Département de l'ALLIER

Arrondissement de MONTLUCON

C O M M U N E de DOMÉRAT

Nbre de conseillers municipaux en exercice : 29

Présents à la séance : 22
Votants : 28

Date de l'affichage de la convocation :

20 juin 2023

Date de l'affichage à la porte de la Mairie de la liste des délibérations :

29 juin 2023

OBJET *: Ville de Montluçon : modification de la charte informatique.*

230627-02

Ville de DOMERAT
03410 DOMERAT
Le 29 JUIN 2023
Contrôle de légalité FAST

RÉPUBLIQUE FRANCAISE

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS DU CONSEIL MUNICIPAL

L'an deux mille vingt-trois, le 27 juin, à 19 heures, le conseil municipal de la commune de DOMÉRAT, assemblé au lieu habituel de ses séances, au nombre de vingt-deux, en session ordinaire, sous la présidence de madame Pascale LESCURAT, maire, en suite de la convocation faite par madame le maire de ladite commune, le 20 juin 2023.

Présents : Mme LESCURAT..Mr DE SOUSA..Mmes. JOUANNIN..PIRES..Mr DUFLOUX..Mme BERGERON..Mrs LIMOGES..HAMELIN..MALBET..Mmes DELERIS.. COULANGEON..BERRUER..Mr LACAUX..Mme LAFAYE.. Mrs PINHEIRO.OSTERTAG..Mme DUCEAU..Mrs DELEAU.. LEFEBRE..Mmes CHIROL..AURAT..CLEMENSAT.

Secrétaire de séance : Mr SURLEAU.

Ayant donné mandat de procuration : Mr BOY à Mme JOUANNIN, Mme FAUCHARD à Mme LESCURAT, Mr LUQUET à Mr PINHEIRO, Mme MATHIAUD à Mme DUCEAU, Mr RICHOUX à Mr DUFLOUX, Mr DEQUAIRE à Mme CLEMENSAT.

Le procès-verbal de la séance du 2 mai 2023 est approuvé (date de publication : 29 juin 2023).

Il est rappelé à l'assemblée la délibération du 15 décembre 2016 approuvant la signature d'une convention de mutualisation informatique avec la ville de Montluçon et Montluçon communauté ainsi que d'une charte précisant les droits et obligations de tous les usagers du système informatique ainsi mutualisé.

Ce document a été actualisé afin de prendre en compte la nouvelle règlementation en vigueur en termes de protection des données à caractère personnel (RGPD).

Il est proposé à l'assemblée d'approuver la nouvelle charte applicable à tous les utilisateurs de la ville de Domérat conformément au document ci-annexé qui sera soumis au comité social territorial lors de sa séance du 26 juin prochain.

Le conseil municipal, après délibération et à l'unanimité,

APPROUVE la nouvelle charte conformément au document ci-annexé.

.../...

Pour extrait conforme au registre,
Légalement signée par :

Pascale LESCURAT,
Maire de Domérat.

Guillaume SURLEAU,
Secrétaire de séance.

Date de publication sur le site internet : 29 juin 2023

Conseil municipal du 27/06/2023

CHARTE DE BONNE PRATIQUE DE L'INFORMATIQUE DANS LA COLLECTIVITE

Ville de
DOMÉRAT

Table des matières

ARTICLE 1 - PREAMBULE

La présente charte, approuvée lors du conseil municipal du 15 décembre 2016, rappelle les règles d'utilisation des moyens informatiques et téléphoniques de la commune de Domérat afin de favoriser un usage optimal de ces ressources en termes de sécurité, de confidentialité, de performance, de respect de la réglementation et des personnes.
Ce règlement s'applique à l'ensemble des agents, tous statuts confondus, aux élus, stagiaires, visiteurs, et plus généralement à tous les utilisateurs des moyens informatiques et téléphoniques de la commune de Domérat.

Protection des données à caractère personnel

Ce règlement a également pour objet de sensibiliser les utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer.

La Ville de Domérat a désigné un Délégué à la Protection des Données à caractère personnel (DPO). Ce dernier a pour mission de veiller au respect des dispositions du Règlement Européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et communément appelé Règlement Général sur la Protection des Données (RGPD).

Les utilisateurs sont au cœur de la protection des données à caractère personnel, et par conséquent des libertés et de la vie privée des personnes concernées.

Les utilisateurs s'engagent par le respect de la présente charte, à respecter les principes fondamentaux de la protection des données à caractère personnel, à savoir notamment la minimisation de la collecte et la préservation de la confidentialité, de l'intégrité et de la sécurité des données à caractère personnel. Compte-tenu du caractère sensible de certaines données à caractère personnel traitées, les utilisateurs se doivent de faire preuve de la plus grande vigilance possible concernant la protection des données. Le DPO se tient à la disposition des utilisateurs qui souhaiteraient disposer d'informations ou de conseils complémentaires relatifs à la protection des données à caractère personnel.

Les utilisateurs sont informés que les données à caractère personnel les concernant sont conservées par la Ville de Domérat pendant toute la durée de leur activité au sein de la collectivité et durant les délais en vigueur en matière de prescription.

Conformément à la loi, les utilisateurs sont informés qu'ils disposent d'un droit d'accès et de rectification relatif à l'ensemble des informations les concernant.

ARTICLE 2 - DEFINITIONS

On désignera de façon générale sous le terme « moyens informatiques», les ressources informatiques de calcul ou de gestion locales, nomades ou non, mis à disposition par la ville de Domérat pour l'exercice de l'activité professionnelle, ainsi que celles auxquelles il est possible d'accéder à distance, directement ou en cascade, à partir du réseau administré ou utilisé par la commune de Domérat. On désignera par «moyens téléphoniques», tous les téléphones fixes ou portables, radiotéléphones, assistants personnel, fax modems mis à disposition par la ville pour l'exercice de l'activité professionnelle.
On désignera par «services Internet/Intranet», la mise à disposition par des serveurs locaux ou distants, de moyens d'échanges et d'informations diverses : site web, messagerie, forum...

L'activité professionnelle est celle qui est nécessaire, utile, dépendante ou complémentaire à l'activité des services municipaux, quelle qu'en soit la nature.

ARTICLE 3 - ACCES AUX RESSOURCES INFORMATIQUES, SERVICES INTERNET/INTRANET ET MOYENS TELEPHONIQUES

Le droit d'accès aux ressources informatiques et de télécommunications de la collectivité est conditionné par l'engagement écrit de l'utilisateur à respecter la charte informatique de la ville de Domérat. Cet engagement est matérialisé par la signature du formulaire d'acceptation de la charte figurant en annexe. Les accès informatiques sont personnels et incessibles.

3.1 UTILISATION DES RESSOURCES :

Les ressources informatiques, l'usage des services Internet/Intranet et du réseau pour y accéder, ainsi que les moyens téléphoniques, sont mis à disposition des utilisateurs, tels que définis à l'article 5 de la présente charte, pour l'exercice des activités de la commune de Domérat ou des services offerts à la population, voire des prestations demandées par la commune de Domérat à ses prestataires, même occasionnels (ex : stagiaires).
Toutefois, il est admis qu'un usage raisonnable et limité des ressources à des fins personnelles peut être toléré, à la condition expresse de respecter les dispositions de la présente charte. Cet usage personnel des ressources ne pourra être qu'occasionnel et limité, dans le temps et par son objet.

3.2 DOCUMENTS PRIVES ET PROFESSIONNELS :

Il est rappelé que les moyens apportés par la collectivité sont destinés principalement à l'exercice des fonctions de chaque agent dans le cadre de son activité professionnelle.

L'utilisateur veillera à distinguer clairement les documents, courriers, messages, etc. qu'il considère comme personnels, des documents professionnels, notamment en les rangeant dans des dossiers distincts nommés « PRIVE », et/ou en faisant figurer « PRIVE » en tête du nom des documents et de l'objet des courriels.
Tout document ou courriel ne respectant pas cette règle sera considéré comme professionnel.

3.3 RESPONSABILITES :

L'utilisateur est informé que sa propre responsabilité, celle de son chef de service, et la responsabilité de la commune de Domérat peuvent être engagées civilement et pénalement du fait de son comportement. Il veillera donc à respecter les lois et règlements en vigueur, notamment ceux mentionnés l'article 6, ainsi que les règles d'utilisation de sécurité et de bon usage décrites dans la présente charte.

3.4 ABUS ET CONTROLES :

L'utilisateur est informé que tout abus de l'utilisation non professionnelle pourra faire l'objet de sanctions. De ce fait, il reconnaît avoir été averti que le système d'information de la commune de Domérat fait l'objet de surveillance constante (serveurs, réseaux, postes de travail, téléphones, logiciels, virus), et qu'en cas de comportement suspect, certains équipements pourront être soumis à une surveillance particulière, notamment sur les volumes d'informations traitées (enregistrement, téléchargement), les durées anormales d'utilisation, les connexions à des sites internet prohibés ou les tentatives d'intrusions, par exemple.

Ainsi sont conservées de manière automatique durant une période de 6 mois les informations suivantes :

- l'adresse (appelée URL, par exemple http://www.agglo-montlucon.fr/) et l'heure de toute connexion à un site web depuis un ordinateur (identifié par une adresse IP telle que 10.1.100.XX) utilisant le réseau de la ville
- une copie de tout courrier électronique réceptionné et émis par le serveur de messagerie de la ville, y compris les courriels non sollicités (SPAM). Ces derniers sont écartés par des procédés de filtrage de la liste des messages délivrés aux agents. Néanmoins, les agents reçoivent régulièrement des courriels dans la boîte « courriers indésirables » intitulés « MailinBlack», qui permettent de récupérer les messages écartés par le filtrage anti-spam.

La gestion de ces données est faite dans le respect de la loi « Informatique et Libertés » du 6 janvier 1978 modifiée et du Règlement Général sur la Protection des Données du 27 avril 2016, qui prévoient, pour toute personne, un droit d'accès et de rectification aux données qui la concernent, ayant fait l'objet d'un traitement informatique. L'exercice de ce droit se fait par la voie hiérarchique.

3.5 MESURES CONSERVATOIRES ET SANCTIONS :

Tout utilisateur ne suivant pas les règles et obligations rappelées dans cette charte pourra se voir, par mesure conservatoire, suspendre l'accès aux ressources informatiques, téléphoniques, ou à certains services (internet, messagerie…).

En cas de manquement grave et d'intention manifeste de nuire au bon fonctionnement des ressources ou à l'activité des services, il sera passible de sanctions disciplinaires proportionnelles à la gravité des manquements constatés.

Tout utilisateur n'ayant pas respecté les lois pourra être poursuivi civilement et/ou pénalement.

3.6 PRISE DE MAIN ET OBSERVATION A DISTANCE :

Le service informatique dispose d'outils de prise de main à distance qui sont généralement employés pour dépanner les utilisateurs, en leur montrant directement les manipulations qu'ils ont à faire. Ces prises de main et observations à distance se feront toujours avec l'accord préalable de l'intéressé : il est averti par un message à l'écran qu'il doit valider pour que la prise de main à distance ou l'observation puisse démarrer.

3.7 ABSENCE DE L'AGENT :

En cas d'absence de l'agent, la continuité du service doit être assurée. L'agent doit veiller à ce que le service puisse accéder aux documents, logiciels et dossiers indispensables à l'activité (transmission des documents et dossiers aux collègues, ou mise à disposition dans un dossier partagé, création de comptes pour accéder aux applications, à l'exclusion de toute communication de mots de passe personnels). Si l'absence est imprévue (maladie, accident), le supérieur hiérarchique pourra demander au service informatique l'accès à l'espace de travail de l'agent. En cas de départ définitif ou de mutation, le successeur récupère les documents de travail ainsi que les messages d'ordre professionnel, à l'exception des documents et messages privés (voir paragraphe Documents privés et professionnels).

ARTICLE 4 - REGLES D'UTILISATION, DE SECURITE ET DE BON USAGE

Tout utilisateur est responsable du bon usage des équipements mis à sa disposition. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale.
L'utilisation de ces ressources doit être rationnelle et loyale afin d'éviter leur saturation ou leur détournement à des fins personnelles.

En particulier, l'utilisateur doit appliquer les recommandations suivantes :

4.1 SECURITE DES DONNEES ET DU RESEAU

4.1.1 Mots de passe :

Il convient de s'identifier clairement et utiliser des mots de passe pour protéger l'accès à ses matériels et programmes. Ces mots de passe ne doivent pas être communiqués ni notés sur des supports accessibles à autrui, ils ne doivent pas être faciles à deviner par une personne mal intentionnée (pas de prénoms ou dates de naissance de proches, par exemple). Ils doivent comporter au moins 8 caractères, et devront être changés au moins une fois par an, en évitant de reprendre ceux qui ont déjà été utilisés.
Pour des raisons de sécurité, le service informatique se réserve le droit d'imposer un changement régulier des mots de passe.
Les mots de passe sont personnels et chaque utilisateur est responsable de l'utilisation qui peut en être faite. L'emploi de mots de passe communs à plusieurs personnes est interdit. Néanmoins, cette disposition ne s'applique pas lorsque les comptes ou les ordinateurs sont liés à une fonction ou à une structure (exemple : messagerie d'un service, guichet : Accueil par exemple).

Seules les personnes du service informatique peuvent exceptionnellement être amenées à utiliser un mot de passe d'un utilisateur, avec son accord, pour résoudre un problème que ce dernier leur aura signalé.

L'utilisateur ne communiquera aucun mot de passe au téléphone s'il n'est pas absolument sûr de l'identité et de l'habilitation de son interlocuteur. En cas de doute, il devra rappeler la personne au service informatique (numéro interne), pour poursuivre l'opération.

4.1.2 Usurpation d'identité :

Ne pas tenter de masquer sa véritable identité ou d'usurper l'identité d'une autre personne pour essayer d'accéder à ses informations ou ses traitements.

Les courriels sont notamment protégés par le secret de la correspondance. Nul ne peut en prendre connaissance sans autorisation de l'émetteur ou du destinataire, à l'exception d'un juge d'instructions ou d'un officier de police judiciaire qui peut, en cas de plainte, procéder à la saisie des données nécessaires à la manifestation de la vérité.

Il convient de signaler au service informatique toute tentative d'accès anormal à son poste de travail et, de façon générale, toute anomalie que l'on peut constater.

4.1.3 Données d'autrui :

Ne pas tenter de lire, modifier, copier ou détruire des données autres que les siennes. En particulier, ne pas modifier de fichiers contenant des informations comptables ou d'identification, ni tenter de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées, exception faite des données diffusées dans des dossiers publics ou partagés qui sont clairement identifiés.

Il est expressément rappelé qu'accéder sans autorisation à des informations d'autres utilisateurs, les copier, les divulguer, les modifier ou les effacer, peut être sanctionné pénalement.

4.1.4 Informations confidentielles – Conformité RGPD :

Ne pas divulguer d'informations confidentielles, notamment par téléphone, à des tiers qui ne doivent pas les connaître. En particulier, les traitements ou fichiers concernant des données à caractère personnel (nom, numéro…) doivent faire l'objet d'une déclaration dans le registre des traitements de la collectivité. Les modalités de ces déclarations sont définies par le DPO. Ces déclarations stipulent notamment les finalités exactes des traitements, la liste des destinataires des diverses informations, leur durée de conservation, ainsi que les mesures de sécurité mises en oeuvre…

Le DPO de la collectivité accompagne les services dans cette démarche.

Le RGPD et la loi du 20 juin 2018 relative à la protection des données personnelles fixent un ensemble de contraintes pour ces traitements : respect des finalités et des durées de conservation déclarées, information des personnes concernées, qui ont aussi un droit d'accès et de rectification aux données les concernant, accès sécurisé aux données et obligation de sauvegardes.

Les fichiers non automatisés (papier) dont les informations proviennent ou sont appelées à être enregistrées dans ces traitements, sont soumis aux mêmes contraintes, et doivent donc être utilisés avec les mêmes précautions.

4.1.5 Accès aux postes de travail :

Ne pas laisser des ressources ou services accessibles à des tiers en cas d'absence du poste de travail ; mettre l'ordinateur en veille ou verrouiller le poste avant de s'absenter, même momentanément.
La mise en fonction automatique de l'économiseur d'écran, au bout de quelques minutes d'inactivité, est vivement recommandée, avec saisie obligatoire d'un mot de passe pour quitter la veille.
Restreindre l'accès aux locaux accueillant les traitements sensibles, notamment ceux soumis à la conformité RGPD. Veiller à ce que les impressions ou sauvegardes contenant des informations sensibles ou nominatives (noms, adresses, photos de personnes…) ne soient pas accessibles à des personnes non autorisées (conservation obligatoire sous clé dans les bureaux recevant du public). Egalement, tout support (papier, CDROM…) doit être rendu illisible avant mise au rebut.

4.1.6 Sauvegardes :

Les données professionnelles doivent être stockées sur les serveurs.
Les serveurs sont sauvegardés automatiquement toutes les nuits.
Les données personnelles doivent être stockées sur le disque dur du Pc de l'utilisateur dans un dossier nommé « PRIVE ».
Les sauvegardes de ces données nommées « PRIVE » sont à la charge de l'utilisateur et ne sont pas prises en compte par la DSI.
Les sauvegardes des traitements automatisés de données nominatives, doivent tenir compte des durées de conservation déclarées dans le registre des traitements de la collectivité. Il convient donc de veiller à ce que ces durées de conservation soient respectées en supprimant ou en anonymisant les données périmées dans les traitements, mais également les sauvegardes, les exports et les états, quel qu'en soit le support (disque dur, CDROM, serveur NAS, papier…).
La sauvegarde contenant des données personnelles sur des serveurs situées en dehors de l'union européenne (One Drive, Google drive…) n'est pas autorisée.

4.1.7 Téléchargement et installation de logiciels :

Aucun téléchargement ou installation d'application n'est autorisé à l'exception de ceux affectés par les agents de la DSI, dont c'est la fonction.
Ne pas télécharger, installer, utiliser ou contourner les restrictions d'utilisation d'un logiciel pour lequel la commune n'a pas acquis de licence. Seules les agents du service informatique sont habilités à installer des logiciels, y compris des logiciels libres, et utilisent pour cela des comptes d'administrateurs sur les machines. Les autres utilisateurs disposent de comptes d'utilisation restreints qui sont suffisants pour un usage courant.
Tous les logiciels doivent faire l'objet d'une demande officielle d'installation au service informatique qui en définira les modalités.

4.1.8 Droits de reproduction :

Ne pas copier un logiciel pour utiliser sur un autre poste, ou en dehors de son lieu de travail. Les copies de sauvegarde de logiciels, prévues par le code de la propriété intellectuelle, sont exclusivement effectuées par le service informatique, sauf dans le cas de l'acquisition directe d'un logiciel par un autre service.
Des droits de reproduction existent également pour les œuvres littéraires, musicales, photographiques, audiovisuelles, qui ne doivent en aucun cas être téléchargées sur internet, reproduites ou diffusées sans autorisation de l'auteur, ou du propriétaire des droits d'exploitation.

4.1.9 Photographies, droit à l'image :

L'image d'une personne ne peut être utilisée ou diffusée sans son consentement écrit (celui de son responsable pour un mineur). D'une manière générale, les photos que les agents peuvent être amenés à prendre dans l'exercice de leurs fonctions ne doivent pas comporter de personnes, plaques d'immatriculation, enseignes de magasins étrangères à l'affaire : il est recommandé de flouter ces éléments.
Les photos prises dans le cadre des activités de la commune de Domérat ou dans ses locaux ne peuvent pas être utilisées à des fins personnelles, et sont interdites à la diffusion externe sans autorisation expresse.
Cette recommandation s'applique aux enregistrements vidéo et sonores.

4.1.10 Equipements étrangers :

Ne pas connecter sans autorisation, à un poste ou au réseau, un équipement étranger à la commune de Domérat (disques durs externes, modems…) et susceptible de provoquer des dysfonctionnements, ou d'introduire des virus informatiques.
Toute connexion de clé USB ou DVD/CDROM doit avant lecture, faire l'objet d'une analyse antivirus par le logiciel prévu à cet effet. Le service Informatique est à la disposition des agents, en cas de difficulté.
Toute connexion d'un nouveau matériel doit se faire avec l'autorisation préalable du service informatique.

4.1.11 Messagerie :

Ne pas ouvrir de pièce jointe d'un courriel dont on n'est pas absolument certain de la provenance et de l'innocuité. Si cette pièce jointe est un document contenant des macros (tels que Word ou Excel), ne pas permettre l'exécution de ces macros dans ce cas. Il est possible que des actions préjudiciables soient effectuées par ces macros (macrovirus).
La messagerie dispose d'un outil de filtrage qui élimine automatiquement tout message suspect, en entrée et en sortie. La sélection est faite sur le type et le nom des pièces jointes. Sont également éliminés tous les messages considérés comme des « pourriels » (spam), et qui sont reconnus par la teneur du titre ou du texte du message. Attention, ces filtres ne sont pas fiables à 100%. Certains courriels ne sont pas détectés, et il peut aussi arriver que des messages légitimes soient écartés. Si vous avez des raisons de penser qu'un message vous étant destiné a été éliminé, adressez-vous au service informatique qui pourra effectuer des vérifications.
Par ailleurs, une copie de tout message électronique entrant ou sortant est conservée 6 mois. L'utilisation à titre professionnel de comptes de messagerie non gérés par la mairie de Domérat est interdite. Les comptes professionnels se terminent obligatoirement en @domerat.agglo-montlucon.fr

▲ Remarque importante :
Un message électronique peut constituer une preuve, et peut engager fermement son expéditeur et son destinataire : il existe un risque réel pour qu'un agent prenne des engagements qu'il faudra ensuite respecter. Toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent donc à la messagerie. L'envoi de messages électroniques doit respecter les mêmes procédures de contrôle, de validation, d'autorisation que les courriers.
Il est souhaitable de mettre systématiquement en copie des messages importants son responsable et le responsable du destinataire, et il est obligatoire de transmettre pour validation à un responsable tout message qui aurait valeur contractuelle ou d'engagement de la collectivité.
Par ailleurs, tout message important doit être conservé à des fins d'archivage.

4.1.12 Virus :

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...

Des comportements inhabituels d'un logiciel ou d'un ordinateur tels que l'ouverture de fenêtres intempestives, l'activité inexpliquée du disque dur ou la dégradation importante des performances peuvent traduire la présence d'un logiciel parasite : contacter immédiatement le service informatique.

4.1.13 Antivirus :

Le service informatique installe sur les machines un logiciel destiné à les protéger des programmes malveillants. Cet outil ne doit pas être désinstallé, et il est paramétré pour se mettre à jour régulièrement (reconnaissance de nouveaux virus). Le paramétrage ne doit donc pas être modifié, et il est recommandé aux utilisateurs d'ordinateurs portables de se connecter régulièrement au réseau informatique pour que cette mise à jour puisse être effectuée.

Attention, en cas de détection de virus, un message du logiciel antivirus vous avertit : veuillez contacter immédiatement le service informatique si besoin.

4.1.14 Accès à l'Internet :

Tout utilisateur connecté au réseau de la collectivité bénéficie d'un accès à l'internet sécurisé. Cet accès utilise une liaison dédiée qui est mutualisée pour tous les agents des collectivités. Il sert également pour la connexion de certains sites distants qui ne sont pas reliés en fibre optique à la cité administrative. Les moyens et les restrictions cités ci-dessous sont mis en œuvre afin d'assurer une qualité de service maximale pour les services de la collectivité et l'accès aux logiciels métiers.

Les agents veilleront à garantir l'intégrité de la collectivité lors de l'utilisation de services disponibles sur le réseau internet : la composition de l'adresse électronique et/ou de son adresse IP, engage la responsabilité de l'agent, ainsi que celle de la collectivité.

Les accès doivent s'effectuer dans un cadre professionnel. Sont proscrits par la loi, la consultation de documents, de textes, d'images ou de sites Internet sur la pédophilie, sur des sites à caractère pornographique, raciste, trafic de stupéfiants,…

La DSI a dans ce sens, mis en œuvre une politique cohérente afin de respecter la législation.

La navigation sur Internet est limitée par une solution de filtrage d'URL automatique qui interdit l'accès aux sites sensibles les plus connus (sites à caractère pornographique, pédophilie, raciste, etc…). Ce logiciel émet des états de lieux de la navigation. La DSI communiquera ces états à la Direction des Ressources Humaines et aux responsables des services sous couvert du Directeur Général des Services. En cas de non respect de la loi, la décision peut être prise d'isoler les postes des agents responsables de l'abus.

Afin d'assurer une bonne qualité des services Internet et de communication avec les sites distants, mais aussi pour des raisons de sécurité, sont interdits et éventuellement bloqués :

- Le téléchargement des fichiers Multimédias (mp3, vidéos, images, logiciels)
- Forum de discussion, réseaux sociaux (MSN, Facebook, etc.)
- L'accès aux flux multimédias (YouTube, etc…)
- L'accès aux sites Peer to Peer (Kazaa, Emule)

Néanmoins et pour tout besoin spécifique (uniquement dans le cadre de son travail), il sera possible d'ouvrir certains sites, sur demande écrite du Directeur de service, avec l'accord du DGS.
La demande, une fois validée, sera archivée à la DSI.

4.2 REGLES MINIMALES DE COURTOISIE ET DE RESPECT D'AUTRUI

Il convient de faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques (courriels, forums de discussions...)

4.2.1 Opinions personnelles et propos illicites :

Ne pas émettre d'opinions personnelles étrangères à son activité professionnelle, et susceptibles de porter préjudice à la commune de Domérat. Sont notamment interdits la consultation, la rédaction, le téléchargement, l'enregistrement, l'envoi et la diffusion de messages, textes, images, films, pages web, etc. à caractère injurieux, raciste, antisémite, discriminatoire, insultant, dénigrant, diffamatoire, dégradant, pornographique, faisant l'apologie de crime, incitant à la haine...
De même, les propos susceptibles de révéler les opinions politiques, religieuses, philosophiques, les mœurs, la santé des personnes, ou encore de porter atteinte à leur vie privée ou à leur dignité, ainsi que les messages portant atteinte à l'image, la réputation ou à la considération de la commune de Domérat sont à proscrire.

4.2.3 Emploi de la langue Française :

Eviter l'emploi de termes en langue étrangère dans des courriers ou communications. Lorsque des termes français de même sens existent, leur emploi est recommandé.

ARTICLE 5 - APPLICATION DE LA CHARTE

La présente charte s'applique à l'ensemble des agents de la commune de Domérat, tous statuts confondus, aux élus, stagiaires, visiteurs et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques et téléphoniques de la commune de Domérat.

Elle fera l'objet d'une large diffusion, tant collective qu'individuelle, par tout moyen utile (parapheur, messagerie, note de service, affichage…) afin que nul ne puisse en ignorer son existence et son contenu.
Ainsi, dès l'entrée en vigueur de la présente charte, chaque personne concernée et visée au présent article aura accès au texte de la version en vigueur. Elle devra en prendre immédiatement connaissance et sera tenue sans délai au respect des règles qui y sont édictées.
La présente version de la charte a été soumise à l'avis du comité social territorial.
Chaque nouvelle version sera validée et diffusée de la même manière. La version en vigueur sera la plus récente.

ARTICLE 6 - BASES LEGALES

Le présent article a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires définissant notamment les droits et obligations des personnes utilisant les moyens informatiques. Il ne s'agit en aucune manière d'une liste exhaustive.

• 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.

•Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

•Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée par l'ordonnance no 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi no 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

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

•Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

• Code pénal, pris notamment en ses articles 323-1 à 323-7 visant les atteintes aux systèmes de traitement automatisé des données.

• Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

• L'Ordonnance n° 2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, permet notamment à une administration de répondre par voie électronique à une demande d'information d'un usager ou d'une autre administration qui lui a été adressée par la même voie, et prévoit que les actes des administrations peuvent être signés électroniquement pour assurer l'identification du signataire et l'intégrité des actes.

• Code de la Propriété Intellectuelle. Il reconnait les logiciels comme œuvres de l'esprit, et à ce titre, ils sont protégés sans nécessiter de dépôt ou d'enregistrement.

• Code du Patrimoine, pris notamment en ses articles L211-1 à L211-4. Il définit les archives comme étant l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité. Les archives publiques sont notamment les documents qui procèdent de l'activité des collectivités territoriales.

• Loi n° 94-665 du 4 août 1994, modifiée, relative à l'emploi de la langue française. Elle prévoit lorsqu'ils existent, l'emploi de termes français de même sens en lieu et place des termes étrangers.

Annexe

Formulaire d'acceptation de la Charte informatique

Engagement à respecter les préconisations et les consignes de la charte d'utilisation informatique

Consultable sur intranet et auprès de votre Secrétariat de Direction

Nom	
Prénom	
Qualité (1)	☐ Adjoint(e), Elu(e) ☐ Agent ☐ Contractuel ☐ Stagiaire ☐ Visiteur
Collectivité (1)	☐ Ville de Domérat ☐ CCAS de Domérat
Direction	
Service	

(1) Cocher la case correspondante

Je certifie avoir pris connaissance des principes énumérés dans la charte informatique :

Je prends l'engagement de respecter les règles d'utilisation des moyens informatiques et téléphoniques de ladite charte

Date : / /20

Nom, Prénom :

Signature :

Ce formulaire est destiné à formaliser nominativement l'engagement de l'utilisateur à respecter la présente charte. La base légale en est le consentement de l'utilisateur. La fourniture de données personnelles est rendue nécessaire pour obtenir l'accès aux ressources informatiques, services internet/intranet et moyens téléphoniques. Les données à caractère personnel recueillies sont le nom et le prénom. Les données recueillies sont destinées au service des Ressources Humaines. Les utilisateurs sont informés que les données à caractère personnel les concernant sont conservées par la Ville de Domérat pendant toute la durée de leur activité au sein de la collectivité et durant les délais en vigueur en matière de prescription. Conformément au règlement n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et communément appelé Règlement Général sur la Protection des Données (RGPD) les utilisateurs sont informés qu'ils disposent d'un droit d'accès et de rectification relatif à l'ensemble des informations les concernant.

Ce formulaire est à retourner au service des Ressources Humaines dans les meilleurs délais

CHARTE INFORMATIQUE
DE LA COMMUNE DE DOMERAT