Envoyé en préfecture le 03/06/2026
Reçu en préfecture le 03/06/2026
Publié le 03/06/2026
ID : 031-200066819-20260528-DE_079_2026-DE

Volvestre
COMMUNAUTÉ DE COMMUNES

CHARTE INFORMATIQUE ET NUMÉRIQUE

Version du 18/03/2026
Approuvée par délibération n°xxxxxxx
Après avis favorable du CST du 08/04/2026

SIÈGE ADMINISTRATIF
34 Av. de Toulouse CS 70009
31390 Carbonne
05 61 90 80 70
contact@cc-volvestre.fr

créateur DE LIENS

SOMMAIRE

Envoyé en préfecture le 03/06/2026
Reçu en préfecture le 03/06/2026
Publié le
ID : 031-200066819-20260528-DE_079_2026-DE

1. INTRODUCTION

1.1. CONTEXTE ET ENJEUX

La Communauté de Communes du Volvestre (CCV) met à disposition de ses agents des ressources informatiques et numériques indispensables à l'exercice de leurs missions.
Ces outils, essentiels au bon fonctionnement des services, doivent être utilisés de manière responsable, sécurisée et conforme aux réglementations en vigueur.

En effet, l'usage de ces technologies ouvre de nombreuses possibilités en matière de performance et d'efficacité. Toutefois, cette ouverture vers l'extérieur comporte également des risques importants : atteintes à la confidentialité, à l'intégrité et à la sécurité des données (virus, intrusions, vols), pertes de productivité, coûts additionnels, et mise en jeu de la responsabilité de la communauté de communes comme des agents.

La CCV est ainsi exposée à des responsabilités importantes, notamment en lien avec les actions de ses agents et l'utilisation des moyens mis à leur disposition. C'est pourquoi le bon usage des ressources informatiques repose sur le bon sens, la vigilance et le respect de règles techniques, déontologiques et légales.

Chaque agent doit prendre conscience de ses engagements et des conséquences de ses actes. L'usage des outils numériques engage non seulement la responsabilité professionnelle, mais aussi, dans certains cas, la responsabilité personnelle, civile ou pénale.

La charte d'usage des ressources informatiques vise à :

- rappeler les principes fondamentaux et les règles de fonctionnement,
- informer les utilisateurs de leurs droits et devoirs, notamment en matière de confidentialité et de respect de la vie privée,
- sécuriser la CCV et ses agents contre les risques liés à une mauvaise utilisation des outils numériques.

Enfin, l'application des technologies de l'information et de la communication doit rester compatible avec les impératifs de sécurité du système d'information, le bon fonctionnement des services, et le respect des droits et libertés de chacun.

1.2. OBJECTIFS DE LA CHARTE

La présente charte a pour vocation de définir les règles d'utilisation des systèmes d'information et des équipements numériques mis à disposition par la Communauté de Communes du Volvestre.

Elle constitue un cadre de référence visant à garantir :

- la sécurité des données,
- le respect de la vie privée,
- la continuité des services,
- la protection du patrimoine informationnel de la CCV.

Elle poursuit trois objectifs principaux :

→ Organiser l'usage des ressources informatiques

La charte ne cherche pas à restreindre l'utilisation des outils numériques, mais à en encadrer l'usage dans un cadre clair, maîtrisé et conforme à la réglementation. Elle permet ainsi de structurer l'accès aux ressources tout en assurant leur bon fonctionnement.

→ Sensibiliser aux risques liés à l'usage des outils numériques

Face aux responsabilités de la CCV, il est essentiel de sensibiliser les agents aux enjeux de sécurité, d'intégrité et de confidentialité des informations traitées. Une mauvaise utilisation peut exposer la CCV à des risques juridiques, techniques et organisationnels.

→ Rappeler les droits et obligations des utilisateurs

La charte formalise les règles légales, déontologiques et de sécurité applicables à l'usage des systèmes d'information. Elle rappelle à chaque utilisateur ses droits, mais aussi ses devoirs, dans une logique de responsabilité individuelle et collective.

1.3. CHAMP D'APPLICATION

La présente charte s'applique à l'ensemble des utilisateurs des ressources informatiques de la CCV, quels que soient leur statut ou leur lien avec la communauté de communes.
Sont notamment concernés :

- les agents titulaires, contractuels, stagiaires, apprentis et intérimaires,
- les élus, bénévoles et toute autre personne amenée à utiliser les outils numériques de la CCV,
- les prestataires extérieurs ayant accès aux données ou aux systèmes d'information.

Tout contrat conclu avec un prestataire devra faire référence à cette charte et l'intégrer en annexe.

Dès son entrée en vigueur, chaque agent se verra remettre un exemplaire de la charte. Il devra en prendre connaissance et s'engager à la respecter, conformément au récépissé prévu à cet effet.

La charte couvre l'ensemble des ressources informatiques et numériques mises à disposition par la CCV, incluant sans limitation :

- les ordinateurs fixes et portables,
- les téléphones mobiles et smartphones professionnels,
- les tablettes et équipements nomades,
- les serveurs et systèmes de stockage,
- les messageries électroniques et outils de communication,
- les logiciels et applications métiers,
- les accès Internet et réseaux,
- les données et fichiers hébergés sur les systèmes de la CCV,
- les outils d'intelligence artificielle et services en ligne.

2. PRINCIPES GÉNÉRAUX ET CADRE JURIDIQUE

2.1. CADRE JURIDIQUE ET TEXTES DE RÉFÉRENCE

L'utilisation des systèmes d'information de la Communauté de Communes du Volvestre s'inscrit dans le respect des textes législatifs et réglementaires en vigueur.
Chaque utilisateur est tenu de respecter les obligations de réserve, de discrétion et de secret professionnel, conformément aux dispositions :

- de la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires,
- de la loi n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale.

Cette charte vise également à informer les utilisateurs des principaux textes encadrant la sécurité des systèmes d'information et la protection des données :

Textes de référence :

- Règlement Général sur la Protection des Données (RGPD – Règlement UE 2016/679)
- Loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés : elle protège les libertés individuelles face à l'usage de l'informatique.
- Loi n°85-660 du 3 juillet 1985 sur les droits d'auteur et les droits des artistes-interprètes
- Loi n°2000-230 du 13 mars 2000 sur la signature électronique et l'adaptation du droit de la preuve aux technologies de l'information.
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
- Code civil (articles 1316-1 et 1367)
- Code pénal :
  - Articles 323-1 à 323-8 (loi n°88-19 du 5 janvier 1988, dite loi GODEFRAIN) : lutte contre la fraude informatique (accès frauduleux, altération du fonctionnement, falsification de documents, etc.).
  - Article 432-9 : atteinte au secret des correspondances.
- Code de la propriété intellectuelle.
- Code des relations entre le public et l'administration.

La jurisprudence relative à l'usage des outils numériques en milieu professionnel complète ce cadre, notamment en matière de responsabilité individuelle et de respect des droits fondamentaux.

2.2. RÈGLES GÉNÉRALES

Les utilisateurs des ressources informatiques de la Communauté de Communes du Volvestre sont tenus d'adopter un comportement responsable et conforme aux lois et règlements en vigueur.

À ce titre, ils s'engagent notamment à :

- **Respecter les accès autorisés** : toute tentative d'accès à des données, services ou sites non autorisés est strictement interdite.
- **Assumer la responsabilité de leurs actions** : chaque utilisateur est responsable de l'usage qu'il fait des outils numériques, ainsi que du contenu qu'il affiche, télécharge ou transmet.
- **Préserver le bon fonctionnement du réseau** : il est interdit d'effectuer des opérations susceptibles de nuire à la stabilité, à la sécurité ou à la performance du système d'information.
- **Veiller à l'image de la CCV** : en naviguant sur Internet ou en communiquant par voie électronique, l'utilisateur représente l'établissement. Il doit donc adopter une attitude professionnelle et respectueuse.
- **Utiliser la messagerie avec discernement** : comme pour tout autre moyen de communication (courrier, téléphone), l'usage de la messagerie électronique doit respecter la hiérarchie, les missions confiées, ainsi que les règles élémentaires de courtoisie et de bienséance. En effet, l'utilisateur est responsable des messages envoyés ou reçus.

2.3. DROITS ET OBLIGATIONS DES UTILISATEURS

Tout agent ou utilisateur des ressources informatiques de la CCV s'engage à respecter les principes suivants :

Les outils numériques mis à disposition doivent être utilisés dans le cadre des missions confiées, avec professionnalisme, loyauté et bonne foi. Chaque utilisateur est responsable de l'usage qu'il fait des équipements et des données, ainsi que du contenu qu'il affiche, télécharge ou transmet.

À titre exceptionnel et lorsqu'aucune autre solution n'est possible, un usage personnel ponctuel de l'ordinateur peut être toléré, sous réserve qu'il reste raisonnable, ne nuise pas à la sécurité des systèmes ni à la continuité du service, et soit exercé en toute responsabilité.
Pour ces usages ponctuels, l'agent peut créer un dossier intitulé « personnel » en local sur son ordinateur (et non sur le serveur), afin de distinguer clairement les fichiers personnels des documents professionnels. Ce dossier doit rester limité en taille et ne contenir aucun élément susceptible de compromettre la sécurité ou la conformité réglementaire.

Chaque utilisateur doit adopter un comportement vigilant face aux menaces informatiques (virus, intrusions, etc.) et contribuer à la préservation de la sécurité du système. Cela implique notamment :

- de ne pas perturber la disponibilité du réseau,
- de respecter les contraintes liées à la maintenance,
- de n'utiliser que les ressources matérielles ou logicielles fournies par la CCV,
- de ne pas introduire de ressources externes non autorisées (ex. : clé USB, logiciels non validés).

Les données produites par ou pour la CCV sont confidentielles et demeurent sa propriété. Leur diffusion ou utilisation à des fins personnelles est interdite sans l'accord explicite de l'autorité territoriale.

L'utilisateur doit :

- respecter l'intégrité et la confidentialité des informations traitées,
- éviter tout contenu portant atteinte à la dignité humaine, à la vie privée ou aux droits fondamentaux,

Il est interdit de stocker, transmettre ou afficher des contenus discriminatoires, injurieux ou diffamatoires.

Il est interdit de reproduire ou diffuser des contenus protégés par des droits d'auteur sans autorisation. L'installation ou la copie de logiciels sans licence est également proscrite.

Le droit d'accès au système d'information est strictement personnel et incessible. Chaque utilisateur doit veiller à ne pas partager ses identifiants ou permettre un accès non autorisé aux ressources informatiques.

2.4. DROIT ET OBLIGATIONS DE LA COMMUNAUTÉ DE COMMUNES DU VOLVESTRE

La CCV s'engage à garantir la disponibilité, la sécurité et l'intégrité de son système d'information.
À ce titre, elle met en œuvre les actions suivantes :

→ Fournir aux utilisateurs les équipements informatiques et les logiciels nécessaires à l'exercice de leurs missions.
→ Assurer la mise à jour régulière des matériels et logiciels afin de maintenir un niveau de sécurité conforme aux standards en vigueur, dans le respect des règles d'achat et des budgets alloués.
→ Proposer des formations adaptées pour permettre une utilisation efficace et sécurisée des outils numériques.
→ Informer les utilisateurs des contraintes d'exploitation susceptibles d'impacter leur activité (interruptions de service, opérations de maintenance, modifications techniques, etc.).
→ Respecter la confidentialité des données personnelles des utilisateurs, notamment lors d'interventions techniques ou de diagnostics.
→ Garantir que les données produites par ou pour la CCV restent confidentielles et ne soient diffusées qu'avec l'accord explicite de l'autorité territoriale.
→ Établir les règles d'utilisation du système d'information et veiller à leur application.
→ Assurer la sécurité et l'intégrité des ressources matérielles et logicielles dans le cadre des engagements budgétaires et des impératifs techniques.

L'utilisation des ressources informatiques peut faire l'objet d'analyses et de contrôles, dans le respect de la législation en vigueur.

3. UTILISATION DES ÉQUIPEMENTS

3.1. MATÉRIELS MIS À DISPOSITION

Les équipements informatiques (ordinateurs, téléphones, tablettes, etc.) sont attribués nominativement aux agents pour l'exercice de leurs fonctions.
Chaque agent est responsable du matériel qui lui est confié et doit en assurer une utilisation conforme aux règles établies.
Toute utilisation détournée, négligence grave ou dégradation volontaire engage la responsabilité de l'agent, qui est tenu d'assurer l'entretien élémentaire de son matériel : propreté, manipulation appropriée, rangement sécurisé. En cas de dysfonctionnement, il doit en informer rapidement le service informatique.

Il est strictement interdit :

- de modifier la configuration matérielle des équipements,
- d'installer ou de retirer des composants sans l'autorisation du service informatique,
- d'utiliser des périphériques ou logiciels externes non validés par la CCV.

Chaque utilisateur dispose d'un ensemble cohérent composé de :

- Matériel : unité centrale ou client léger (pour les machines virtuelles), écran, clavier, souris, etc.
- Système d'exploitation : Windows, macOS, selon les besoins.
- Logiciels : suite bureautique, outils de communication, logiciels de gestion, applications spécifiques.
- accès Wi-Fi sécurisé.

Des équipements complémentaires peuvent également être mis à disposition selon les besoins :

- ordinateurs portables,
- vidéoprojecteurs, écrans multimédia,
- téléphones mobiles,
- Etc.

3.2. ORDINATEURS FIXES ET PORTABLES

Afin de garantir la sécurité du système d'information et le bon fonctionnement des équipements informatiques, chaque utilisateur s'engage à respecter les règles suivantes :

Verrouillage du poste

Le poste de travail doit être systématiquement verrouillé en cas d'absence, même brève, à l'aide de la combinaison de touches appropriée (ex. : Windows + L) ou via le verrouillage automatique. Cette mesure prévient tout accès non autorisé aux données.

Extinction en fin de journée

Sauf nécessité de service dûment justifiée, les postes doivent être éteints à la fin de la journée. Cela contribue à la sécurité du système, à la réduction de la consommation énergétique et facilite les opérations de maintenance.

Mises à jour de sécurité

Les mises à jour automatiques du système ne doivent pas être désactivées. Elles sont essentielles pour la protection contre les vulnérabilités. Le service informatique peut, le cas échéant, bloquer certaines mises à jour jugées problématiques, sur la base d'un bulletin d'information préalable.

Installation de logiciels

L'installation de tout logiciel doit faire l'objet d'une validation préalable par le service informatique. L'ajout de logiciels non autorisés peut compromettre la sécurité du système et entraîner des dysfonctionnements.

Utilisation de périphériques externes

Ces dispositifs présentent des risques de sécurité (virus, perte de données). Leur utilisation doit être signalée au service informatique et autorisée avant tout usage.
Il est recommandé de privilégier les espaces de stockage internes à la CCV :

- collaboratifs (serveur de fichiers),
- personnels (OneDrive).

Ordinateurs portables

Les ordinateurs portables doivent être transportés dans une housse de protection adaptée et ne jamais être laissés sans surveillance, notamment dans les véhicules. Cette précaution vise à prévenir les vols et les pertes de données sensibles.

3.3. TÉLÉPHONES MOBILES

Les téléphones mobiles professionnels sont attribués en fonction des besoins du service.
Leur utilisation doit être prioritairement dédiée aux communications liées à l'activité professionnelle et au bon fonctionnement des missions confiées.
Un usage personnel raisonnable est toléré, notamment pour les appels et messages, à condition qu'il :

- reste ponctuel et modéré,
- n'entraîne pas de surcoût pour la CCV,
- ne nuise ni à la disponibilité du matériel ni à l'efficacité du service.

Afin de garantir la sécurité des données et des équipements, les smartphones doivent être protégés par un code PIN et un mot de passe de déverrouillage robuste. La fonction de verrouillage automatique doit être activée,

Toute perte ou vol d'un appareil doit être signalée immédiatement au service informatique et à la hiérarchie pour permettre le blocage à distance et la protection des données.

L'installation d'applications sur les smartphones professionnels doit rester :

- limitée à des usages utiles et compatibles avec les missions professionnelles,
- exempte de tout risque pour la sécurité du système d'information,
- exclue pour les applications inappropriées en milieu professionnel.

4. MESSAGERIE ÉLECTRONIQUE

4.1. BONNES PRATIQUES

Chaque agent dispose d'une adresse électronique attribuée selon un format standardisé par le service informatique. Cette adresse constitue le canal exclusif pour les échanges professionnels.

L'usage de la messagerie est prioritairement réservé aux communications liées à l'activité professionnelle. Toutefois, un usage personnel ponctuel et raisonnable peut être toléré, à condition qu'il ne compromette ni la sécurité du système ni le bon fonctionnement du service.

Les messages échangés via la messagerie professionnelle sont présumés avoir un caractère professionnel. Ils peuvent, à ce titre, être consultés par la hiérarchie, sauf s'ils sont clairement identifiés comme personnels par l'utilisateur, notamment par la mention explicite « personnel » ou « privé » dans l'objet du message.

Il est attendu de chaque utilisateur qu'il consulte sa messagerie régulièrement afin d'assurer la continuité des échanges et le bon déroulement des missions confiées.
L'usage de la messagerie professionnelle doit respecter les principes suivants :

- → **Objet clair et précis** : chaque message doit comporter un objet explicite permettant d'identifier rapidement son contenu.
- → **Courtoisie professionnelle** : les messages doivent respecter les règles de politesse et de bienséance. L'usage de formules d'appel et de politesse est recommandé.
- → **Concision et clarté** : privilégier des messages courts, structurés et allant à l'essentiel. Le style doit rester courant, sans abréviations ni formulations trop familières. Les sigles doivent être explicités pour garantir la compréhension du destinataire. L'usage des majuscules est à éviter car il peut être perçu comme agressif. **Une relecture systématique est indispensable avant envoi, afin de corriger les fautes d'orthographe ou de grammaire et de s'assurer de la clarté du propos.**
- → **Signature professionnelle** : utiliser la signature électronique standardisée comprenant les nom, prénom, fonction, service et coordonnées de la CCV.
- → **Destinataires appropriés** : identifier avec soin les destinataires du message :
  - À : pour les personnes dont une réponse ou une action est attendue.
  - CC : pour les personnes à informer, sans attente de réponse ou d'action. À utiliser avec modération.
  - CCI : à privilégier pour les envois à un grand nombre de destinataires, afin de respecter la confidentialité (RGPD). L'expéditeur doit se mettre en destinataire principal.

Les envois massifs non justifiés et l'usage systématique de la fonction « Répondre à tous » sont à éviter.

Différence entre messagerie électronique et Teams

Microsoft Teams est un outil complémentaire à la messagerie électronique, adapté à des usages plus directs et informels :

- Messagerie électronique : à privilégier pour les communications formelles, les échanges avec des interlocuteurs externes, les transmissions de documents officiels ou les demandes nécessitant une traçabilité.
- Teams : recommandé pour les échanges rapides, les discussions internes, les messages instantanés ou les collaborations en temps réel. Il permet de fluidifier les échanges sans alourdir les boîtes mail.

L'usage de Teams contribue à une meilleure réactivité et à une communication plus agile au sein des équipes, tout en réduisant le volume de courriels.

4.2. GESTION DES PIÈCES JOINTES

L'envoi de pièces jointes par courriel doit respecter plusieurs règles afin de garantir l'efficacité, la sécurité et la lisibilité des échanges.

Il convient de limiter la taille des fichiers transmis. Cette pratique permet d'éviter les saturations de boîtes mail et de faciliter l'accès aux documents.

Les formats de fichiers utilisés doivent être standards et largement compatibles, tels que les formats PDF ou les formats courants de la suite Office, afin de garantir leur ouverture par tous les destinataires.

Avant tout envoi, l'utilisateur doit vérifier que les pièces jointes correspondent bien au contenu annoncé dans le message, qu'elles sont correctement nommées selon les règles en vigueur au sein de la Communauté de Communes du Volvestre, et qu'elles ne contiennent pas d'informations confidentielles non destinées aux destinataires.

Il est essentiel de décrire brièvement le contenu de la pièce jointe dans le corps du message, afin que le destinataire sache ce qu'il s'apprête à télécharger.

Deux pratiques distinctes doivent être observées selon le type de destinataire :

- En interne, lorsque le document est déjà disponible sur le serveur commun, il est préférable d'envoyer un lien vers ce document.
- En externe, le document peut être joint directement au courriel. Il convient alors de s'assurer que le nom du fichier est explicite. En cas de fichier volumineux, seuls l'usage des services de transfert sécurisé SMASH ou France Transfert sont autorisés.

Concernant les accusés de réception, il est important de noter que les notifications automatiques ne garantissent ni la lecture ni la prise en compte du message. Elles ne confirment que l'ouverture du courriel. Pour obtenir une confirmation fiable, il est préférable d'intégrer directement dans le corps du message une formule telle que : « *Merci de bien vouloir accuser réception de ce message* ». Cette démarche est plus efficace et permet de s'assurer que le destinataire a bien pris connaissance du contenu.

4.3. CONSERVATION ET ARCHIVAGE

La messagerie professionnelle est un outil de travail à part entière. Son bon usage implique une organisation rigoureuse, une gestion efficace des courriels et le respect des règles de conservation et de sécurité.

Il est recommandé de maintenir une boîte de réception claire et fonctionnelle. Les messages traités doivent être régulièrement archivés ou supprimés. Pour faciliter le classement et les recherches, il est conseillé de créer une arborescence simple, avec une dizaine de dossiers thématiques correspondant aux affaires suivies, éventuellement complétée par des sous-dossiers. Cette organisation ne constitue pas un archivage au sens réglementaire, mais une méthode de rangement temporaire.

Les courriels sans valeur professionnelle (publicités, messages en copie sans lien avec les missions, newsletters non lues) doivent être supprimés. Les pièces jointes utiles doivent être enregistrées dans les dossiers numériques appropriés sur le serveur, puis le message peut être supprimé s'il ne contient pas d'autres informations pertinentes. La corbeille doit être vidée régulièrement, car les messages supprimés y restent stockés et occupent de l'espace.

Chaque boîte aux lettres dispose d'un quota de stockage défini (par exemple, 50 Go pour une boîte Exchange). Une boîte saturée peut empêcher la réception de nouveaux messages et perturber le fonctionnement du service. Il est donc essentiel de gérer régulièrement les volumes de courriels.

Les courriels ayant une valeur juridique, administrative, financière ou historique doivent être archivés conformément aux règles de conservation en vigueur. Lorsqu'un message fait partie intégrante d'un dossier, il doit être enregistré dans le dossier numérique correspondant et, si nécessaire, imprimé pour être intégré au dossier papier.

Tri et conservation des courriels

Le tri des courriels doit permettre de limiter les doublons, de réduire le poids des boîtes aux lettres et de garantir la traçabilité des échanges. Les courriels doivent être classés selon leur utilité :

- **À conserver** : messages à valeur administrative, juridique ou stratégique (devis, correspondance officielle, notes de service, directives).
- **À supprimer** : courriels personnels, spams, avis sans lien avec l'activité professionnelle, brouillons.
- **À traiter temporairement** : messages informatifs utiles sur une courte durée.

En cas d'absence prolongée, il est impératif de paramétrer un message d'absence clair et informatif. Ce message doit indiquer la durée de l'absence et, si possible, les coordonnées d'un collègue à contacter en cas d'urgence. Pour les absences de courte durée (1 à 2 jours), cette démarche n'est pas obligatoire.
En cas de besoin pour la continuité de service, une délégation de consultation poura être mise en place.

5. INTERNET ET RÉSEAUX SOCIAUX

L'accès à Internet mis à disposition par la CCV est destiné en priorité à un usage professionnel. Il peut également être utilisé à des fins syndicales dans le cadre des décharges d'activité ou autorisations spéciales d'absence. Un usage personnel ponctuel et raisonnable est toléré en dehors des heures de travail, à condition qu'il ne nuise ni au bon fonctionnement du service ni à la sécurité du système d'information.

Les utilisateurs s'engagent à ne pas consulter de sites contraires aux lois et règlements en vigueur, notamment ceux à caractère pornographique, pédopornographique, violent, faisant l'apologie de crimes ou délits, de jeux d'argent en ligne ou de téléchargement illégal. Toute navigation sur des sites portant atteinte à la dignité humaine est strictement interdite.

L'accès à Internet fait l'objet d'un filtrage automatique par le fournisseur d'accès et d'une journalisation des connexions, dans le respect de la réglementation en vigueur. Ces données de connexion peuvent être consultées en cas d'incident de sécurité ou de manquement grave, mais ne font l'objet d'aucun contrôle en temps réel. Leur traitement est encadré par la norme simplifiée CNIL n°46 et ne vise pas à surveiller individuellement les agents.

Téléchargements et stockage

Les téléchargements doivent être strictement limités aux besoins professionnels. Le téléchargement de contenus protégés par des droits d'auteur (musique, films, logiciels, etc.) sans autorisation est interdit et constitue une infraction pénale.
Le stockage de fichiers non professionnels issus d'Internet est toléré de manière limitée. Conformément aux recommandations de la CNIL, tous les fichiers présents sur les postes de travail sont présumés professionnels, sauf s'ils sont clairement identifiés comme personnels.
Si vous souhaitez conserver des documents personnels, ceux-ci doivent être rangés dans un dossier intitulé « Personnel » ou « Privé », situé sur votre espace local. Le stockage de fichiers personnels reste interdit sur les espaces partagés du réseau, tels que les serveurs de fichiers.

Réseaux sociaux professionnels

Seuls les services communication et tourisme sont autorisés à gérer les comptes officiels de la communauté de communes sur les réseaux sociaux, chacun pour sa partie respective. Toute création de compte au nom de la CCV doit être validée par la direction.

Les agents disposent de leur liberté d'expression sur les réseaux sociaux à titre personnel, dans le respect de leur obligation de réserve et de discrétion professionnelle. Il est essentiel de bien distinguer les usages personnels et professionnels, notamment en évitant d'utiliser l'adresse électronique professionnelle pour créer ou gérer des comptes personnels.
Même sur un compte privé, les agents doivent veiller à ne pas publier de contenus susceptibles de nuire à l'image de la communauté de communes ou de divulguer des informations confidentielles.
Une attention particulière doit être portée à la diffusion d'informations personnelles ou professionnelles, qui peuvent être exploitées à des fins malveillantes (usurpation d'identité, ingénierie sociale, etc.).
Enfin, la publication de photos ou vidéos prises dans le cadre professionnel est soumise à autorisation préalable, dans le respect du droit à l'image des personnes concernées.

6. GESTION DES FICHIERS ET DES DONNÉES SUR LE SERVEUR

La CCV met à disposition des agents plusieurs espaces de stockage sur serveur, conçus pour favoriser le travail collaboratif et garantir la sécurité des données professionnelles.

Les répertoires partagés, organisés par direction et par service, permettent le partage de documents selon des droits d'accès définis par la hiérarchie. Ces espaces sont réservés aux documents professionnels et doivent être utilisés conformément aux règles de gestion documentaire.

Le stockage local sur le disque dur de l'ordinateur est à proscrire pour les documents professionnels. Seul le stockage sur serveur assure la sauvegarde, la pérennité des données et la continuité de service en cas d'incident technique.

6.1. NOMMAGE ET ORGANISATION DES FICHIERS

Une bonne organisation des fichiers facilite la recherche, le partage et la collaboration.
Il est essentiel d'adopter une nomenclature claire et cohérente, en évitant les abréviations obscures.
Les noms de fichiers doivent être explicites et suivre les recommandations du document « Infographie Nommage » annexé à la présente charte.
Les documents doivent être rangés dans une arborescence logique et hiérarchisée, en évitant l'accumulation de fichiers à la racine des répertoires partagés. Pour les documents sujets à modifications fréquentes, un système de versionnage (date ou numéro de version dans le nom du fichier) est recommandé.
La gestion des doublons est également essentielle : il convient de limiter les copies inutiles et de privilégier les liens ou raccourcis vers le document original.

6.2. DROITS D'ACCÈS, CONFIDENTIALITÉ ET GESTION DES DOCUMENTS

Chaque utilisateur doit respecter les droits d'accès définis pour les espaces de stockage numériques. Il est strictement interdit de tenter de contourner ces restrictions.

Les documents contenant des informations sensibles, notamment des données personnelles ou confidentielles, doivent être stockés dans des répertoires sécurisés, avec des accès limités aux seules personnes habilitées. Tout partage externe de documents doit être validé par la hiérarchie et réalisé exclusivement via les outils sécurisés prévus à cet effet.

La suppression de fichiers dans les espaces partagés doit être effectuée avec discernement. En cas de doute sur la valeur ou l'utilité d'un document, il est recommandé de consulter sa hiérarchie avant toute suppression définitive.

Certains documents peuvent porter la mention « confidentiel » ou « diffusion restreinte ». Ces classifications doivent être scrupuleusement respectées, et la diffusion de ces documents doit être strictement limitée aux destinataires autorisés.

Les documents papier contenant des informations sensibles doivent être rangés en lieu sécurisé lorsqu'ils ne sont pas utilisés, ne jamais être laissés à la vue de tous, notamment dans les bureaux partagés ou à proximité des imprimantes, et doivent être détruits à l'aide d'un destructeur de documents lorsqu'ils deviennent obsolètes ou inutiles.
Lors du travail à distance, une vigilance accrue est requise afin d'éviter que des personnes non habilitées puissent accéder à des informations professionnelles confidentielles.

6.3. SAUVEGARDE ET CONTINUITÉ DE SERVICE

Les documents stockés sur les serveurs de la CCV font l'objet de sauvegardes automatiques régulières. En cas de suppression accidentelle ou de fichier corrompu, le service informatique peut procéder à une restauration.
Les fichiers enregistrés uniquement sur un disque local ou sur des supports externes (clé USB, disque dur) ne sont pas sauvegardés par la CCV. L'agent en assume seul la responsabilité en cas de perte.

L'espace disponible sur les postes de travail étant limité, il est recommandé de procéder régulièrement au nettoyage des répertoires tels que le dossier « Téléchargements ». Les documents professionnels doivent être classés dans les dossiers appropriés du serveur, en veillant à éviter les doublons inutiles.
Les documents n'ayant plus d'utilité courante mais devant être conservés pour des raisons réglementaires ou historiques doivent être transférés vers un espace d'archivage adapté. Pour cela, il convient de se rapprocher du responsable des archives.

7. SÉCURITÉ INFORMATIQUE

La sécurité du système d'information de la Communauté de Communes du Volvestre repose sur la vigilance permanente de chaque agent. Adopter une posture responsable et rester informé des menaces numériques est essentiel.

Chaque utilisateur doit faire preuve de prudence dans ses échanges numériques et être attentif aux signaux d'alerte suivants :

Phishing (hameçonnage)

Ne jamais répondre ni cliquer sans vérification si un message présente :

- Un expéditeur inconnu ou une adresse suspecte ;
- Une demande urgente ou inhabituelle ;
- Des fautes d'orthographe ou un langage approximatif ;
- Des liens ou pièces jointes non sollicités ;
- Une demande d'informations confidentielles (identifiants, mots de passe, données personnelles).

En cas de doute, ne pas ouvrir le message et contacter immédiatement le service informatique.

Se méfier des tentatives de manipulation par téléphone, courriel ou en personne visant à obtenir des accès ou des informations sensibles.

Sites web malveillants

Éviter la navigation sur des sites à risque (téléchargement illégal, contenus illicites). Le filtrage Internet de la CCV bloque de nombreux sites, mais la vigilance individuelle reste indispensable.

Rançongiciels (ransomware)

Ne jamais ouvrir une pièce jointe ou cliquer sur un lien dans un message suspect. En cas de doute, vérifier l'authenticité du message par un autre canal.

Protection des données sensibles

- Ne jamais transmettre d'informations confidentielles (identifiants, données personnelles) par messagerie simple.
- Utiliser les outils de chiffrement ou les plateformes sécurisées mises à disposition par la CCV.
- Ne jamais communiquer un mot de passe, même dans le cadre d'échanges internes.

Gestion des spams et messages indésirables

- Ne pas répondre aux spams ou messages suspects.
- Ne pas cliquer sur les liens qu'ils contiennent.
- Signaler immédiatement ces messages au service informatique pour traitement et prévention.

7.1. GESTION DES MOTS DE PASSE

Les mots de passe constituent la première ligne de défense en matière de sécurité informatique. Leur robustesse, leur unicité et leur confidentialité sont essentielles pour protéger les accès aux systèmes et aux données.

Conformément aux recommandations de l'A.N.S.S.I. (Agence Nationale de la Sécurité des Systèmes d'Information), un mot de passe robuste doit :

- Contenir au minimum 12 caractères (7 caractères pour les systèmes moins sensibles, à défaut).
- Combiner lettres majuscules et minuscules, chiffres et caractères spéciaux.
- Ne pas contenir :
  - de mots du dictionnaire,
  - de suites logiques (ex. : 123456, azerty),
  - d'informations personnelles évidentes (ex. : prénom, date de naissance).

Les mots de passe des comptes sensibles doivent être renouvelés régulièrement, au minimum tous les 6 mois, ou immédiatement en cas de suspicion de compromission.

Le système vous invitera à effectuer ce changement selon la temporalité définie.
Les mots de passe sont strictement personnels. Il est formellement interdit de :

- Les communiquer à quiconque, y compris à sa hiérarchie ou au service informatique.
- Les noter sur un support non sécurisé (post-it, document non chiffré).
- Les enregistrer dans un navigateur sur un poste partagé.

En cas de perte, contactez le service informatique qui procédera à la réinitialisation du mot de passe. Il n'aura pas accès à votre mot de passe initial.

Tout dysfonctionnement ou anomalie doit être signalé immédiatement au service informatique.

7.2. AUTHENTIFICATION ET ACCÈS

Pour garantir la sécurité des données et des systèmes, chaque agent doit respecter les principes suivants :

Utilisation personnelle des comptes

- Chaque agent doit utiliser exclusivement son propre compte utilisateur.

- L'usage du compte d'un collègue est strictement interdit, y compris en cas d'absence.

Authentification forte

- L'accès aux comptes Microsoft est soumis à une procédure de double authentification. Chaque utilisateur doit fournir un numéro de téléphone valide afin de garantir la sécurité de son compte.
- L'agent doit alors respecter les procédures spécifiques communiquées par le service informatique.

Comptes génériques ou partagés

- L'usage de comptes génériques ou partagés est à proscrire, sauf exception dûment justifiée et validée par la direction.
- Lorsqu'ils existent, leur usage doit être :
  - limité aux personnes habilitées,
  - tracé pour garantir la traçabilité des actions.

Déconnexion obligatoire

- Il est impératif de se déconnecter de toutes les applications et du système :
  - en fin de journée,
  - ou lors de toute absence prolongée.
- Cela permet de préserver l'intégrité des systèmes et d'éviter toute exposition inutile.

7.3. INCIDENTS DE SÉCURITÉ

La réactivité face aux incidents de sécurité est essentielle pour limiter les impacts et renforcer la protection du système d'information de la Communauté de Communes du Volvestre.

Tout incident de sécurité, réel ou suspecté, doit être signalé sans délai au service informatique et à la hiérarchie. Cela inclut notamment :

- La perte ou le vol de matériel (ordinateur, téléphone, clé USB, etc.) ;
- La suspicion de compromission d'un mot de passe ;
- La réception d'un message suspect ou un comportement informatique inhabituel ;
- Une infection par un virus ou un logiciel malveillant ;
- La constatation d'un accès non autorisé à un système ou à des données.

Le signalement d'un incident, même s'il résulte d'une erreur de l'agent, ne donne lieu à aucune sanction, dès lors qu'il est fait de bonne foi. L'objectif est de limiter les conséquences et d'améliorer collectivement la sécurité.

En cas d'incident, l'agent concerné doit :

- Coopérer pleinement avec le service informatique pour analyser la situation ;
- Participer à la mise en œuvre des mesures correctives nécessaires.

En cas d'incident majeur :

- Respecter les consignes de communication transmises par la hiérarchie ;
- Ne pas communiquer publiquement (réseaux sociaux, presse, etc.) sans autorisation explicite.

7.4. INSTALLATION D'UN LOGICIEL

Toute demande d'installation d'un logiciel (même gratuit) doit être adressée par mail à son responsable de service, en précisant :
- Le nom du logiciel et sa version,

- La finalité professionnelle de son utilisation,
- La source officielle de téléchargement.

Le responsable vérifiera auprès du service informatique la compatibilité, la sécurité et la conformité avant toute installation. Aucun logiciel ne doit être installé directement par l'agent sans validation préalable

8. PROTECTION DES DONNÉES PERSONNELLES (RGPD)

8.1. PRINCIPES ET OBLIGATIONS

La Communauté de Communes du Volvestre traite de nombreuses données personnelles dans le cadre de ses missions. Chaque agent est responsable de leur protection et doit respecter les principes du Règlement Général sur la Protection des Données (RGPD).

Tout traitement de données personnelles doit respecter les principes suivants :

- Licéité : le traitement doit reposer sur une base légale (mission d'intérêt public, obligation légale, consentement, etc.).
- Finalité déterminée : les données doivent être collectées pour des objectifs précis, explicites et légitimes, et ne pas être utilisées à d'autres fins.
- Minimisation : seules les données strictement nécessaires doivent être collectées. Éviter toute collecte « au cas où ».
- Exactitude : les données doivent être exactes et à jour. Les informations erronées doivent être corrigées ou supprimées.
- Limitation de conservation : les données ne doivent pas être conservées indéfiniment. Il faut respecter les durées légales ou réglementaires.
- Sécurité et confidentialité : des mesures techniques et organisationnelles appropriées doivent être mises en œuvre pour protéger les données.

8.2. DROITS DES PERSONNES CONCERNÉES

Les agents doivent faciliter l'exercice des droits des personnes (usagers, agents, partenaires) :

- Droit à l'information : informer clairement sur l'usage des données.
- Droit d'accès : permettre à toute personne de consulter ses données.
- Droit de rectification : corriger les données inexactes ou incomplètes.
- Droit à l'effacement : possibilité de demander la suppression de données dans certains cas.
- Droit d'opposition : possibilité de s'opposer à certains traitements.
- Droit à la limitation : possibilité de demander la suspension temporaire d'un traitement.

Toute demande d'exercice de droits doit être transmise sans délai au référent RGPD de la CCV pour traitement dans les délais légaux.

8.3. OBLIGATIONS DES AGENTS

Chaque agent doit adopter une posture responsable au quotidien :

- Se former régulièrement aux bonnes pratiques en matière de protection des données.
- Appliquer les bons réflexes :
  - Ne collecter que les données nécessaires ;
  - Limiter l'accès aux seules personnes habilitées ;
  - Ne pas diffuser de données sans vérification ;
  - Sécuriser les documents contenant des données sensibles.

- Respecter le secret professionnel : toute donnée personnelle connue dans le cadre des fonctions est couverte par l'obligation de discrétion.
- Signaler immédiatement toute violation de données (perte, accès non autorisé, divulgation, etc.) au service informatique et au référent RGPD.

8.4. CAS PARTICULIERS ET DONNÉES SENSIBLES

Certaines données nécessitent une vigilance renforcée :

- Données sensibles (origine ethnique, opinions politiques, convictions religieuses, santé, etc.) : leur traitement est interdit sauf exceptions strictement encadrées.
- Données relatives aux enfants (guichet unique, crèches, relais petite enfance) : faire preuve d'une attention particulière à leur confidentialité.
- Données de santé : leur traitement doit être limité aux personnes habilitées et faire l'objet de mesures de sécurité renforcées.
- Diffusion publique (site internet, réseaux sociaux, publications) : toute publication de données personnelles doit être précédée d'une vérification et, si nécessaire, du recueil du consentement.

9. INTELLIGENCE ARTIFICIELLE

9.1. CONTEXTE ET DÉFINITION

L'intelligence artificielle (IA) désigne l'ensemble des technologies permettant à des systèmes informatiques d'exécuter des tâches qui requièrent habituellement une intervention humaine. Ces tâches incluent notamment le traitement du langage naturel, l'analyse de données, la génération de contenus ou encore l'aide à la décision.
Le développement rapide des outils d'IA offre des perspectives d'amélioration de l'efficacité des services publics.
Leur intégration à terme dans les pratiques professionnelles accompagnera les missions de la Communauté de Communes du Volvestre.
Toutefois, leur utilisation doit être encadrée afin de garantir la sécurité des données, le respect des obligations réglementaires et des principes éthiques.
Cette disposition s'applique à l'ensemble des outils intégrant des fonctionnalités d'intelligence artificielle, qu'il s'agisse d'outils grand public (tels que Copilot, ChatGPT, assistants conversationnels, etc.) ou de solutions spécialisées intégrées aux logiciels métiers.
Il est rappelé que l'usage d'un outil d'intelligence artificielle ne décharge en aucun cas l'agent de sa responsabilité professionnelle. L'agent demeure pleinement responsable des contenus produits et des décisions prises, y compris lorsqu'ils sont réalisés ou assistés par un outil d'IA.

L'utilisation de l'IA fera l'objet d'un travail concerté, afin de
- Définir une stratégie d'usage de l'IA, alignée avec les orientations de la CCV et les besoins opérationnels
- Elaborer un référentiel ou protocole d'usage, précisant l'outil retenu, les modalités d'utilisation, le périmètre d'action autorisé, ainsi que les mesures de prévention des risques (sécurité, éthique, dérives potentielles)
- Former les agents concernés, pour garantir une appropriation maîtrisée et pertinente de l'outil dans leurs missions

9.2. CAS D'USAGE AUTORISÉS ET INTERDITS

Dans l'attente de ce travail, l'utilisation des outils d'intelligence artificielle est **autorisée** dans les cas suivants, sous réserve du respect des règles de sécurité, de confidentialité, de conformité réglementaire et d'éthique :

- → Aide à la rédaction : amélioration de la formulation, correction orthographique et grammaticale, restructuration de textes, recherche de synonymes, adaptation du niveau de langage.
- → Synthèse et analyse : résumé de documents volumineux, extraction d'informations clés, organisation d'idées, préparation de supports de présentation.
- → Traduction : traduction de documents ou d'échanges dans une langue étrangère, sous réserve d'une vérification humaine du résultat.
- → Assistance technique : aide à la résolution de problèmes informatiques simples, recherche de solutions techniques, apprentissage de nouvelles compétences.
- → Créativité et brainstorming : génération d'idées, propositions de plans d'action, exploration de solutions alternatives dans un cadre professionnel.
- → Automatisation de tâches répétitives : utilisation d'outils d'IA intégrés dans les logiciels métiers pour automatiser des tâches administratives simples et récurrentes.

En revanche, certains usages de l'intelligence artificielle sont **interdits ou strictement encadrés** afin de prévenir les risques juridiques, éthiques ou organisationnels :

- o Décisions automatisées : l'IA ne peut être utilisée seule pour prendre des décisions ayant un impact significatif sur les droits des personnes (ex. : attribution d'aides, décisions en ressources humaines, sanctions). Une intervention humaine reste obligatoire.
- o Évaluation des agents : l'IA ne peut être utilisée comme outil principal ou exclusif pour évaluer la performance ou le comportement des agents.
- o Profilage des usagers : tout traitement visant à établir des profils comportementaux doit être strictement encadré et conforme au RGPD.
- o Communication officielle sensible : les communications officielles portant sur des sujets sensibles ou stratégiques doivent être rédigées par un agent et ne peuvent être entièrement déléguées à un outil d'IA.
- o Traitement de données massives : l'analyse de grandes quantités de données personnelles à l'aide d'outils d'IA nécessite la réalisation préalable d'une analyse d'impact relative à la protection des données (AIPD).

L'utilisation des outils d'intelligence artificielle doit s'accompagner d'une vigilance constante et d'un respect des principes éthiques fondamentaux. Les agents sont invités à adopter une posture critique et responsable dans leurs usages.

Les outils d'IA peuvent reproduire ou amplifier des biais existants (discriminations, stéréotypes, inégalités). Il est essentiel d'exercer un regard critique sur les résultats produits et de ne pas les considérer comme neutres ou infaillibles.

L'usage de l'IA ne doit en aucun cas porter atteinte au principe d'égalité de traitement des usagers. Aucune rupture d'équité ne doit être introduite dans l'accès aux services publics ou dans la manière dont les usagers sont pris en charge.

Il convient de privilégier les outils d'IA dont le fonctionnement peut être expliqué et compris, en particulier lorsqu'ils sont utilisés dans des contextes ayant un impact direct sur les usagers.

Le domaine de l'intelligence artificielle évolue rapidement. Les agents doivent se tenir informés des évolutions technologiques, des bonnes pratiques et des risques émergents. Ils sont encouragés à participer aux formations proposées par la CCV.

Tout comportement inattendu, résultat inapproprié ou problème technique lié à l'usage d'un outil d'IA doit être signalé sans délai au service informatique, afin d'assurer un suivi et une correction appropriés.

10. SANCTIONS ET CONTRÔLE

La Communauté de Communes du Volvestre s'engage à assurer une application rigoureuse et équilibrée de la présente charte d'usage des outils numériques. À ce titre, des actions de sensibilisation, de contrôle et d'accompagnement sont mises en œuvre.

Les agents bénéficient d'une formation ou d'informations régulières sur les bonnes pratiques numériques et la sécurité informatique. Le service informatique reste disponible pour répondre à toute question relative à l'application de la charte, dans une logique d'accompagnement et de prévention.

Des contrôles techniques peuvent être réalisés afin de vérifier le bon fonctionnement des systèmes, de détecter d'éventuels incidents de sécurité et de s'assurer du respect des règles d'usage. Ces contrôles sont effectués dans le respect de la réglementation en vigueur, notamment en matière de protection de la vie privée.
Certaines actions, telles que les connexions ou les modifications de fichiers sensibles, peuvent faire l'objet d'une traçabilité automatique, conformément aux dispositions légales.

Le non-respect de la charte constitue un manquement aux obligations professionnelles.
Les manquements graves peuvent entraîner des sanctions disciplinaires. Sont notamment considérés comme graves :

- l'usage abusif des ressources informatiques à des fins personnelles,
- l'installation de logiciels non autorisés présentant un risque pour la sécurité,
- le contournement délibéré des mesures de sécurité,
- la consultation de sites interdits,
- la communication non autorisée d'informations confidentielles,
- l'usage inapproprié d'outils d'intelligence artificielle exposant des données sensibles.

Certains comportements peuvent constituer des fautes très graves, justifiant des sanctions disciplinaires lourdes, voire un licenciement :

- la divulgation volontaire d'informations confidentielles ou protégées,
- l'installation ou la propagation délibérée de programmes malveillants,
- l'usurpation d'identité numérique,
- l'accès frauduleux à des systèmes ou à des données,
- l'utilisation des systèmes informatiques à des fins illégales.

Enfin, certains actes peuvent également relever du droit pénal et faire l'objet de poursuites judiciaires. Cela concerne notamment :

- l'accès frauduleux à un système de traitement automatisé de données (article 323-1 du Code pénal),
- l'atteinte au secret professionnel (article 226-13 du Code pénal),
- la diffusion de contenus illicites (images, propos),
- le téléchargement ou la diffusion de contenus contrefaits.

Envoyé en préfecture le 03/06/2026
Reçu en préfecture le 03/06/2026
Publié le
ID : 031-200066819-20260528-DE_079_2026-DE

La CCV privilégie une approche fondée sur le dialogue et la prévention. L'objectif de la charte est d'accompagner les agents vers des usages numériques responsables, dans un cadre sécurisé et conforme aux obligations professionnelles.

11. ENTRÉE EN VIGUEUR DE LA CHARTE

La présente charte entre en vigueur à compter de son approbation en Conseil communautaire, après information du Comité Social Territorial. Elle est diffusée à l'ensemble des agents par voie électronique et reste accessible en permanence sur les ressources de la CCV (Fichiers\00_Fonctionnement\00_02_Ressources\Informatique\Charte_informatique).

Chaque agent est invité à prendre connaissance de la charte et à en accuser réception par la signature d'un document attestant qu'il en a pris connaissance et qu'il s'engage à en respecter les dispositions.

Lors de leur arrivée dans la CCV, les nouveaux agents reçoivent la charte et bénéficient d'une présentation de ses principes. Une formation aux bonnes pratiques numériques leur est proposée dans les premiers mois suivant leur prise de fonction.

Compte tenu de l'évolution rapide des technologies, des usages numériques et des menaces en matière de cybersécurité, la charte fait l'objet d'une révision régulière.

Elle peut être adaptée pour tenir compte des évolutions technologiques, des modifications réglementaires, des retours d'expérience, des incidents constatés ou des évolutions organisationnelles de la CCV.

Les agents sont encouragés à faire remonter au service informatique toute suggestion d'amélioration ou toute difficulté rencontrée dans l'application de la charte. Toute modification substantielle fera l'objet d'une information spécifique à l'ensemble des agents.

Envoyé en préfecture le 03/06/2026
Reçu en préfecture le 03/06/2026
Publié le
ID : 031-200066819-20260528-DE_079_2026-DE

ANNEXES

Annexes :

- N°1 : Récépissé d'engagement
- N°2 : Bonnes pratiques au quotidien
- N°3 : Connexion VPN et travail à distance
- N°4 : Infographie nommage des fichiers

Envoyé en préfecture le 03/06/2026
Reçu en préfecture le 03/06/2026
Publié le
ID : 031-200066819-20260528-DE_079_2026-DE

ANNEXE 1 : RÉCÉPISSÉ D'ENGAGEMENT

Je soussigné(e) :

Nom :

Prénom :

Service :

Fonction :

En tant qu'utilisateur(trice) des moyens et outils numériques mis à disposition par la Communauté de Communes du Volvestre, je déclare avoir pris connaissance de la charte d'usage des outils numériques et de la sécurité de l'information, et m'engage à en respecter l'ensemble des dispositions dans l'exercice de mes fonctions.

Je suis informé(e) que le non-respect de ces règles peut constituer un manquement aux obligations professionnelles et entraîner des sanctions disciplinaires proportionnées à la gravité des faits, voire, dans certains cas, des poursuites pénales conformément à la législation en vigueur.

Je m'engage également à :

- Signaler tout incident de sécurité dont j'aurais connaissance ;
- Respecter la confidentialité des informations professionnelles ;
- Participer aux formations proposées par la CCV en matière de sécurité numérique et de bonnes pratiques.

Fait à :

Le :

Signature de l'agent :

Document établi par le Service Informatique – Communauté de Communes du Volvestre
Version 2025

ANNEXE 2 : BONNES PRATIQUES AU QUOTIDIEN

Chaque matin
- ☐ Vérifier que mon poste de travail n'a pas été utilisé en mon absence.
- ☐ Consulter ma messagerie et signaler tout message suspect.
- ☐ M'assurer qu'aucun mot de passe n'est à renouveler.

Pendant la journée
- ☐ Verrouiller mon poste à chaque absence, même brève.
- ☐ Ne jamais laisser de documents confidentiels visibles.
- ☐ Réfléchir avant de cliquer sur un lien ou d'ouvrir une pièce jointe.
- ☐ Vérifier les destinataires avant d'envoyer un message sensible.
- ☐ Utiliser les espaces de stockage réseau plutôt que le disque local.
- ☐ Appliquer la règle des 3 questions avant toute action sensible :
  - Est-ce que je connais la source ?
  - Est-ce cohérent avec ce que j'attends ?
  - Que se passe-t-il dans le pire des cas ?
- ☐ En cas de doute, contacter le service informatique, un collègue ou sa hiérarchie.
- ☐ Signaler tout incident ou comportement anormal, même mineur.

En fin de journée
- ☐ Ranger les documents papier confidentiels.
- ☐ Fermer toutes les applications et sessions ouvertes.
- ☐ Éteindre mon poste de travail (sauf consigne contraire).
- ☐ Verrouiller physiquement mon bureau si nécessaire.

Messagerie
- Consulter mes courriels 2 à 3 fois par jour, pas en continu.
- Traiter les messages par ordre de priorité.
- Utiliser des dossiers et règles de tri automatique.
- Me désabonner des newsletters non essentielles.

📁 **Gestion documentaire**

- Adopter une nomenclature claire et cohérente pour mes fichiers.
- Ranger les documents au fur et à mesure.
- Utiliser la fonction de recherche plutôt que de dupliquer les fichiers.
- Archiver régulièrement les documents obsolètes.

🤝 **Travail collaboratif**

- Utiliser les espaces partagés pour les documents d'équipe.
- Indiquer clairement la version et le statut des documents (brouillon, validé, etc.).
- Communiquer sur l'avancement des dossiers communs.
- Respecter l'organisation collective des répertoires partagés.

🛠️ **Confort et matériel**

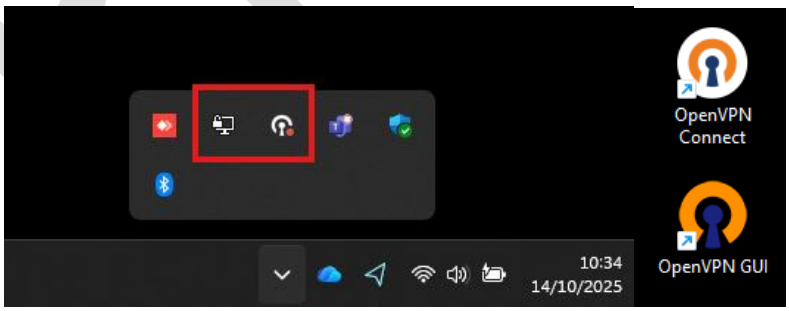
- Signaler tout matériel défectueux ou inadapté.
- Demander un aménagement de poste si nécessaire.
- Consulter la médecine du travail en cas de fatigue visuelle ou de troubles physiques.

ANNEXE 3 : ACCÈS VPN

Dans le cadre du travail à distance (télétravail ou accès en dehors des sites de la CCV), les agents doivent utiliser un client VPN (Virtual Private Network) installé par le service informatique pour se connecter de manière sécurisée au réseau interne. Une fois la connexion établie, ils peuvent accéder aux fichiers hébergés sur le serveur.

⚠️ Seuls les agents équipés d'un ordinateur portable fourni par la CCV peuvent bénéficier de ce mode d'accès. L'utilisation d'ordinateurs personnels est strictement exclue pour des raisons de sécurité.

Deux versions du client VPN peuvent être utilisées. Elles sont identifiables dans la zone encadrée en rouge sur la capture d'écran ci-dessous :



OPENVPN GUI :

Le client VPN à utiliser est identifiable par une icône représentant un écran avec un cadenas. Lorsque celui-ci est inactif, il n'affiche aucune couleur de fond.

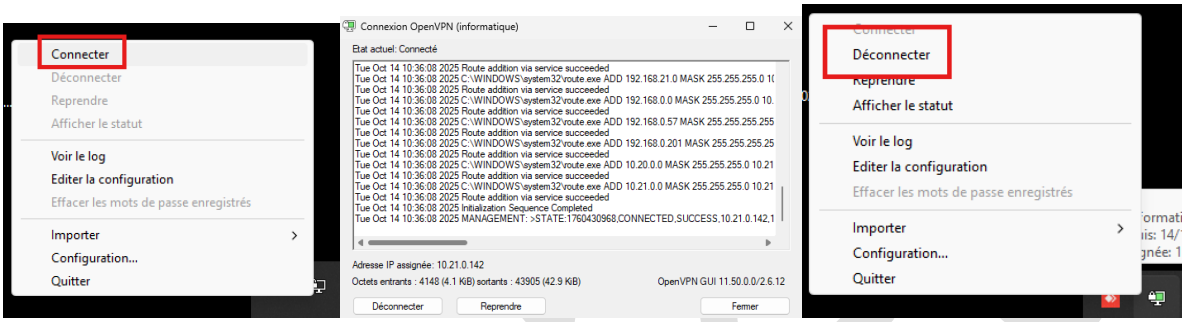
🔐 **Connexion**

1. Cliquez avec le bouton droit de la souris sur l'icône.
2. Sélectionnez « Connecter ».
3. Une fenêtre temporaire s'ouvre, puis l'icône dans la barre des tâches passe à un fond vert, indiquant que la connexion est établie.

🔓 Déconnexion

À la fin de votre session :

1. Refaites un clic droit sur l'icône.
2. Choisissez « Déconnecter » pour fermer la connexion VPN.



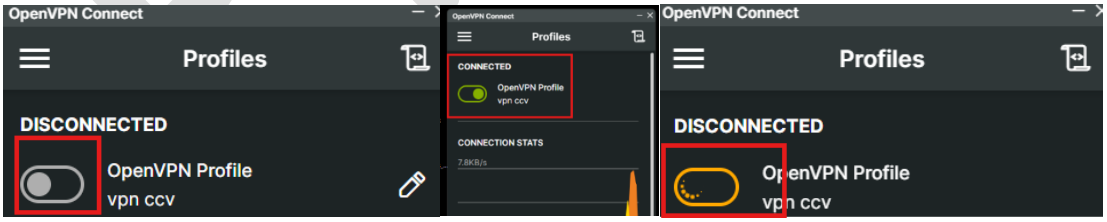
⚠️ En cas de problème

Si la fenêtre ne se ferme pas correctement ou si l'icône reste jaune, cela signifie que la connexion n'a pas été établie. Dans ce cas, contactez le service informatique.

OPENVPN CONNECT :

🔓 Connexion via l'interface en forme de trou de serrure :

- Avant connexion : Le voyant est rouge.
- Pour se connecter : Cliquez simplement sur l'icône, puis faites glisser le curseur vers la droite. Une fois la connexion établie, le voyant passe au vert et la mention « CONNECTED » apparaît au-dessus du curseur.
- Pour se déconnecter : En fin de session, faites glisser le curseur vers la gauche.



⚠️ En cas de problème :

Si le curseur reste orange et tourne en boucle (voir capture 3), cela signifie que la connexion n'a pas pu s'établir. Dans ce cas, contactez le service informatique.

Envoyé en préfecture le 03/06/2026
Reçu en préfecture le 03/06/2026
Publié le
ID : 031-200066819-20260528-DE_079_2026-DE

ANNEXE 4 : RÉFÉRENTIEL MARIANNE

MARIANNE
Les engagements qualité

LE SERVICE PUBLIC S'ENGAGE POUR AMÉLIORER LA QUALITÉ DE SERVICE

DES INFORMATIONS QUI RÉPONDENT À VOS ATTENTES, UNE ORIENTATION EFFICACE

Engagement 1 Nous vous apportons les **informations indispensables** à la réalisation de vos démarches et nous veillons à leur **mise à jour** sur tous les supports.

Engagement 2 Nous **facilitons l'utilisation de nos services** sur internet et la réalisation de vos démarches en ligne.

Engagement 3 Nous vous orientons vers **le bon service** ou vers la **bonne administration** et nous **vous aidons** à réaliser vos démarches.

UN ACCUEIL AIMABLE ET ATTENTIONNÉ

Engagement 4 Nous vous accueillons **avec courtoisie** dans le respect mutuel, nous vous **informons de votre délai d'attente**, et nous veillons à **votre confort**.

Engagement 5 Nous **facilitons l'accès aux démarches** pour les personnes en situation de handicap.

Engagement 6 Nous **accueillons de manière adaptée** les personnes en difficulté.

DES RÉPONSES CLAIRES DANS LES DÉLAIS ANNONCÉS

Engagement 7 Nous répondons de **façon claire et précise** à vos demandes et à vos réclamations :

- dans un **délai maximum d'une semaine** lorsqu'elles sont adressées par voie électronique (courriels, formulaires de contact en ligne, téléprocédures).
- dans un **délai maximum de deux semaines** lorsqu'elles sont adressées par courrier.

Engagement 8 Nous **répondons à tous vos appels** en limitant au maximum votre temps d'attente.

À VOTRE ÉCOUTE POUR PROGRESSER

Engagement 9 Nous utilisons vos remarques et vos suggestions pour **améliorer nos services.**

Engagement 10 Nous **évaluons régulièrement votre satisfaction** et nous communiquons les résultats de ces évaluations.

LE SERVICE PUBLIC S'ENGAGE AUPRÈS DE SES AGENTS

Engagement 11 Nous **formons nos collaborateurs** et nous leur donnons les **outils nécessaires** pour leur permettre d'orienter et de **faciliter les démarches** des usagers.

Engagement 12 Nous **évaluons nos pratiques**, nous impliquons nos collaborateurs et nous prenons en compte leurs retours pour améliorer la qualité de service.

+ Pour connaître vos droits et réaliser vos démarches, consultez **www.service-public.fr**, le site officiel de l'administration française

Premier ministre
Secrétariat général pour la modernisation de l'action publique

+ Retrouvez plus d'informations sur le référentiel Marianne et le baromètre annuel de la qualité de l'accueil sur **www.modernisation.gouv.fr**

Envoyé en préfecture le 03/06/2026
Reçu en préfecture le 03/06/2026
Publié le
ID : 031-200066819-20260528-DE_079_2026-DE

ANNEXE 5 : INFOGRAPHIE DE NOMMAGE DES FICHIERS