Charte d'utilisation des services numériques établie le 09/02/2026

Table des matières

Préambule

Les différents outils technologiques utilisés offrent aux utilisateurs une grande ouverture vers l'extérieur. Cette ouverture peut apporter des améliorations de performances importantes si l'utilisation de ces outils technologiques est faite à bon escient et selon certaines règles. L'usage des moyens numériques mis à disposition doit permettre de préserver le système d'information, le bon fonctionnement des services et les droits et libertés de chacun.

L'objectif de la présente charte informatique, document d'information et de référence, est donc de formaliser les règles légales et de sécurité relatives à l'utilisation de tous les outils d'information et de communication au sein de la collectivité.

Une mauvaise utilisation des différents outils technologiques peut entrainer des conséquences graves : risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, risque d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles ou non (virus, intrusions sur le système d'information, vols de données).

Chaque utilisateur doit avoir conscience qu'il joue un rôle actif dans ce contexte, et doit s'engager à respecter la présente charte.

Champ d'application

La présente charte s'applique à minima à l'ensemble des utilisateurs disposant d'un accès au système d'information par contrat, convention ou délégation, et notamment :

- Les agents municipaux et communautaires (titulaires, contractuels...)
- Les vacataires, les intérimaires
- Les stagiaires, apprentis ou équivalents
- Les élus
- Les employés de sociétés prestataires
- Les bénévoles, visiteurs, partenaires expressément autorisés, qui seraient amenés à utiliser les services numériques

Identifiants et mots de passe

Chaque utilisateur du réseau informatique se voit attribuer un compte auquel sont associés des moyens d'authentification (identifiant login/mot de passe, carte, clé...) Il est responsable de l'utilisation qui est faite de ce compte et il lui appartient donc de ne pas transmettre ses moyens d'authentification à une tierce personne. À cet effet, ses secrets d'authentification (mot de passe, code pin...) ne doivent être notés sur aucun support et sont incessibles, intransmissibles et personnels.

Chaque mot de passe doit obligatoirement être modifié à intervalle régulier, avoir un nombre de caractères suffisant, combinant minuscules, majuscules, caractères spéciaux et chiffres.

Les règles de renouvellement et de composition des mots de passe évoluent en fonction des normes de cybersécurité. La Direction des Services Numériques (DSN) les définit en conséquence et en informe les utilisateurs.

Un durcissement de l'authentification pourra être nécessaire pour les accès externes et/ou en mobilité impliquant l'installation d'une application spécifique de sécurité sur un équipement personnel ou l'utilisation d'un numéro de téléphone personnel pour l'envoi de code de confirmation unique par SMS.

Matériel informatique, téléphonique, audiovisuel et radio

L'utilisation des équipements est réservée à des fins professionnelles. Néanmoins, un usage personnel et ponctuel est toléré à des fins de consultation de sites/messageries Web/réseaux sociaux à condition que cela n'entrave pas le fonctionnement ni ne nuise à la sécurité des systèmes d'information.

La fabrication et L'utilisation des équipements numériques ont un impact environnemental significatif.

- Les équipements mis à disposition de chaque utilisateur sont de valeur, il convient d'en prendre soin pour prolonger au mieux leur durée de vie, ce qui s'inscrit dans la démarche de sobriété numérique engagée par la collectivité.
- L'utilisateur veillera à limiter autant que possible la consommation d'énergie des équipements en recourant au mode veille et en éteignant les équipements en fin de journée. C'est également à cette condition que les mises à jour essentielles seront installées sur les ordinateurs.

Les supports amovibles (clé USB, disque dur externe, etc.) sont parmi les premiers vecteurs de virus. Un même support amovible ne doit pas être connecté successivement sur un équipement personnel et professionnel. Des mesures de restriction d'usage des supports USB pourront être décidées en cas d'alertes de sécurité répétées.

En cas de dysfonctionnement, de blocage, de perte ou de vol d'équipement, les utilisateurs doivent en informer immédiatement le centre de services de la DSN et le DPO si des données personnelles sont concernées. Ils doivent par ailleurs assister la collectivité, dans toutes les démarches (déclaration d'assurance, dépôt de plainte, aide au diagnostic, notification auprès de la CNIL…) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

Accès au réseau

La connexion d'ordinateurs étrangers au parc sur le réseau interne (hors wifi invité) est interdite, sauf autorisation écrite de la DSN.

Télétravail, nomadisme

L'emploi d'ordinateurs portables, de smartphones ou de tablettes expose des informations potentiellement sensibles dont le vol ou la perte entraineraient des conséquences importantes sur les activités de l'organisation.

Lorsque ces matériels sont utilisés à l'extérieur, notamment dans le cadre de réunion ou d'intervention hors des locaux de la collectivité et à domicile (télétravail), les utilisateurs en assurent la garde et la responsabilité.

Les équipements nomades (ordinateurs portables, smartphones, tablettes...) sont mis à disposition pour un usage strictement professionnel et ne doivent en aucun cas être utilisés par des personnes ne faisant pas partie de la collectivité et/ou n'ayant pas signé la présente charte (tiers, famille...).

En termes de sécurité et de confidentialité, les utilisateurs sont soumis aux mêmes obligations que les utilisateurs restant sur site. Ils devront suivre toutes les prescriptions complémentaires qui leur seront signifiées.

Droit à la déconnexion

Le droit à la déconnexion garantit à tout utilisateur la possibilité de ne pas se connecter aux outils numériques mis à disposition, et de ne pas être contacté, ni de répondre à une sollicitation, en dehors de ses horaires et journées de travail.

Ce droit ne s'applique pas en cas de situation de crise ou exceptionnelle, de nécessité de continuité du service public et lors de périodes d'astreinte.

Messagerie

La messagerie est un vecteur important de propagation des virus et de « phishing » (technique utilisée par des cyber délinquants pour collecter des données personnelles). Il est en effet très simple de diffuser par courrier électronique un fichier attaché contenant un virus ou un lien Internet (url) pour inciter à télécharger un programme infecté. L'utilisateur s'engage à se tenir informé et à appliquer les consignes de sécurité d'usage de la messagerie diffusées par la DSN au travers des outils intranet.

L'utilisateur s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine, à la vie privée, aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou toute autre forme de discrimination.

Au même titre que pour le courrier papier ou le téléphone, chacun est responsable des messages envoyés et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues, des règles élémentaires de courtoisie et de bienséance et en conscience de l'impact carbone d'un message trop lourd ou trop largement diffusé.

Tout message envoyé ou reçu depuis votre messagerie professionnelle est supposé avoir un caractère professionnel, et à ce titre peut être ouvert par l'Autorité territoriale, sauf s'il est clairement identifié comme étant personnel (par exemple, avec l'indication "Personnel" ou "Privé" en objet) ou classé dans un répertoire "Personnel".

Internet

Des moyens techniques de filtrage d'accès limitent les possibilités de navigation sur Internet ; ils ne dégagent pas pour autant de ses responsabilités l'utilisateur qui s'engage :

- Lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine : pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine, à la violence à l'égard d'une personne, d'un groupe de personnes en raison de leur origine, de leur appartenance ou non à une ethnie, une nation, une race, une religion déterminée ou toute autre forme de discrimination.
- A ne pas télécharger, en tout ou partie, des données numériques soumises aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.)
- A ne pas télécharger des logiciels, des vidéos, des photos n'ayant pas de lien avec les fonctions ou les activités professionnelles.

Les administrateurs de la DSN peuvent procéder, dans le périmètre de leurs missions, encadrées par la charte des administrateurs, à tout moment, au contrôle des connexions entrantes et sortantes.

Supervision / Journaux de connexion

La DSN est responsable du bon fonctionnement des services numériques ainsi que de la sécurité globale du système d'information mis à disposition. Elle doit assurer une disponibilité maximale des différents moyens qu'elle met à la disposition des utilisateurs.

Ces préoccupations techniques l'amènent par exemple à surveiller l'encombrement des boîtes aux lettres, la saturation de l'accès commun à Internet, la volumétrie et la typologie des requêtes principales ainsi que l'espace disque des serveurs de stockage.

La DSN peut avoir accès à l'ensemble des composants matériels et logiciels du système d'information et ce à n'importe quel moment, sans avertissement, afin d'effectuer tout acte de protection et de bonne administration du système d'information.

La DSN s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent l'ensemble des activités effectuées par un utilisateur sur le système d'information. La DSN est la seule habilité à exploiter ces informations, dont la durée de conservation, conformément aux recommandations de la CNIL, est déterminée de manière proportionnée à la finalité poursuivie et n'excède en aucun cas 1 an.

Dans le cadre de l'assistance d'un utilisateur, avec le consentement de l'agent, les administrateurs de la DSN peuvent être amenés dans le cadre de leurs fonctions à accéder à des informations privées à des fins de diagnostic et d'administration.

Chaque administrateur technique de la DSN s'engage au travers d'une charte spécifique « des administrateurs du SI ». Cette charte est destinée à préciser les devoirs et les droits de toutes personnes chargées de la gestion de ressources informatiques, de moyens de télécommunication ou de logiciels. Notamment, y figure l'obligation du secret professionnel afin de préserver la confidentialité des informations.

Départ d'un utilisateur

Tout utilisateur, lors de la cessation de son activité au sein de la collectivité, perd immédiatement son habilitation à utiliser les systèmes d'information internes.
Il doit (ou à défaut son supérieur hiérarchique) :

- Prévenir la DSN de son départ
- Restituer tous les matériels mis à sa disposition,
- Effacer de son poste de travail et des serveurs tous ses éventuels fichiers, messages et données privés.

Il ne peut effectuer une copie de son travail professionnel qu'après autorisation écrite de son supérieur hiérarchique dûment habilité.

Sensibilisation et Usage lié à l'Intelligence Artificielle (IA)

L'utilisation des IA génératives peut conduire à divulguer des informations confidentielles en exfiltrant des données professionnelles. En outre, les utilisateurs peuvent être amenés à y intégrer des données à caractères personnel.

Chaque utilisateur pourrait être tenu responsable de la fuite de ces données.

Par conséquent, chaque utilisateur s'engage à ne pas intégrer de documents ou de données de la collectivité dans les outils tiers et extérieur aux systèmes d'informations basés sur l'intelligence artificielle, en dehors de ceux désignés par la DSN.

Toute utilisation d'outils ou de services intégrant de l'IA doit se conformer aux principes et obligations définis dans la **charte d'usage de l'Intelligence Artificielle.**

Protection des données personnelles

Le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à la libre circulation de ces données (RGPD) et la législation française en vigueur dans le domaine de la protection des données, notamment la loi « informatique et Libertés » telle que modifiée par l'ordonnance n°2018-1125 du 12 décembre 2018, visent à protéger les personnes physiques à l'égard du traitement de leurs données personnelles.

La politique générale de protection des données à caractère personnel de notre collectivité prévoit les modalités d'utilisation de ces données.

Tous les traitements comprenant des données personnelles, y compris lorsqu'elles résultent de croisement ou d'interconnexion de traitements préexistants, sont soumis à la réglementation en vigueur.

Seuls les traitements effectués à titre totalement privé, comme la constitution d'un agenda personnel, échappent à cette réglementation.

La mise en place d'une application non connue de la DSN, à usage professionnel contenant des données personnelles (sur Excel par exemple), doit être évitée au maximum et dans le cas contraire, faire l'objet d'une validation de la hiérarchie et être inscrite au registre de traitement des données, après avis du référent RGPD et du délégué à la protection des données (DPO).

Toute violation de données personnelles doit être signalée le plus rapidement possible au DPO ou au référent RGPD de sa direction.

Par ailleurs, chaque utilisateur dispose d'un droit d'accès, de rectification et d'effacement relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information. Ces droits s'exercent auprès du DPO.

Opposabilité et Manquement à la charte

La présente Charte a été soumise à l'avis :

- Des Comités Sociaux Territoriaux de la Ville en date du JJ/MM/AAAA
- Des Comités Sociaux Territoriaux de la CUGR en date du JJ/MM/AAAA
- Des instances du CCAS en date du JJ/MM/AAAA
- Des instances de la CAISSE DES ECOLES en date du JJ/MM/AAAA

Elle est rendue opposable dès son annexion au règlement intérieur de la collectivité.
Le non-respect des règles édictées sera signalé à la hiérarchie.

Tout manquement aux règles et mesures définies par la présente charte est susceptible d'engager la responsabilité pénale et/ou civile de l'utilisateur et d'entrainer des sanctions administratives à son encontre.

Glossaire

- Antivirus : logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants
- CNIL : Dans l'univers numérique, la Commission nationale de l'informatique et des libertés (CNIL) est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.
- Cyber délinquant : Celui qui utilise l'informatique et éventuellement Internet pour commettre des faits de délinquance
- Cybersécurité : La cybersécurité désigne Les technologies pour protéger son patrimoine informationnel, protéger les personnes concernées des atteintes à leurs données.
- Données personnelles : Les données à caractère personnel sont des informations qui permettent sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

- DPO : Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.
- Filtrage internet : Le filtrage de contenu web est une technique qui bloque et filtre l'accès à des contenus web inappropriés ou dangereux.
- IA générative : L'IA générative ou l'intelligence artificielle générative fait référence à l'utilisation de l'IA pour créer de nouveaux contenus, comme du texte, des images, de la musique, de l'audio et des vidéos.
- Lien internet (url) : Adresse d'un site ou d'une page hypertexte sur Internet (ex. http://www.reims.fr).
- Mise à jour : action qui consiste à mettre à niveau un outil ou un service informatique en téléchargeant un nouveau programme logiciel
- Nomadisme : Le nomadisme numérique désigne toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité.
- Phishing (hameçonnage) : méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.
- RGPD : Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE). Il est entré en application le 25 mai 2018. Il responsabilise les organismes publics et privés qui traitent leurs données.
- Sobriété numérique : La sobriété numérique est un terme qui désigne les efforts faits afin de chercher la modération dans nos productions et nos usages numériques. Concrètement, il s'agit de chercher à réduire volontairement à la fois la quantité d'équipements numériques, leurs usages ainsi que les ressources qu'ils consomment, dans le but de répondre à nos besoins sans dégrader les conditions écologiques de la planète.
- Supervision informatique : Aussi appelée « monitoring du système informatique », elle vise à contrôler et à surveiller le système informatique de l'entreprise afin de s'assurer qu'il fonctionne bien.
- Système d'information (SI) : c'est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs
- Télétravail : Le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication (article L. 1222-9 du code du travail). Le télétravail est donc une forme de nomadisme numérique.
- Virus informatique : Un *virus informatique* est une application malveillante ou un logiciel utilisé pour exercer une activité destructrice sur un appareil ou un réseau local.