usage précis qu'il souhaite en faire.
L'utilisation de l'application « Transfert de fichiers » mise à disposition par la collectivité est préférable dans la mesure du possible moyennant la création d'un compte dédié.

12 Messagerie

Une messagerie est un outil de communication et d'échanges avec des tiers. L'Utilisateur dispose d'une adresse de messagerie électronique professionnelle.

Les personnes qui disposent d'une adresse e-mail sont répertoriées dans l'annuaire de messagerie électronique.

Il est nécessaire de prendre en compte les aspects administratifs, juridiques et contractuels des échanges par messagerie électronique ainsi que les règles de communication usuelles.

Les mêmes règles s'appliquent aux messageries de service (adresse mail générique) utilisées pour centraliser les demandes aux équipes régulièrement sollicitées.

12.1 Messagerie et usage privé

La messagerie est destinée à un usage professionnel. Toutefois, un usage privé est toléré et décrit au chapitre 10 « Usage à des fins privées ».

Dans son utilisation de la messagerie, l'Utilisateur ne doit pas perturber le fonctionnement normal de cette dernière en provoquant des ralentissements ou des pannes.
L'utilisation de la messagerie ne doit pas détourner l'Utilisateur de sa fonction au sein de la Collectivité.

12.2 Règles de bons usages

Afin de garantir un fonctionnement optimal, il convient d'observer les règles d'utilisation suivantes :

- L'Utilisateur doit s'appliquer à rédiger des messages courts et clairs pour éviter toute surcharge informationnelle nuisant à l'efficacité de la communication.

- Un message électronique adressé à un correspondant interne ou externe doit être rédigé avec autant de soin et selon le même formalisme et les mêmes règles qu'un courrier papier. Pour rappel, le message électronique est un écrit pouvant engager la responsabilité de la Collectivité.

- L'Utilisateur doit s'attacher à réduire le volume des messages et éviter les pièces jointes trop volumineuses. L'Utilisateur privilégie l'utilisation du service de transmission dédié (l'application de la collectivité transfert de fichiers) lors de la manipulation de fichiers volumineux.

Il est recommandé de lire quotidiennement ses messages et les traiter dans les meilleurs délais, c'est à dire :

- Détruire les messages ne nécessitant pas d'être conservés.
- Détruire les messages envoyés dès que l'expéditeur a été informé de leur réception et de leur lecture sauf nécessités particulières.
- Enregistrer les pièces jointes (sur le réseau ou localement) et détruire le message auquel elles sont attachées sauf nécessités particulières.
- Utiliser les listes de diffusion avec modération et discernement après avoir vérifié que tous les membres de la liste sont concernés par le message envoyé.
- Éviter l'envoi de copies à un nombre injustifié de destinataires.
- Ne pas répondre à un message envoyé en masse, c'est-à-dire privilégier le « répondre à » plutôt que « répondre à tous » si ce n'est pas nécessaire.
- Les règles hiérarchiques et d'organisation des pouvoirs internes de signatures doivent être respectées. Ainsi il est souhaitable de mettre systématiquement en copie de message important, son responsable, et le responsable du destinataire.
- L'Utilisateur signe ses mails avec les mentions précises du nom et de la qualité de l'expéditeur dans le respect des règles en vigueur.

- L'Utilisateur ne doit pas envoyer de message électronique à un destinataire extérieur à la Collectivité, s'il n'en a pas l'autorité du fait de sa fonction ou l'autorisation de sa hiérarchie.

Il convient de rappeler que la courtoisie constitue une règle de base dans tous les échanges électroniques.

12.3 Secret professionnel

Les agents soumis au secret professionnel voient leur obligation de non-divulgation persister dans l'usage de la messagerie électronique.

L'Utilisateur identifie les informations couvertes par le secret professionnel en les stockant dans un dossier « secret professionnel ». Ces messages devront contenir dans l'objet l'information suivante : [SECRET PROFESSIONNEL].

Un message électronique peut contenir un document administratif soumis au principe de la liberté d'accès et au droit à communication.
En conséquence, les transmissions par e-mail sont autorisées uniquement pour les copies de décisions administratives exécutoires, pour lesquelles toutes les mesures de publicité auront été accomplies.

Toute demande d'un usager (hors administration ou organisme extérieur), reçue par message électronique, doit faire l'objet d'un accusé de réception selon les mêmes règles que pour le courrier papier.

12.4 Respect de la Continuité de service

Afin d'assurer la continuité de service, l'Utilisateur devra, en cas d'absence planifiée, mettre en place un message informant de la durée de son absence et indiquant les coordonnées de la personne à contacter en cas de besoin.

Par ailleurs, le supérieur hiérarchique d'un Utilisateur peut demander un accès à la messagerie professionnelle de ce dernier, à titre dérogatoire et pour assurer la continuité de service et dans un délai défini. Ces droits d'accès seront supprimés à l'expiration.

Sont exclus de cette possibilité les messages expressément identifiés comme personnels ou ceux contenant des informations couvertes par le secret professionnel identifiées dans un dossier « secret professionnel ».

Toutefois dans le cadre d'une procédure pénale ou par décision de justice, le contenu de ces messages peut être consulté par la Collectivité.

En cas de départ, l'Utilisateur devra s'assurer de transférer à la personne désignée les messages nécessaires pour assurer la continuité des dossiers traités avant son départ.

12.5 Sécurité des données transmises par messagerie

En l'absence de dispositif de chiffrement et de certification dans les échanges, l'intégrité et la confidentialité des documents transmis sur Internet via la messagerie ne peuvent être garanties.

L'Utilisateur doit demander l'autorisation formelle du responsable hiérarchique s'il autorise la transmission de fichier, documents ou informations à caractère confidentiel ou soumis au secret professionnel. La Collectivité rappelle que la fuite de document est passible de sanctions.

La réception d'e-mails accompagnés de pièces jointes est l'une des causes principales d'introduction des logiciels malveillants dans les systèmes informatiques.

Pour cette raison, il est demandé à l'Utilisateur de :

- Signaler au support informatique la réception d'un message suspect : ne correspondant pas à un envoi à caractère strictement professionnel et spécifiquement attendu (envois réguliers et programmés ou transmission avec avis préalable de l'expéditeur).

- D'être prudent à la réception de message provenant de l'extérieur de personnes inconnues ou dont l'objet paraît suspect.

Afin de limiter les messages indésirables, les sollicitations abusives ainsi que les risques de SPAM et de logiciel malveillants, l'Utilisateur diffuse son adresse e-mail avec parcimonie. L'Utilisateur n'est pas autorisé à utiliser son adresse e-mail professionnelle pour créer un compte sur un site web ou s'inscrire à une liste de diffusion personnelle.

13 Téléphonie

L'utilisateur est tenu d'utiliser les outils de téléphonie mis à sa disposition par la Collectivité à des fins professionnelles, et conformément aux lois et règlement, à l'ordre public et aux bonnes mœurs, au respect de l'image de la Collectivité.

L'usage à des fins personnelles est toléré, à titre privé, et conformément aux prescriptions du règlement. La Collectivité a mis en place des dispositifs techniques permettant de tracer les informations relatives aux appels téléphoniques.

La Collectivité s'engage à n'exercer aucun contrôle sur les listes des appels émis et reçus par les représentants du personnel et les représentants syndicaux dans le cadre de leur mandat.

14 Visioconférence

L'Utilisateur de visioconférence accepte par sa participation à une séance que son image et le son soient exploités par tout moyen technique rendu nécessaire au bon déroulement de la visioconférence.

L'utilisateur de ce système renonce dans l'exercice de leurs fonctions à leur droit à l'image.

L'utilisateur n'utilise pas la visioconférence pour des réunions à caractère confidentiel, s'il n'a pas l'assurance qu'elle est sécurisée.

L'Utilisateur ne diffuse pas de contenu confidentiel s'il n'y est pas habilité.

15 Moyens d'impression

Le système d'information de la Collectivité est équipé de photocopieurs multifonctions, qui offrent notamment des services de copie, impression et scanner.

L'usage des imprimantes individuelles est restreint à des besoins très spécifiques.

La Collectivité recommande aux Utilisateurs de n'imprimer des documents et e-mails que lorsque cela est nécessaire. L'utilisateur privilégie les copies et impressions en noir et blanc, et utilise le format recto / verso ou plusieurs pages sur une même face.

L'utilisateur récupère les documents imprimés dès leur impression, afin de se prémunir de perte ou de fuite d'informations sensibles.

L'utilisateur jette les documents inutiles dans les dispositifs de collecte de papier.
L'utilisateur utilise les dispositifs de broyage adéquats lorsque les informations sont confidentielles.

16 Badge

Chaque badge est strictement personnel et engage la responsabilité de l'Utilisateur.

Il est interdit de le céder, le donner ou le prêter.

Pour des raisons de sécurité, l'Utilisateur du badge veille également à ne pas permettre le passage à des personnes non munies de leur badge pour des portes munies de lecteurs de commande. L'utilisation du badge engage de fait son utilisateur à respecter le règlement intérieur du bâtiment dans lequel il pénètre. En cas de non-respect des règles, le badge sera désactivé.

En cas de perte ou de vol, il convient de prévenir immédiatement le service gestionnaire à la direction des ressources humaines afin que les droits associés au badge perdu soient supprimés.

Les droits d'accès de l'Utilisateur aux bâtiments sont programmés d'après les informations fournies et vérifiés lors de la création du badge.

Lors du départ d'un Utilisateur ou d'un changement de fonction, les autorisations d'accès attribués seront supprimées ou modifiées selon la procédure en vigueur.

Les journaux d'événements, centralisés de manière exhaustive par le logiciel de gestion du système de contrôle des accès, sont consultables par le gestionnaire du système.
Des vérifications peuvent être effectuées afin d'identifier les accès réalisés, les refus, les erreurs ou anomalies.

L'Utilisateur qui fait usage d'un badge non délivré par la collectivité est passible de sanctions disciplinaires.

17 Administration

L'Administrateur technique quel que soit son périmètre est garant du bon fonctionnement et de la sécurité du système d'information ainsi que de la disponibilité des données et des applications informatiques de la Collectivité.

Il dispose au même titre que les Utilisateurs de la Collectivité d'un compte personnel qui permet de tracer toutes les informations relatives à ses actions.
Dans l'exercice de ses missions, l'Administrateur technique veille à faire respecter les droits et devoirs des Utilisateurs définis par le présent règlement et en application des dispositions légales et règlementaires.

Les Utilisateurs sont informés que l'Administrateur technique peut avoir accès à l'ensemble du système d'information de la Collectivité, à n'importe quel moment et ce afin d'effectuer tout acte de protection, ce qui comprend notamment :

- La sauvegarde, la conservation et la diffusion des informations collectées et traitées dans le cadre des activités de la Collectivité,
- La vérification de la date de création ou de la diffusion desdites informations,
- La protection de l'intégrité et de la confidentialité des données du système d'information,
- Le contrôle d'absence d'intrusion dans le système d'information ou de matériels en violation des dispositions légales et réglementaires en vigueur,
- La mise à jour, la maintenance, la correction et la réparation des matériels et logiciels nécessaires à l'utilisation et au bon fonctionnement du système d'information.

L'Administrateur technique est habilité à mettre en place des outils de contrôle et de surveillance répondant à la finalité de sécurité du système d'information de la Collectivité.

L'Administrateur dispose de privilèges importants dont il ne doit pas tirer un profit personnel. L'Administrateur est tenu à une obligation de confidentialité stricte, excepté

dans les cas où sa responsabilité pénale est susceptible d'être engagée, où l'intérêt de la Collectivité est menacé.

L'Administrateur technique ne doit pas utiliser ou divulguer les informations couvertes par le secret professionnel ou le secret des correspondances privées, et toutes les informations relatives à la vie privée des Utilisateurs, ou des administrés. Les Administrateurs techniques sont autorisés à prendre la main à distance sur le poste de travail de l'Utilisateur avec son accord préalable.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsque l'Utilisateur n'est pas connecté à son poste de travail, l'Administrateur Technique peut être amené à intervenir sur l'environnement technique des postes de travail.

Seul l'Administrateur technique est autorisé à introduire dans le système d'information de nouveaux matériels ou logiciels, à sa demande ou à celle de l'Utilisateur. Il motivera par une analyse la décision d'installer ou non le nouveau composant.

18 Systèmes de supervision et de contrôle

La Collectivité met en place :

- Sur le réseau des dispositifs de protection (pare-feu, détection et prévention d'intrusion et proxy-cache) pour filtrer le trafic entrant et sortant du SI.
- Sur les postes de travail des logiciels de protection contre les attaques informatiques (pare-feu, antivirus, détection d'intrusion).
- Des systèmes de protection contre les logiciels malveillants et les messages indésirables sur les outils de messagerie.

L'Utilisateur ne doit pas tenter de désactiver, de désinstaller ou de perturber le fonctionnement de ces outils.

En cas de détection de virus ou de menaces, la Collectivité se réserve le droit de retenir, d'isoler et/ou de supprimer tout élément infecté.

Ces dispositifs sauvegardent des journaux d'activité contenant des données à caractère personnel sur le comportement des Utilisateurs.

L'Utilisateur est informé que des traitements permettent de contrôler et de prévenir les anomalies liées à une intrusion ou un usage déraisonné du système d'information.
En cas de dysfonctionnement constaté, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs Utilisateurs.

19 Communication et Approbation

Le présent règlement sera porté à la connaissance de tous les Utilisateurs et mis à disposition sur l'intranet de la Collectivité.

L'Utilisateur s'engage à appliquer l'ensemble des dispositions du présent règlement. Il est systématiquement remis à tout nouvel arrivant. Il fait l'objet d'une clause spécifique aux contrats liant la Collectivité à des partenaires.

Des actions de communication / formation internes sont organisées afin d'informer les Utilisateurs des pratiques recommandées.

Les dispositions décrites dans ce règlement sont applicables depuis le 01/01/2021

En fonction des évolutions réglementaires, législatives et techniques, ce règlement fera l'objet de mises à jour présentées aux représentants du personnel lors de comités techniques paritaires.

20 Sanctions

Le non-respect des règles et précautions figurant dans le présent règlement engage la responsabilité personnelle de l'Utilisateur dès lors qu'il est prouvé que les faits lui sont personnellement imputables ou qu'il fournit à un tiers des informations permettant de commettre une infraction. Cela l'expose, de manière appropriée et proportionnée à la faute commise, à des sanctions disciplinaires et/ou pénales.

La responsabilité pénale de l'utilisateur peut être engagée telle que définie au Chapitre III : « Des atteintes aux systèmes de traitement automatisé de données », articles 323-1 à 323-8 du code pénal.

De tels comportements peuvent être punis pénalement, au sens notamment de l'article 323-1 du Code pénal qui prévoit que :

« *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.*

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

Spécifiquement concernant les données à caractère personnel et les atteintes aux droits de la personne concernée, toute violation du présent règlement expose chaque utilisateur à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Nom du traitement	Finalités	Licéité	Catégories de données	Données sensibles	Durée de conservation
Carrière et paye	Gestion de la carrière et de la paye des agents de la collectivité et des élus, entretien professionnel	Obligations légales et exécution du contrat de travail : - Loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la FPT - Art. 18 de la loi n° 83-634 du 13 juillet 1983 - Loi n°2009-972 du 3 août 2009 relative à la mobilité et aux parcours professionnels dans la fonction publique - Art. 1-1 du décret n° 88-145 du 15 février 1988 - Article 1er du décret n° 2011-675 du 15 juin 2011relatif au dossier individuel des agents publics et à sa gestion sur support électronique	- État-civil, identité, données d'identification, images - Vie personnelle - Vie professionnelle - Informations d'ordre économique et financier - Données de connexion	Oui : - NIR - Données de santé (arrêts de travail, travailleurs handicapés) - Appartenance syndicale pour les représentants syndicaux	Application de la réglementation en matière RH
Temps de travail et absences	Gestion du temps de travail des agents : pointage, workflow des absences (demande, validation, justificatifs), gestion des absences (plannings), suivi et consultation des compteurs d'absence (congés, RTT autorisations spécifiques), simulation de plannings de présence individuelle	Obligations légales et exécution du contrat de travail : - Décret n°91-875 du 6 septembre 1991 relatif au régime indemnitaire dans la FPT - Décret n°2001-623 du 12 juillet 2001 relatif à l'aménagement et à la réduction du temps de travail dans la fonction publique territoriale - Délibération du protocole temps de travail de la collectivité	- État-civil, identité, données d'identification, images - Vie personnelle - Vie professionnelle - Données de connexion - Données de localisation	Non	Application de la réglementation en matière RH
Formations et compétences	Gestion des formations et compétences des agents, gestion prévisionnelle des emplois et des compétences	Obligations légales et intérêt légitlme du respponsable de traitement : - Loi n°84-594 du 12 juillet 1984 relative à la formation des agents de la fonction publique territoriale - Décret n°2008-512 du 29 mai 2008 relatif à la formation statutaire obligatoire dans la fonction publique territoriale (FPT) - Décret n°2007-1845 du 26 décembre 2007 relatif à la formation professionnelle tout au long de la vie des agents de la fonction publique territoriale (FPT)	- État-civil, identité, données d'identification, images - Vie professionnelle	Non	Application de la réglementation en matière RH
Recrutements	Gestion des recrutements internes et externes, gestion des stages	Exécution d'un contrat ou mesures précontractuelles	- État-civil, identité, données d'identification, images - Vie personnelle - Vie professionnelle	Non	Application de la réglementation en matière RH
Dotations individuelles	Gestion des dotations individuelles des agents : fournitures, EPI, véhicules	Obligation légale et exécution du contrat de travail	- État-civil, identité, données d'identification, images - Vie professionnelle	Non	Application de la réglementation en matière RH
Frais de déplacement	Gestion des déplacements professionnels, des demandes et des remboursements de frais de déplacements	Obligation légale : - Loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la FPT - Décret n°2001-654 du 19 juillet 2001 fixant les conditions et les modalités de règlements des frais occasionnés par les déplacements des personnels territoriaux	- État-civil, identité, données d'identification, images - Vie personnelle - Vie professionnelle	Non	Application de la réglementation en matière RH
Elections professionnelles	Organisation des élections professionnelles pour la désignation des reprsentants du personnel	Obligations légales	- État-civil, identité, données d'identification, images - Vie professionnelle	Oui : appartenance syndicale des candidats	Application de la réglementation en matière RH

Nom du traitement	Finalités	Licéité	Catégories de données	Données sensibles	Durée de conservation
Action sociale pour les agents	Fournir des prestations d'action sociale aux agents	Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images - Vie personnelle - Vie professionnelle - Informations d'ordre économique et financier	Non	Application de la réglementation en matière RH
Médecine du travail	Gestion de la médecine du travail en application de la réglementation, suivre la santé des agents au travail, mettre en œuvre des mesures préventive, accidents du travail, maladie professionnelle, commission de réforme, comité médical	Obligations légales	- État-civil, identité, données d'identification, images - Vie personnelle - Vie professionnelle	Oui : NIR, données de santé	Application de la réglementation en matière RH
Indemnités chômage	Gestion des indémnités chômage des agents licenciés	Obligations légales	- État-civil, identité, données d'identification, images - Vie professionnelle - Informations d'ordre économique et financier	Non	Application de la réglementation en matière RH
Dossiers agents	Gestion des dossiers agents en application de la réglementation	Obligations légales	- État-civil, identité, données d'identification, images - Vie personnelle - Vie professionnelle - Informations d'ordre économique et financier - Données de connexion	Oui : NIR, données de santé, données relatives aux condamnations pénales ou aux infractions	Application de la réglementation en matière RH
Risques professionnels et document unique	Identifier les risques professionnels, mettre en œuvre les mesures de sécurité, assurer la sécurité des agents et des biens, respecter les obligations réglementaires en la matière, registre santé sécurité	Obligations légales	- État-civil, identité, données d'identification, images - Vie professionnelle	Oui : données de santé	Application de la réglementation en matière RH
Budget et masse salariale	Définition, pilotage et maitrise du budget et de la masse salariale	Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images - Vie professionnelle - Informations d'ordre économique et financier	Non	Application de la réglementation en matière RH
Déclaration Sociale Nominative	Déclaration obligatoire des cotisations sociales	Obligations légales	- État-civil, identité, données d'identification, images - Vie professionnelle - Informations d'ordre économique et financier	Oui : - NIR - Données de santé (arrêts de travail, travailleurs handicapés)	Application de la réglementation en matière RH
Communication et affichage RH	Affichage et diffusion des informations réglementaires RH telles que les listes d'agents à l'issue des CAP	Obligations légales	- État-civil, identité, données d'identification, images - Vie professionnelle	Non	Application de la réglementation en matière RH
Echanges de données avec les organisations syndicales	Transmission des données entre le Département et les OS dans le cadre des obligations légales (instances de représentation du personnel)	Obligations légales	- État-civil, identité, données d'identification, images - Vie professionnelle	Non	Application de la réglementation en matière RH
Gestion des postes et effectifs	Connaissance et maitrise des postes et effectifs du Département, gestion prévisionnel des postes (tableau des effectifs, ...)	Obligations légales et Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images - Vie professionnelle	Non	Application de la réglementation en matière RH

Nom du traitement	Finalités	Licéité	Catégories de données	Données sensibles	Durée de conservation
Attribution et gestion des droits d'accès aux ressources informatiques	Fournir aux agents de manière sécurisée les outils et ressources numériques dont ils ont besoin pour l'exercice de leurs missions	Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images	Non	Tant que l'agent fait partie du Département
Gestion de la sécurité du SI par la traçabilité des actions	Assurer la sécurité du Système d'Information	Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images - Données de connexion	Non	Application de la réglementation en matière sécurité des SI
Traçabilité de la navigation internet	Respect de la réglementation en tant que fournisseur d'accès internet pour ses agents	Obligations légales	- État-civil, identité, données d'identification, images - Données de connexion - Internet	Non	Application de la réglementation en matière sécurité des SI (1 an)
Téléphonie	Gestion de la facturation des communications	Exécution du contrat avec le prestataire de télécommunication	- État-civil, identité, données d'identification, images - Données de connexion (historique des appels)	Non	Historique des appels
Contrôle d'accès aux bâtiments	Assurer la sécurité des accès aux bâtiments	Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images - Vie professionnelle - Données de connexion - Données de localisation	Non	1 an
Vidéosurveillance	Assurer la sécurité des accès aux bâtiments	Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images	Non	Pas de conservation des données
Organigrammes et annuaires	Communication interne et travail collaboratif	Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images - Vie professionnelle	Non	Tant que l'agent fait partie du Département
Intranet et communication interne	Communication interne et travail collaboratif	Intérêt légitime du responsable de traitement	- État-civil, identité, données d'identification, images - Vie professionnelle	Non	Tant que l'agent fait partie du Département

Licéité (Article 6 du RGPD)
Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:
a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Catégories de données (définition CNIL) :
- État-civil, identité, données d'identification, images (ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)
- Vie personnelle (ex. habitudes de vie, situation familiale, etc.)
- Vie professionnelle (ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)
- Informations d'ordre économique et financier (ex. revenus, situation financière, données bancaires, etc.)
- Données de connexion (ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)
- Données de localisation (ex. déplacements, données GPS, GSM, …)
- Internet (ex. cookies, traceurs, données de navigation, mesures d'audience, …)

Données sensibles :
La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).