



DÉLIBÉRATION DU CONSEIL MUNICIPAL DE SCIENTRIER

Envoyé en préfecture le 08/08/2025

Reçu en préfecture le 08/08/2025

Publié le

ID : 074-217402627-20250626-029_2025-DE



Délibération n°029 /2025

OBJET : Adoption d'une charte relative à l'usage des outils numériques et à la protection des données personnelles

L'an deux mil vingt-cinq, et le vingt-six juin à vingt heures trente minutes, le Conseil Municipal s'est réuni en salle des commissions à SCIENTRIER, sur convocation adressée à tous ses membres, le dix-neuf juin précédent, par Madame Patricia DEAGE, Maire en exercice de la Commune de SCIENTRIER.

Conseillers en exercice : 11

Présents : 8

BARBIER Sarah, BRANTUS Michel, BRON Isabelle, DEAGE Patricia, DESALMAND Stéphane, DESALMAND Nadège, FLOQUET Sandra, PIEUCHOT Sophie

Absents : BERARD Nicolas, LAMBERT Adrien

Absents excusés : DAKIN-GARVAL Sylvain

Procuration : BRON Isabelle pour DAKIN-GARVAL Sylvain

Secrétaire de séance : DESALMAND Nadège

Madame le Maire indique que la mise en place d'une charte informatique au sein des services municipaux revêt une importance particulière. En effet, les outils numériques occupent aujourd'hui une place centrale dans le fonctionnement des collectivités, qu'il s'agisse de la gestion des courriels, des logiciels métiers, de l'accès aux données administratives ou encore des échanges dématérialisés avec les partenaires institutionnels et les administrés. Il est donc essentiel de disposer d'un cadre clair et partagé fixant les règles d'utilisation des équipements et ressources informatiques mis à disposition des agents communaux.

Cette charte a pour vocation de sécuriser l'usage des outils numériques, de prévenir les usages inadaptés ou à risque et de rappeler à chacun ses responsabilités en matière de protection des données personnelles et de respect de la réglementation en vigueur. Elle participe également à garantir la continuité et la qualité du service public rendu à la population.

Madame le Maire précise par ailleurs que, comme l'ensemble des communes membres de la Communauté de Communes Arve et Salève, la commune de Scientrier bénéficie de l'accompagnement d'un prestataire extérieur spécialisé pour toutes les questions relatives au Règlement Général sur la Protection des Données (RGPD). Chaque année, ce prestataire réalise un suivi et un accompagnement auprès de la collectivité afin de veiller au respect des obligations réglementaires en matière de protection des données personnelles et de sécurité numérique.

C'est dans ce cadre que le prestataire a recommandé la formalisation et l'application d'une charte informatique destinée à accompagner les agents dans la bonne utilisation des équipements et services numériques municipaux. Ce document vient ainsi renforcer le cadre existant et constitue un outil de

sensibilisation et de prévention indispensable pour un usage responsable
sein de la collectivité.

Madame Le Maire propose à l'assemblée délibérante l'adoption d'un charte informatique :

Article 1. INTRODUCTION

Ce texte est avant tout un code de bonne conduite.

Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des règles minimales de courtoisie et de respect d'autrui.

Les salariés, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens de communication mis à leur disposition et à les utiliser.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources.

Pour tout renseignement complémentaire, vous pouvez vous adresser à : rh@scientrier.fr

Article 2. DEFINITIONS

On désignera de façon générale sous le terme « ressources informatiques », les moyens informatiques de calcul ou de gestion ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entreprise (PC portables ou fixes, tablettes, téléphones portables ou fixes, logiciels, réseaux, serveurs, messagerie, internet etc.).

On désignera par « services informatiques », la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : Web, messagerie, forum...

On désignera sous le terme « utilisateur », les personnes internes ou externes ayant accès ou utilisant les ressources informatiques et services Internet [(élus, agents, mandataires sociaux, salariés, intérimaires, stagiaires, partenaires, consultants, etc.)]

On désignera sous le terme « entité » les entités administratives créées par la Mairie de Scientrier pour l'accomplissement de ses missions, telles que les services, agences et directions administratives.

Article 3. ACCES AUX RESSOURCES INFORMATIQUES ET SERVICES INFORMATIQUES

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

L'accès à des fins personnelles peut toutefois être toléré, dans un cadre d'utilisation raisonnable (par exemple : lors des pauses déjeuners ou en dehors des heures travaillées), dès l'instant que cette utilisation ne perturbe pas l'activité professionnelle des autres utilisateurs.

Les utilisateurs sont invités à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de message à caractère personnel.

L'activité professionnelle est celle prévue par les statuts de la Mairie de Scientrier, à savoir :

- assurer la gestion administrative, technique et financière de la commune ;

- mettre en œuvre les politiques publiques locales dans des domaines tels que l'urbanisme, les affaires scolaires, la voirie, l'environnement, l'action sociale et les services à la population.

L'outil informatique constitue, à ce titre, un support indispensable au traitement et à la sécurisation des données publiques et personnelles, à la communication interne et externe, ainsi qu'à la gestion quotidienne des services municipaux et des relations avec les administrés.

L'utilisation des ressources informatiques partagées et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation.

Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Toute autorisation prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée.

La Mairie de Scientrier pourra en outre prévoir des restrictions d'accès spécifiques à son organisation : carte à puce d'accès ou d'authentification, filtrage d'accès sécurisé...

Article 4. REGLES D'UTILISATION, DE SECURITE ET DE BON USAGE

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès.

Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de son entité. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles. En particulier, il doit appliquer les recommandations de sécurité de la Mairie de Scientrier ;

- Il doit assurer la protection de ses informations et de leurs échanges et il est responsable des droits qu'il donne aux autres utilisateurs. Il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels mis à sa disposition ;
- Il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater ;
- Il doit s'adresser à la Direction Générale et obtenir leur validation préalable pour toute installation de logiciel ou autre programme ;
- Il choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers (cf. politique de mot de passe : annexe p.10).
L'utilisation d'un gestionnaire de mot de passe est recommandée ;
- Il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage ;
- Il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité ;
- Il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier le ou les fichiers contenant des informations d'identification ;
- Il ne doit pas quitter son poste de travail ni ceux en libre-service sans se déconnecter en laissant des ressources ou services accessibles.
- Assurer une gestion des mots de passe en conformité avec les règles RGPD (voir la fiche d'infographie) et ne pas :
 - 1- Communiquer son mot de passe à autrui.
 - 2- Stocker ses mots de passe dans un fichier en clair, sur un papier ou dans un lieu facilement accessible par d'autres personnes.
 - 3- Enregistrer ses mots de passe dans son navigateur sans mot de passe maître.
 - 4- Utiliser des mots de passe ayant un lien avec soi (nom, date de naissance, etc.).
 - 5- Utiliser le même mot de passe pour des accès différents.
 - 6- Conserver les mots de passe par défaut.
 - 7- S'envoyer par e-mail ses propres mots de passe.

Article 5. CONDITIONS DE CONFIDENTIALITE

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.

Les utilisateurs s'engagent, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin de protéger la confidentialité des informations auxquelles ils ont accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir des informations.

Article 6. RESPECT DE LA LEGISLATION CONCERNANT LES LOGICIELS

Il est strictement interdit d'effectuer des copies de logiciels commerciaux ainsi que d'installer des logiciels piratés pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin par le responsable de l'entreprise. Par ailleurs, l'utilisateur ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel.

Article 7. PRESERVATION DE L'INTEGRITE DES SYSTEMES INFORMATIQUES

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques...

Tout travail de recherche ou autre, risquant de conduire à la violation de la règle définie dans le paragraphe précédent, ne pourra être accompli qu'avec l'autorisation du directeur technique et dans le strict respect des règles qui auront alors été définies.

L'utilisateur devra notamment être particulièrement vigilant concernant les tentatives de spam, phishing ou autre ransomware. Il ne faut donc jamais ouvrir de mail, pièce jointe, lien etc. d'expéditeur dont on aurait des doutes sur l'origine ou sur les intentions.

Article 8. USAGE DES SERVICES INTERNET (Web, Messagerie, Forum)

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect des principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

En particulier :

- Il ne doit pas se connecter, ou essayer de se connecter, sur un serveur autrement que par les dispositions prévues par ce serveur, ou sans y être autorisé par les responsables habilités ;
- Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- Il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers,
- Il ne doit pas utiliser internet de manière à gêner l'accès des autres utilisateurs (par exemple avec le streaming ou les vidéos en ligne),
- Il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,

- Il ne doit pas déposer des documents sur un serveur sauf si ce serveur est autorisé par les responsables habilités,
- Il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions...
- Il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à la Mairie de Scientrier ;
- Il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire ;
- Il doit fournir à une personne invitée dans les locaux de la Mairie de Scientrier l'accès au réseau « invité » du portail d'accès au wifi.

La Mairie de Scientrier ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne sera pas conforme à ces règles.

Article 9. ANALYSE ET CONTRÔLE DE L'UTILISATION DES RESSOURCES

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

Si la Mairie constate une faute (notamment une violation des présentes directives ou de toute autre politique, procédure, directive ou instruction de la Mairie) ou un acte criminel impliquant des ressources de la Mairie, les fichiers ou informations contenus dans celles-ci pourront être utilisés pour documenter cette faute et pourront être divulgués aux autorités compétentes, à l'intérieur et à l'extérieur de la Mairie et l'utilisateur sera passible d'une action disciplinaire.

Article 10. RAPPEL DES PRINCIPALES LOIS FRANCAISE

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique :

- La loi du 06 Janvier 1978 dite « informatique et liberté » et le règlement n°2016/679 du 14 Juin 2016 dit Règlement Général sur la Protection des Données (RGPD) (<http://www.cnil.fr>);
- Pour la fonction publique, Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, imposant notamment les obligations de réserve, de discrétion et de secret professionnel des agents publics ;
- La législation relative à la fraude informatique (articles 323-1 à 323-7 du Code Pénal – Livre III – Titre II – Chapitre III) : Lien vers le Code Pénal
- La législation relative à la propriété intellectuelle : lien vers le Code de la Propriété Intellectuelle
- La loi du 04 Août 1994 relative à l'emploi de la langue française : Lien vers la Loi relative à l'emploi de la langue française ;
- La législation applicable en matière de cryptologie : Lien vers la législation applicable en matière de cryptologie ;

Tout litige qui pourrait résulter de cette charte devra dans un premier temps être réglé de façon amiable entre les parties.

Si aucun accord amiable ne peut être trouvé, le litige sera alors traité par le tribunal compétent.

Article 11. DONNEES PERSONNELLES

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que le Règlement Général sur la Protection des Données (RGPD), définissent les conditions dans lesquelles des traitements de données personnels peuvent être opérés. Elle institue au profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers.

Il est rappelé aux utilisateurs que les traitements de données à caractère personnel doivent être déclarés au sein du registre de traitements de données de la Mairie de Scientrier.

Les utilisateurs souhaitant réaliser des traitements relevant du RGPD sont invités à prendre contact avec le DPO de la Mairie de Scientrier (dgs@scientrier.fr) avant d'y procéder.

Article 12. SANCTIONS

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Le fonctionnaire ou l'agent contractuel qui ne respecte pas cette charte fera l'objet de poursuite disciplinaire selon la réglementation en vigueur.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

Article 13. APPLICATION ET FIN D'APPLICATION

La présente charte s'applique à l'ensemble des agents de la commune de Scientrier tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques de l'entreprise ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré par l'entreprise.

Elle sera annexée, à titre d'information, aux contrats de travail conclus avec les salariés qui auront accès au système informatique de leur entité.

Lorsqu'un salarié quitte l'entreprise, il a l'obligation de détruire toutes les données contenues sur son PC.

Après en avoir délibéré, et considérant l'intérêt de ce document pour la collectivité et ses agents, il est proposé au Conseil Municipal :

- **D'ADOPTER** la charte informatique jointe en annexe.

Ainsi fait et délibéré,

Les jours, mois et an que susdit
Pour extrait conforme
Le Maire
Patricia DEAGE

Le Secrétaire,

