

Règlement d'Utilisation du Système d'Information



Ville de Castelnau-d'Aud

Direction Générale des Services
Service Informatique

AVANT PROPOS

La mise en place d'un intranet et de la connexion Internet à haut débit nous a conduits à la rédaction d'un Règlement d'utilisation du Système d'Information.

La connexion Internet ouvre notre réseau sur le monde extérieur. Nous avons bien sûr pris en compte ce fait pour l'installation de tous les systèmes de sécurité permettant d'interdire l'accès de notre intranet à toute personne extérieure et de le protéger contre tous les virus que se propagent sur Internet.

Malgré cela, une intrusion est toujours envisageable et nous devons nous donner les moyens de « tracer » tout ce qui a été fait sur le Système d'Information, dans le cas où nous serions victimes d'une attaque de pirates informatiques.

C'est pourquoi nous tenons à attirer votre attention sur le fait que votre connexion au Système d'Information se fait par un nom d'utilisateur et un mot de passe (cf. paragraphe « accès sécurisé au réseau » du Règlement) qui engage votre responsabilité, dans le sens où toute action effectuée sur le réseau sous votre nom d'utilisateur vous sera attribuée.

Ne communiquez donc votre mot de passe à personne. Tous les ordinateurs étant équivalents sur le réseau, si un tiers doit se servir du votre, il devra le faire en utilisant son propre nom d'utilisateur.

L'observation de cette règle simple peut nous éviter des ennuis en cas d'usurpation des droits d'accès à notre Système d'Information.

Sommaire

Préambule	4
Généralités	4
Objet du Règlement	4
Champ d'application	5
Administrateur du Système d'Information	5
Respect des obligations CNIL / RGPD	5
Avis du Comité Social Territorial	6
La protection du Système d'Information	6
Sécurité et vigilance	6
Accès sécurisé au réseau	7
Les sauvegardes.....	7
Les pare-feux et antivirus.....	7
Contrôle et maintenance par l'Administrateur	7
Introduction de Matériels et Logiciels	8
Non-respect de ces dispositions	8
La messagerie	8
Adresse électronique	8
Message électronique et pouvoirs internes.....	9
Contenu du message électronique	9
Protection des Informations	9
Format et taille des messages électroniques.....	9
Règles de conservation de la messagerie	10
Utilisation privée de la messagerie	10
La navigation sur le web	10
Navigateur.....	10

Participation à des forums.....	10
Téléchargement de logiciels ou d'œuvres protégées.....	10
Consultation de sites illicites	11
Consultation d'internet à des fins privées.....	11
Intranet	11
Mise en place et fonctionnement de l'Intranet.....	11
Données nominatives et personnelles	11
Opérations de contrôle de sécurité.....	11
Place de l'Amicale des Retraités dans le Système d'Information	13
Outils d'information mis à disposition.....	13
Règles de communication.....	13
Place des syndicats dans le Système d'Information.....	13
Outils d'information mis à disposition.....	13
Règles de communication.....	14
Mesures d'urgence et plan de reprise d'activité.....	14
Sanctions.....	15
Sanctions disciplinaires.....	15
Affichage et formalités – Entrée en vigueur.....	15

Préambule

La ville de Castelnaudary a toujours privilégié la transparence de son Système d'Information. Afin d'éviter toute dérive par ignorance des règles et de leurs conséquences, un rappel de ces règles est important. En effet le contexte des nouvelles technologies est complexe et évolutif. La connaissance des règles d'utilisation est primordiale afin d'établir clairement ce qui relève du domaine privé et ce qui relève du domaine professionnel sur le lieu de travail. Préserver le Système d'Information, dans le respect des droits et libertés de chacun, telle est l'ambition de ce Règlement d'utilisation du Système d'Information de la ville de Castelnaudary.

Généralités

Objet du Règlement

L'objet du Règlement est d'indiquer les règles d'utilisation et de fonctionnement du Système d'Information de la Collectivité.

On entend par Système d'Information de la Collectivité :

- l'ensemble des ordinateurs, fixes ou portables, et tout autre matériel informatique, connectique ou bureautique (compris les serveurs, hubs, commutateurs, câbles du réseau, fax, photocopieurs, téléphones, fixes ou portables, appareils photos numériques, matériel d'infographie)
- l'ensemble des logiciels contenus ou faisant fonctionner, inter opérer ou protégeant lesdits ordinateurs et matériels informatiques, (compris les protocoles de communication TCP/IP,)

permettant :

- la constitution et la création
- l'échange, la circulation, la diffusion,
- la duplication, reproduction et stockage,

de :

- données, fichiers, base de données,
- intranet, extranet
- images, sons, textes,
- flux quelconques d'information,

entre :

- les " utilisateurs " entre eux,
- les " utilisateurs " et l'extérieur,

et ce quelle que soit la finalité du flux d'information.

Champ d'application

Le présent Règlement s'applique à tous les utilisateurs autorisés du Système d'Information de la ville de Castelnaudary

L'intrusion non autorisée dans le Système d'Information de la ville de Castelnaudary peut être considérée comme une infraction selon l'article 323-1 du Code Pénal.

Article 323-1 du Code Pénal :

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 30 000 euros 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 45 000 euros d'amende.

Administrateur du Système d'Information

Le responsable du Système d'Information de la ville de Castelnaudary est désigné " Administrateur " du Système d'Information. Il veille à la protection, à la maintenance, au bon fonctionnement du Système d'Information et s'assure du respect du présent règlement. Il agit en concertation avec le service juridique de la ville de Castelnaudary afin de se mettre en conformité avec les dispositions légales, effectuer toutes formalités ou déclarations, en particulier celles issues de la Loi Informatique et Libertés du 6 janvier 1978 et de la loi du 10 juillet 1991 sur le secret des correspondances.

loi du 10 juillet 1991 sur le secret des correspondances

Article 1 : *Le secret des correspondances émises par la voie des télécommunications est garanti par la loi.*

Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi dans les limites fixées par celle-ci.

Respect des obligations CNIL / RGPD

Si l'Utilisateur est amené à constituer un fichier contenant des données à caractère personnel susceptibles de relever de l'application de la loi dite « Informatique et Libertés », l'Utilisateur devra en informer le délégué à la protection des données (DPO) de la ville de Castelnaudary qui est chargé de veiller au respect du RGPD (Règlement Général sur la Protection des Données).

Les 5 principes clés de la protection des données personnelles sont les suivants :

- La finalité : les objectifs du traitement respectent les droits et libertés des individus,
- La pertinence : ne pas collecter plus de données que ce dont on a vraiment besoin,
- La conservation : la durée de conservation doit être définie au préalable,
- Les droits : informer les personnes ; obtenir leur consentement ; assurer leur droit d'accéder à leurs données, le droit de les rectifier et le droit de s'opposer à leur utilisation,
- La sécurité : prendre toutes les mesures nécessaires pour garantir la sécurité des données (disponibilité, intégrité, confidentialité).

Avis du Comité Social Territorial

Le présent Règlement a été soumis à l'avis du Comité Social Territorial de la ville de Castelnaudary, qui a été informé et consulté conformément au 3° de l'article 33 de la loi 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale.

La protection du Système d'Information

Sécurité et vigilance

L'Utilisateur s'engage à utiliser les équipements informatiques de façon loyale et à être vigilant en signalant toute anomalie ou intrusion qu'il pourrait constater. L'Utilisateur est tenu d'informer, sans délai, sa hiérarchie et l'Administrateur de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les équipements informatiques.

L'Utilisateur doit utiliser les équipements informatiques dans le respect des procédures et méthodologies qui sont applicables au sein de la Collectivité (notes, politiques, processus, livrets des procédures, livrets des préconisations, manuels utilisateur, etc.) et s'engage à utiliser exclusivement les outils et services d'accès sécurisés que la Collectivité a mis à la disposition de l'Utilisateur (VPN entreprise notamment).

L'Utilisateur pourra être invité par l'Administrateur à prendre des mesures d'urgence ou de sécurité spécifique, qu'il s'engage à appliquer dès son information.

À des fins de précaution, certaines configurations peuvent être verrouillées par l'Administrateur (poste de travail, accès internet, etc.).

La mise en place d'outils de sécurité par l'Administrateur ne doit pas, toutefois, dispenser les Utilisateurs d'une obligation de vigilance à cet égard.

En effet, tout Utilisateur a la charge, à son niveau, de contribuer à la sécurité des équipements informatiques mis à sa disposition, principalement en évitant l'introduction de codes malveillants susceptibles d'endommager le système d'information de la Collectivité.

L'Utilisateur s'interdit également de :

- Modifier les équipements informatiques de la Collectivité notamment par l'ajout de logiciels, progiciels, ou de matériels pour quelque raison que ce soit ;
- Modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit, en particulier les fichiers contenant des informations comptables ou d'identification ;
- Mettre à la disposition d'Utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a l'usage ;
- Utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués où masquer son identité ;
- Effectuer des opérations pouvant nuire aux relations internes ou externes de la Collectivité ;
- Connecter tout dispositif de stockage externe sur les postes de travail ;
- Utiliser tout moyen de prise en main à distance sans autorisation.

D'une manière générale, toute installation ou utilisation de matériels et logiciels non expressément autorisés, est interdite.

En cas de violation du présent Règlement ou de risque d'atteinte à la sécurité des équipements informatiques de la Collectivité, cette dernière pourra prendre immédiatement toutes mesures conservatoires de sécurité notamment des suspensions et blocages d'accès de l'Utilisateur, sur tout ou partie des équipements informatiques.

Accès sécurisé au réseau

L'accès au réseau est protégé par des mots de passe. Ces mots de passe sont choisis par l'utilisateur de manière individuelle et respectent les préconisations de la CNIL :

1. Longueur minimale 12 caractères
2. Composé de caractères issus de 3 des 4 catégories suivantes :
 - a. Caractères majuscules (A à Z)
 - b. Caractères minuscules (a à z)
 - c. Chiffres en base 10 (0 à 9)
 - d. Caractères spéciaux (par exemple, !, \$, #, %)

Les mots de passe doivent être modifiés tous les 42 jours et le nouveau mot de passe doit être différent du précédent.

En aucune manière ils ne doivent être donnés à un collègue, ni notés sur l'ordinateur de l'utilisateur. L'utilisateur doit le mémoriser. En cas d'oubli, seul l'Administrateur du réseau pourra renouveler le mot de passe de l'utilisateur.

Les sauvegardes

Il est indispensable que les données soient sauvegardées régulièrement. Les sauvegardes sont réalisées par l'Administrateur.

Les pare-feux et antivirus

La ville de Castelnaudary dispose de pare-feux face à l'intrusion et d'antivirus face aux logiciels malveillants, afin que le Système d'Information soit protégé de manière efficace. Les mises à jour sont réalisées par l'Administrateur.

Contrôle et maintenance par l'Administrateur

Les utilisateurs sont avertis que l'Administrateur peut avoir accès à l'ensemble des composants du Système d'Information à n'importe quel moment et ce afin d'effectuer tout acte de protection du Système d'Information. La protection du Système d'Information s'entend de la manière suivante :

- conservation, sauvegarde, absence de diffusion non autorisée des informations appartenant à la collectivité,
- la preuve de la date de création ou de la diffusion desdites informations,
- protection de l'intégrité des données et du fonctionnement du Système d'Information,
- la mise à jour, maintenance, correction, réparation des Matériels et Logiciels.

Dans le cas, où un composant du Système d'Information ne se trouverait pas dans l'enceinte de la Collectivité, l'utilisateur qui en a la garde s'oblige à le restituer ou le confier à l'Administrateur à première demande de sa part.

L'Administrateur pourra mettre en place des outils de contrôle et de surveillance répondant strictement à la finalité de la protection du Système d'Information. Il est rappelé que les délégués du personnel pourront saisir immédiatement l'employeur, s'ils constatent qu'il existe une atteinte aux droits des personnes ou aux libertés individuelles dans la Collectivité qui ne serait pas justifiée par la nature de la tâche à accomplir ni proportionnée au but recherché.

Introduction de Matériels et Logiciels

Seul l'Administrateur est autorisé à introduire dans le Système d'Information de nouveaux Matériels ou Logiciels. En cas de besoins exprimés par un utilisateur pour un nouveau matériel ou logiciel, il devra demander l'autorisation préalable à l'Administrateur avant son admission dans le Système d'Information.

De la même manière, l'Utilisateur s'interdit de porter atteinte à l'intégrité et à la conservation des données et bases de données de la Collectivité, et s'engage à respecter les finalités des équipements informatiques et des traitements de données réalisées au sein de la Collectivité. En tout état de cause, il s'interdit, notamment et en particulier, de charger ou de transmettre, sciemment, des fichiers contenant des virus ou des données altérées.

L'Utilisateur restera responsable d'introduction sur son poste de travail, d'informations ou de matériels violant les règles relatives au droit d'auteur, copyright, par exemple pour défaut de licence d'utilisation.

Non-respect de ces dispositions

Le non-respect des dispositions du présent chapitre peut exposer l'utilisateur aux sanctions prévues au chapitre « Sanctions » du Règlement et à la mise en jeu de sa responsabilité en cas d'intrusion du fait de l'Utilisateur de virus ou d'un tiers non-autorisé dans le Système d'Information ou de perte de données.

Les chapitres suivants précisent les règles relatives à certaines utilisations du Système d'Information.

La messagerie

Adresse électronique

Chaque utilisateur dispose d'une messagerie électronique composée du prénom et du nom. En cas d'homonymie, l'Administrateur fixera la règle d'attribution. Ex : En cas de changement de nom, l'utilisateur pourra demander à l'Administrateur une nouvelle messagerie électronique. L'utilisation d'un pseudonyme ou l'usage d'un faux nom est expressément prohibée, sauf autorisation de l'Administrateur qui s'assurera du bien-fondé de cette utilisation.

Message électronique et pouvoirs internes

Une attention toute particulière doit être portée à la rédaction et à la diffusion des messages. Le message électronique (email ou mel) est un écrit pouvant engager la Collectivité. Le message électronique peut être reconnu comme preuve valable pour établir un fait ou un acte juridique. Les règles hiérarchiques et d'organisation des pouvoirs internes de signatures devront être respectées. Aucun message électronique ne devra être envoyé par un utilisateur à un destinataire extérieur à la collectivité, si l'Utilisateur n'en a pas l'autorité.

Contenu du message électronique

Le message électronique sous réserve de la mention dans le message lui-même ou compte tenu des circonstances s'induisant de son envoi, est considéré comme un acte public. Aucun message électronique y compris relevant de l'utilisation privée, ne devra comprendre des éléments de nature offensante, diffamatoire, injurieuse, ou contraires aux dispositions de la Loi du 29 juillet 1881 sur la liberté de la presse. Cette règle est valable tant à l'égard des autres utilisateurs que de tout tiers extérieur à la Collectivité, lorsque dans ce dernier cas le message électronique est adressé à l'extérieur de la Collectivité.

Loi du 29 juillet 1881 sur la liberté de la presse :

Article 23 : *Seront punis comme complices d'une action qualifiée crime ou délit ceux qui, soit par des discours, cris ou menaces proférés dans des lieux ou réunions publics, soit par des écrits, imprimés, dessins, gravures, peintures, emblèmes, images ou tout autre support de l'écrit, de la parole ou de l'image vendus ou distribués, mis en vente ou exposés dans des lieux ou réunions publics, soit par des placards ou des affiches exposés au regard du public, soit par tout moyen de communication au public par voie électronique, auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet. Cette disposition sera également applicable lorsque la provocation n'aura été suivie que d'une tentative de crime prévue par l'article 2 du code pénal.*

Protection des Informations

Les risques d'interception des messages électroniques exigent de limiter l'utilisation de la messagerie électronique à destination de l'extérieur du Système d'Information aux Informations à caractère non confidentiel, non stratégique et non sensible. Si un utilisateur est contraint d'adresser à l'extérieur des Informations à caractère confidentiel, stratégique ou sensible, outre la signature préalable d'un engagement de confidentialité conforme aux règles imposées par le service juridique de la ville de Castelnaudary, l'Utilisateur devra demander à l'Administrateur de l'assister pour le cryptage de l'Information. L'Administrateur pourra :

- soit installer un outil de cryptage sur le matériel confié à l'utilisateur permettant la diffusion cryptée de l'Information,
- soit assurer lui-même cette transmission cryptée.

Format et taille des messages électroniques

L'Administrateur peut limiter le format, le type et la taille des messages électroniques pièces jointes comprise. Il est interdit d'envoyer des messages ne respectant pas le format, le type et la taille prescrits par l'Administrateur.

Règles de conservation de la messagerie

La messagerie électronique ne sera conservée sur le serveur concerné de la Collectivité que pour une durée courte déterminée par l'Administrateur mais ne pouvant excéder six mois. Au delà de cette date, les messages seront effacés sauf avis contraire donné par l'Utilisateur qui demanderait une prolongation expresse à l'Administrateur.

Utilisation privée de la messagerie

L'Utilisateur peut utiliser la messagerie électronique de la collectivité à des fins privées. Il aura soin dans la mesure du possible de classer ses messages privés (reçus ou envoyés) dans un fichier à part portant la mention " privé " de manière à prévenir l'Administrateur de la nature particulière s'attachant à cette messagerie.

L'usage privé de la messagerie (envoi et réception de messages) ne devra pas gêner le trafic normal des messages professionnels, et ce en termes de volume, de taille des messages échangés et de format des pièces jointes. Il devra s'inscrire dans le respect des obligations du fonctionnaire : neutralité et réserve.

Le caractère privé des messages devra être indiqué dans l'objet et les réponses ne devront être adressées qu'à l'expéditeur.

Les abus, qui pourraient être constatés seront sanctionnés dans le cadre des dispositions du chapitre « Sanctions » du Règlement.

La navigation sur le web

Navigateur

L'Administrateur peut limiter la durée de connexion, imposer des configurations de sécurité du navigateur, imposer des limites de taille au téléchargement de contenu par note de service.

Participation à des forums

La participation à des forums peut engager la responsabilité de la Ville de Castelnaudary. L'Utilisateur doit disposer des autorisations internes afin de s'exprimer au nom de la Ville de Castelnaudary et devra préalablement prendre contact avec la Direction Générale des Services de la ville de Castelnaudary.

Téléchargement de logiciels ou d'œuvres protégées

Le téléchargement de logiciels ou d'œuvres protégées, sans autorisation des ayants-droits, est de nature à engager la responsabilité de la Ville de Castelnaudary et comme tels sont strictement interdits. L'Administrateur se réserve 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.

Consultation de sites illicites

La consultation et le téléchargement du contenu de sites à caractère pornographique, pédophiles sont contraires aux bonnes mœurs et peuvent revêtir le caractère d'une infraction pénale. **Cette activité est strictement interdite.** L'Administrateur se doit d'informer de ces connaissances son Directeur et/ou le Directeur Général des Services qui se réservent le droit de dénoncer tout acte délictueux aux autorités, et ce sans préjudice de l'application des sanctions prévues au chapitre « Sanctions » du Règlement.

Consultation d'internet à des fins privées

La consultation de sites web à titre privé est autorisée dans la mesure où cette navigation n'entrave pas l'accès professionnel et qu'elle ne gêne pas la bonne marche du travail de l'utilisateur.

Il est précisé que le **téléchargement de fichiers musicaux au format mp3** ou tout autre format de compression ne rentrant pas dans l'accès professionnel et gênant la bonne marche du Système d'Information en raison de l'encombrement qu'il génère **est strictement prohibé.**

Intranet

Mise en place et fonctionnement de l'Intranet

L'Intranet fonctionne sous la responsabilité informatique de l'Administrateur et sous la responsabilité éditoriale du Directeur Général des Services. Aucun utilisateur ne peut introduire ou tenter d'introduire un élément de contenu sur l'Intranet sans l'autorisation de l'Administrateur et du Directeur Général des Services. Les utilisateurs pourront formuler toute suggestion à ces derniers quant au contenu ou fonctionnement de l'Intranet.

Données nominatives et personnelles

L'utilisateur sera averti avant diffusion sur l'Intranet de données nominatives et personnelles le concernant et en particulier de son image figurant au Trombinoscope. L'utilisateur pourra demander à l'Administrateur à avoir accès à ses données nominatives et personnelles et pourra demander à l'Administrateur de les rectifier.

Opérations de contrôle de sécurité

Les opérations de contrôle de sécurité se distinguent des opérations de maintenance en ce qu'elles portent sur la sécurité et le bon fonctionnement des équipements informatiques et sur la vérification du respect des dispositions du présent Règlement.

À ce titre, elles répondent à des finalités statistiques, de traçabilité, d'optimisation, de sécurité, ou de détection des abus.

Ainsi, la Collectivité se réserve le droit, notamment de :

- Vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne.
- Diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information.
- Vérifier les habilitations en place sur les postes de travail.
- Contrôler l'origine licite des logiciels installés.
- Conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information.
- Transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.
- En outre, en cas d'incident, la Collectivité se réserve le droit de :
- Surveiller le contenu des informations qui transitent sur son système d'information.
- Vérifier le contenu des disques durs des ressources du système d'information attribuées à ses Utilisateurs.
- Procéder à toutes copies utiles pour faire valoir ses droits.

Les opérations de contrôle ciblé d'un Utilisateur sont effectuées par une « prise en main à distance » ou sur site, en présence de l'Utilisateur devant son poste de travail informatique ou dûment appelé. Il est informé que dans ce cadre, les autorités concernées peuvent notamment être amenées à avoir accès à l'ensemble des informations relatives aux Utilisateurs (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail, ainsi qu'à ouvrir tout message figurant sur sa messagerie et à vérifier l'ensemble des connexions dudit Utilisateur.

Ces opérations de contrôle de sécurité relèvent des fonctions de l'Administrateur, qui a la charge de la qualité, de la protection et de la sécurité des équipements informatiques fournis aux Utilisateurs.

Les personnels relevant du service informatique (administrateur réseau ou système d'exploitation ou toute autorité spécialement « concernée ») sont tenus de respecter le secret professionnel, l'obligation de discrétion professionnelle et la confidentialité des informations auxquelles ils accèdent. Ils ne peuvent utiliser leurs droits d'accès étendus qu'à des fins strictement professionnelles.

En ce qui concerne l'usage des services Internet, il peut être contrôlé a posteriori et peut porter sur le temps de connexion par poste ou sur les sites les plus consultés par l'Utilisateur. En cas de perturbation induite par l'apparition intempestive d'alertes à la suite de tentatives d'infection des systèmes à l'aide de virus informatiques (malwares), l'Administrateur est autorisé à mener toutes les investigations qu'il jugera utiles aux fins d'éradiquer lesdits virus.

Si en cas d'opérations de contrôle, l'Administrateur identifie un faisceau d'indices laissant supposer qu'un Utilisateur met en cause les intérêts et la sécurité de la Collectivité, ou réalise une utilisation anormale, ou identifie un contenu illicite ou préjudiciable, il en informera sa hiérarchie.

Pour des raisons de sécurité des équipements informatiques de la Collectivité, tout matériel ou logiciel installé illicitement ou en violation du présent Règlement pourra être supprimé ou désactivé par l'Administrateur, dès le constat de leur présence sur le poste de travail ou autre matériel.

Place de l'Amicale des Retraités dans le Système d'Information

Outils d'information mis à disposition

L'Amicale des retraités de la ville de Castelnaudary disposera d'une adresse électronique et d'un répertoire au sein du Système d'Information.

L'Amicale des retraités gèrera son répertoire de manière autonome. L'Administrateur garantit à l'Amicale des retraités un accès permanent (sous réserve de la maintenance du Système d'Information et autres opérations de protection du Système d'Information) à ce répertoire par tous les utilisateurs.

Le répertoire peut être complété, sur proposition motivée, après autorisation préalable de la Direction Générale des Services, par des pages d'informations sur l'Intranet.

Règles de communication

L'Amicale des retraités devra dans sa communication au personnel de la ville de Castelnaudary :

- respecter les termes du présent Règlement et la protection des données personnelles,
- veiller au respect des dispositions de la loi sur la liberté de la presse,
- se limiter quant à l'objet de la communication à ce qui rentre dans le cadre de ses attributions,
- respecter les consignes de l'Administrateur en termes de format, de taille, des messages ou de pages intranet.

En cas de non-respect de ces dispositions, le Directeur Général des Services sur proposition de l'Administrateur pourra retirer l'autorisation après avoir préalablement entendu l'Amicale des retraités présenter ses explications.

Place des syndicats dans le Système d'Information

Outils d'information mis à disposition

Les délégués syndicaux disposeront par section syndicale représentative dans la collectivité d'une adresse électronique au nom de leur organisation syndicale et d'un répertoire au sein du Système d'Information.

Les délégués syndicaux gèreront leur répertoire de manière autonome. L'Administrateur garantit aux délégués syndicaux un accès permanent (sous réserve de la maintenance du Système d'Information et autres opérations de protection du Système d'Information) à ces répertoires par tous les utilisateurs.

Les répertoires peuvent être complétés, sur proposition motivée, après autorisation préalable de la Direction Générale des Services, par des pages d'informations sur l'Intranet.

Règles de communication

Les délégués syndicaux devront dans leur communication au personnel de la ville de Castelnaudary :

- respecter les termes du présent Règlement et la protection des données personnelles,
- veiller au respect des dispositions de la loi sur la liberté de la presse,
- se limiter quant à l'objet de la communication à ce qui rentre dans le cadre de leurs attributions,
- respecter les consignes de l'Administrateur en termes de format, de taille, des messages ou de pages intranet,
- Identifier leurs messages comme provenant d'un syndicat

Afin de bien identifier la nature des messages électroniques, les délégués syndicaux devront utiliser dans leur communication syndicale, la boîte aux lettres de leur organisation et non la boîte aux lettres dont ils disposent à leur nom personnel.

Les messages à caractère politique sont interdits. (Ex : appel à voter pour un candidat, ...)

En cas de non-respect de ces dispositions, le Directeur Général des Services sur proposition de l'Administrateur pourra retirer l'autorisation après avoir préalablement entendu les délégués syndicaux présenter leurs explications.

Mesures d'urgence et plan de reprise d'activité

L'Utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérieuse, la Collectivité peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la reprise de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'Utilisateur pourra être amené à la demande de la Collectivité à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure, notamment, le basculement sur un système informatique de relève, une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, déplacement sur des sites de secours tiers, etc.).

Sanctions

Le non-respect des dispositions du Règlement peut entraîner des sanctions disciplinaires.

Sanctions disciplinaires

Loi 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires. Loi dite loi Le Pors

Article 29 : *Toute faute commise par un fonctionnaire dans l'exercice ou à l'occasion de l'exercice de ses fonctions l'expose à une sanction disciplinaire sans préjudice, le cas échéant, des peines prévues par la loi pénale*

Il revient à l'autorité territoriale, à qui appartient le pouvoir disciplinaire, d'apprécier, sous le contrôle du juge administratif, si un acte ou un comportement peut être reconnu comme une faute disciplinaire susceptible de justifier une sanction. Exemple : devoir de neutralité, obligation de réserve, interdiction de messages à caractère raciste, éligieux, discriminatoire ou politique.

Affichage et formalités – Entrée en vigueur

Le Règlement est disponible sur l'intranet de la Ville dans les documents RH, rubrique « Droits et devoirs ».

Un exemplaire du présent Règlement est à disposition à l'Hôtel de Ville, à la Direction Générale des Services et dans chaque Direction de la Ville. Elle sera également remise à chaque agent nouvellement embauché ou changeant de poste et autorisé à utiliser le Système d'Information de la Ville de Castelnaudary.

La hiérarchie est chargée de s'assurer de la diffusion du Règlement en la remettant contre signature de prise de connaissance.

Ce Règlement entrera en vigueur le 1^{er} octobre 2023 après information du Conseil Municipal et avis du Comité Social Territorial.

A Castelnaudary le 1^{er} octobre 2023

Le Directeur Général des Services

Le Maire

Nicolas NAYRAL

Patrick MAUGARD