Envoyé en préfecture le 21/07/2026
Reçu en préfecture le 21/07/2026
Publié le 21/07/2026
ID : 074-200054138-20260708-DEL_2026_100-DE

Mairie de Faverges-Seythenex

CHARTE DE SECURITE INFORMATIQUE, DU BON USAGE DES RESSOURCES INFORMATIQUES, ELECTRONIQUES ET NUMERIQUES

Table des matières

Envoyé en préfecture le 21/07/2026
Reçu en préfecture le 21/07/2026
Publié le 21/07/2026
ID : 074-200054138-20260708-DEL_2026_100-DE

1. OBJECTIFS

La présente charte a pour objectif de définir les règles d'utilisation du système d'information de la commune de Faverges-Seythenex, dans le respect de la législation en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD) et la loi Informatique et Libertés.
Elle vise à garantir la sécurité, l'intégrité et la disponibilité des ressources informatiques, tout en protégeant les données personnelles et en sensibilisant les utilisateurs aux bonnes pratiques.

Tout utilisateur du système d'information s'engage, par l'utilisation des ressources mises à disposition, à respecter les dispositions de la présente charte.

1.1. Objet de la charte

La présente charte définit les conditions générales d'utilisation des services Internet, des réseaux, des services multimédias de la commune de Faverges-Seythenex et plus généralement des moyens de communication au sein de la collectivité conformément au cadre légal et réglementaire en vue de sensibiliser et de responsabiliser l'utilisateur.

Elle vise également à informer les utilisateurs des contrôles mis en place.

Elle s'applique à l'ensemble des utilisateurs : agents permanents, contractuels, stagiaires, élus et prestataires extérieurs ayant accès aux ressources informatiques de la commune.

1.2. Champ d'application de la Charte

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques de la commune de Faverges-Seythenex, ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe.

Le système d'information comprend principalement :

- les ordinateurs fixes et portables,
- les tablettes,
- les smartphones professionnels,
- les serveurs,
- les équipements réseau,
- les logiciels,
- les applications,
- la messagerie électronique,
- Les clés USB,
- l'accès Internet,
- l'accès VPN,
- l'ensemble des données numériques de la collectivité.

L'utilisateur s'engage à prendre connaissance et à appliquer l'ensemble des dispositions de la présente charte qui a un caractère impératif.

La présente charte s'applique à toute personne qui, ayant un lien de droit statutaire ou contractuel avec la collectivité, est amenée à utiliser les outils informatiques et moyens de télécommunications mis à disposition par cette dernière, pour satisfaire à ses missions. Chaque membre du personnel sera tenu informé des adaptations via les voies de communication interne en vigueur dans l'organisme.
La direction de la collectivité s'engage, pour sa part, à mettre en œuvre tous les moyens pertinents, compte tenu de l'état des techniques, afin de garantir la meilleure sécurité possible des installations mises à la disposition des utilisateurs.

1.3. Droits et devoirs des utilisateurs

Chaque utilisateur bénéficie d'un compte nominatif et personnel permettant l'accès aux ressources informatiques nécessaires à l'exercice de ses fonctions.
L'utilisateur s'engage à :

- Utiliser les moyens informatiques mis à disposition uniquement à des fins professionnelles
- Respecter la législation en vigueur, notamment en matière de propriété intellectuelle et de protection des données personnelles
- Préserver la confidentialité de ses identifiants et mots de passe
- Signaler immédiatement toute anomalie ou incident de sécurité au service informatique
- Ne pas installer de logiciel sans autorisation préalable
- Ne pas modifier la configuration matérielle ou logicielle des équipements

Un usage privé modéré et raisonnable de la messagerie et d'Internet est toléré, sous réserve qu'il ne nuise pas au bon fonctionnement du service et reste compatible avec les obligations professionnelles.

1.4. Sanctions

Chaque utilisateur est responsable pénalement pour les infractions qu'il aurait commises par ou au moyen des outils informatiques ou des moyens de communication mis à disposition.
Chaque utilisateur est responsable civilement pour les dommages qu'il aurait causés par ou au moyen des outils informatiques ou des moyens de communication mis à disposition, pour autant qu'il s'agisse d'une faute lourde, de manœuvres frauduleuses ou d'une faute légère ayant un caractère répétitif.

Cela signifie que l'abus des moyens de communication et des outils informatiques mis à disposition par la collectivité peut donner lieu au dépôt d'une plainte en justice ou une requête en indemnisation du dommage.

Le non-respect des règles et mesures de sécurité figurant dans la présente charte expose l'utilisateur, membre du personnel, selon la gravité des infractions et leurs répercussions, à l'application de sanctions disciplinaires.

En outre, la direction de la collectivité se réserve le droit d'engager des poursuites pénales conformément aux dispositions légales en vigueur.
La Collectivité se réserve le droit de contrôler l'utilisation des ressources informatiques dans le respect de la législation en vigueur.

Les contrôles peuvent porter sur :

- Les journaux de connexion et d'activité
- Les flux de messagerie (hors messages identifiés comme privés)
- L'utilisation des espaces de stockage

Le non-respect de la présente charte peut entraîner :

- Un rappel à l'ordre
- Une limitation ou suspension de l'accès aux ressources informatiques.
- Des sanctions disciplinaires pouvant aller jusqu'au licenciement ou à la radiation des cadres.
- Des poursuites judiciaires en cas d'infraction pénale

Les sanctions sont proportionnées à la gravité du manquement constaté.

2. RÈGLES DE SÉCURITÉ

2.1. Sauvegarde des données :

Les utilisateurs doivent enregistrer leurs documents sur les espaces de stockage partagés prévus à cet effet. Des sauvegardes automatiques sont effectuées quotidiennement.

2.2. Confidentialité de l'information et obligation de discrétion

Les agents de la collectivité sont soumis au secret professionnel. Les personnels se doivent de faire preuve d'une discrétion absolue dans l'exercice de leur mission. Un comportement exemplaire est requis dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques est limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées et de les utiliser. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.
Les utilisateurs s'engagent à ne traiter les données personnelles qu'aux seules fins professionnelles autorisées et à respecter la confidentialité des informations auxquelles ils ont accès.

2.3. Protection de l'information

Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Il est important de ne stocker aucune donnée ni aucun document sur ces postes (disques durs locaux). Les bases de données associées aux applications sont implantées sur des serveurs centraux implantés dans des salles protégées. De même, les documents bureautiques produits doivent être stockés sur les serveurs de fichiers, pour lesquels l'utilisateur a reçu une autorisation. Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

L'utilisateur ne doit pas transformer, sans autorisation, des informations professionnelles en informations personnelles, toute donnée ou document professionnel étant propriété exclusive de la collectivité.

Le cas échéant, ceux qui utilisent un matériel portable (exemples : poste, tablette, smartphone, …) ne doivent pas le mettre en évidence pendant un déplacement, ni exposer son contenu à la vue par exemple d'un voisin dans les transports en commun (train…) ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD/DVD, clefs USB, disques durs…).

Envoyé en préfecture le 21/07/2026
Reçu en préfecture le 21/07/2026
Publié le 21/07/2026
ID : 074-200054138-20260708-DEL_2026_100-DE

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les médias de stockage amovibles (exemples : clefs USB, CD/DVD, disques durs…) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données. Leur usage doit être fait avec une très grande vigilance. La collectivité se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.

2.4. Usage des ressources informatiques

L'utilisateur n'est en aucun cas habilité à installer des logiciels, programmes ou nouveaux équipements.
L'installation de logiciels sur des ordinateurs reliés au réseau de l'organisme est de la compétence exclusive du chef de service du Service informatique.

L'usage de toutes plateformes de fichiers partagés via internet (drive ou cloud) est formellement interdit en l'absence d'autorisation préalable du service informatique.

L'utilisateur s'engage à ne pas modifier la configuration des ressources (matériels, réseaux…) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées de la collectivité.

Les logiciels commerciaux acquis par la collectivité ne doivent pas faire l'objet de copies de sauvegarde par l'utilisateur, ces dernières ne pouvant être effectuées que par les personnes habilitées de l'établissement.

Les équipements personnels (ordinateurs, tablettes, smartphones…) ne doivent en aucune circonstance être connectés au réseau filaire de l'établissement. Une demande d'autorisation d'accès au réseau doit préalablement être transmise au service informatique avant toute tentative de connexion.
L'usage d'un équipement personnel dans les locaux de la collectivité se fait sous l'unique et entière responsabilité de son propriétaire. En aucune circonstance, la collectivité ne peut être tenue responsable de dégradation ou de vol de cet équipement.

2.5. Usage des outils de communication

Les outils de communication tels que le téléphone, Internet ou la messagerie sont destinés à un usage exclusivement professionnel. L'usage à titre personnel, dans le cadre des nécessités de la vie privée, est toléré à condition qu'il soit très occasionnel et raisonnable, qu'il soit conforme à la législation en vigueur et qu'il ne puisse pas porter atteinte à l'image de marque de la collectivité. Il est interdit d'utiliser son adresse mail professionnelle pour s'inscrire à des sites dont l'usage ne concerne par la sphère professionnelle.

2.5.1. Usage de la messagerie électronique

La messagerie professionnelle est un outil de travail mis à disposition pour les besoins du service. Son usage doit rester professionnel et respectueux.

- **Principes de base**

La création d'un compte-messagerie fait l'objet d'une habilitation du service informatique. La messagerie permet de faciliter les échanges entre les professionnels de l'établissement, le contenu des messages envoyés doit être conforme aux dispositions juridiques en vigueur.
Les utilisateurs doivent garder à l'esprit que leurs messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant, constituer une preuve ou

un commencement de preuve par écrit ou valoir offre ou acceptation de manière à former un contrat entre la collectivité et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.
Un usage privé de la messagerie est toléré s'il reste exceptionnel. Les messages personnels doivent comporter explicitement la mention « privé » dans l'objet. A défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « privé » ne comporteront pas de signature d'ordre professionnel à l'intérieur du message.
L'usage des listes de diffusion est strictement professionnel.
Il est strictement interdit d'utiliser la messagerie pour des messages d'ordre commercial ou publicitaire, du prosélytisme, du harcèlement, des messages insultants ou de dénigrement, des textes ou des images provocants et/ou illicites, ou pour propager des opinions personnelles qui pourraient engager la responsabilité de l'établissement ou porter atteinte à son image. Les utilisateurs sont tenus par leurs clauses de confidentialité et de loyauté contractuelles dans le contenu des informations qu'ils transmettent par email.
Afin de ne pas surcharger les serveurs de messagerie, les utilisateurs veilleront à éviter l'envoi de pièces jointes volumineuses, notamment lorsque le message comporte plusieurs destinataires. Seules les pièces jointes professionnelles de type « documents » ou « images » sont autorisées. Il est rappelé que le réseau Internet n'est pas un moyen de transport sécurisé.
Il est strictement interdit d'ouvrir ou de lire des messages électroniques d'un autre utilisateur, sauf si ce dernier a donné son autorisation explicite.
L'accès à la messagerie professionnelle depuis un poste extérieur est soumis à l'agrément du service informatique. L'usage de la messagerie pour envoi de données sensibles (données de santé par exemple) n'est pas approprié.

- **Bonnes pratiques :**
  - Utiliser une signature électronique conforme au modèle de la commune
  - Rédiger des objets de message clairs et explicites
  - Le champ « destinataire » (A:) est réservé aux personnes devant mener une action relative au contenu du courriel.
  - Le champ « copie » (Cc:) est réservé aux personnes destinataires du courriel pour information.
  - Le champ « copie cachée » (Cci:) est réservée à la protection de la vie privée des destinataires lorsqu'on ne désire pas divulguer leur adresse de messagerie. En dehors de ce cas de figure, l'utilisation du champ

Cci est à utiliser avec parcimonie. L'utilisateur doit éviter l'envoi de copies (Cc : ou Cci:) à un nombre injustifié de destinataires.

  - L'utilisateur ne doit pas utiliser de fond d'écran dans ses messages.
  - Les mails doivent être signés et contenir l'identité de l'expéditeur.
  - Privilégier la sobriété numérique : Éviter les pièces jointes volumineuses, utiliser des outils de partage pour les fichiers lourds Ne pas transférer d'informations confidentielles sans chiffrement Éviter l'envoi massif de messages et l'utilisation abusive de la fonction " répondre à tous"

- **Gestionnaire d'absence au bureau**

Le gestionnaire (ou indicateur) d'absence du bureau est une fonctionnalité de la messagerie qui permet aux agents absents de répondre automatiquement aux expéditeurs des courriels envoyés pendant leur période d'absence du bureau, en particulier lorsque la continuité de service s'impose, pour améliorer l'accueil et pour faciliter le traitement de l'information. Il appartient à chaque agent de régler le gestionnaire d'absence du bureau de sa propre boite aux lettres ou d'une boite aux lettres sur laquelle il a délégation, avant toute période d'absence, et de s'assurer qu'il est bien désactivé à son retour.

Les informations communément indiquées dans le courriel de réponse automatique sont :

- La date de retour
- La(les) personne(s) à contacter pour assurer la continuité de service pendant cette période.

- **Conservation des messages :**

Les messages électroniques professionnels constituent des documents administratifs et sont archivés conformément aux durées légales de conservation.

2.5.2. Usage d'Internet

L'accès à Internet est accordé dans le cadre de l'activité professionnelle. La navigation doit respecter les principes déontologiques du service public.
L'accès à l'Internet a pour objectif d'aider les personnels à trouver des informations nécessaires à leur mission usuelle, ou dans le cadre de projets spécifiques.
Il est rappelé aux utilisateurs que, lorsqu'ils « naviguent » sur internet, leur identifiant est enregistré. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de internet et à ne pas mettre en danger l'image ou les intérêts de la collectivité

- Sont strictement interdits :
  - La consultation de sites à caractère illicite, pornographique, violent ou discriminatoire.
  - Le téléchargement illégal de contenus protégés par le droit d'auteur.
  - L'utilisation de services de streaming à des fins personnelles pendant le temps de travail.
  - Toute activité portant atteinte à la réputation de la collectivité.

La commune se réserve le droit de mettre en place des dispositifs de filtrage et de contrôle de la navigation. Les logs de connexion peuvent être consultés dans le respect de la législation en vigueur.

2.5.3. Usage du téléphone

La direction de la collectivité met à la disposition de son personnel des lignes téléphoniques (fixe ou mobile).
A partir de la ligne fixe, les communications téléphoniques à caractère personnel de courte ou de longue distance (appels sortants) doivent être limitées uniquement aux cas d'urgence.
On entend par cas d'urgence les situations qui ne peuvent attendre le retour de l'agent dans la sphère privée.
Les appels entrants de courte durée peuvent être autorisés pour peu qu'ils ne perturbent pas le fonctionnement des services.
L'utilisation du téléphone est strictement interdite dans toute situation contraire au respect des règles de sécurité.

2.5.4. Usage du téléphone privé

L'usage du téléphone privé doit se faire dans le respect de l'environnement professionnel et en tout état de cause de manière non abusive. Le mode silencieux ou vibreur doit être activé pendant les heures de travail.

2.6. Usage des logins et des mots de passe

Chaque utilisateur dispose d'un compte nominatif lui permettant d'accéder aux applications et aux systèmes informatiques de l'établissement. Ce compte est personnel. Il est strictement interdit d'usurper une identité en utilisant ou en tentant d'utiliser le compte d'un autre utilisateur ou en agissant de façon anonyme dans le système d'information.

Pour utiliser ce compte nominatif, l'utilisateur doit disposer d'un login et d'un mot de passe.

Les mots de passe doivent comporter au minimum 12 caractères avec majuscules, minuscules, chiffres et caractères spéciaux
Ils doivent être modifiés tous les 6 mois.
Ils ne doivent jamais être communiqués, notés ou partagés.
L'utilisation de mots de passe différents pour chaque service est recommandée.

Chaque utilisateur est responsable de ses compte et mot de passe, et de l'usage qui en est fait. Il ne doit ainsi pas mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de la collectivité dont il a l'usage. Les systèmes informatiques et les applications de la collectivité assurent une traçabilité complète des accès et des opérations réalisées à partir des comptes sur les applications, le réseau, la messagerie, l'Internet, ...
Il est ainsi possible pour la collectivité de vérifier a posteriori l'identité de l'utilisateur ayant accédé ou tenté d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.
C'est pourquoi il est important que l'utilisateur veille à ce que personne ne puisse se connecter avec son propre compte. Pour cela, sur un poste dédié, il convient de fermer ou verrouiller sa session lorsqu'on quitte son poste. Il ne faut jamais se connecter sur plusieurs postes à la fois. Pour les postes qui ne sont pas utilisés pendant la nuit, il est impératif de fermer sa session et éteindre l'ordinateur systématiquement avant de quitter son lieu de travail le soir.
Il est interdit de contourner ou de tenter de contourner les restrictions d'accès aux logiciels. Ceux-ci doivent être utilisés conformément aux principes d'utilisation communiqués lors de formations ou dans les manuels et procédures remis aux utilisateurs.
L'utilisateur s'engage enfin à signaler toute tentative de violation de son compte personnel.

3. INFORMATIQUE ET LIBERTES

3.1. Protection des données personnelles (RGPD)

Conformément au Règlement Général sur la Protection des Données (RGPD) et à la loi Informatique et Libertés modifiée, la commune de Faverges-Seythenex s'engage à protéger les données personnelles.
La création et l'utilisation de fichiers ou de traitements contenant des données personnelles doivent faire l'objet d'une description dans le registre des traitements et être conformes aux règles du RGPD (règlement général de protection des données personnelles) et de la loi informatique et libertés du 6 janvier 1978 modifiée par la loi du 26 juin 2018.
Toutes création ou modification de fichier comportant des données personnelles doit, préalablement à sa mise en œuvre, être déclarée auprès du Délégué à la Protection des Données de la collectivité qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévue, les destinataires des données, le moyen d'information des personnes fichés et les mesures de sécurité à déployer pour protéger les données. Il procède ensuite aux opérations de mise en conformité (registre des traitements, clauses spécifiques ...).
En cas de non-respect des obligations relatives à la loi informatique et libertés et au RGPD, le Délégué à la Protection des Données sera informé et pourra prendre toutes mesures conservatoires nécessaires pour mettre fin au traitement illégal ainsi qu'informer le responsable hiérarchique de l'utilisateur à l'origine du traitement illégal.

- ***Principes fondamentaux*** :

Licéité et loyauté du traitement : les données sont collectées et traitées de manière transparente et pour des finalités déterminées
Minimisation des données : seules les données strictement nécessaires sont collectées

Envoyé en préfecture le 21/07/2026
Reçu en préfecture le 21/07/2026
Publié le 21/07/2026
ID : 074-200054138-20260708-DEL_2026_100-DE

Limitation de la conservation : les données sont conservées uniquement pendant la durée nécessaire
Sécurité et confidentialité des mesures techniques et organisationnelles appropriées sont mises en œuvre

- ***Droits des personnes :***

Toute personne dont les données sont traitées dispose d'un droit d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition et de portabilité. Ces droits peuvent être exercés auprès du Délégué à la Protection des Données (DPO) de la commune.
Contact DPO : mairie@faverges.fr

3.2. Droit à l'image

L'image d'une personne ainsi que les enregistrements vidéo et sonores qui se rapportent à elle, ne peuvent être utilisés ou diffusés sans son consentement écrit.
D'une manière générale, les photos, enregistrements vidéo ou sonores que les agents peuvent être amenés à prendre dans l'exercice de leurs fonctions ne doivent donc pas permettre d'identifier directement ou indirectement des personnes physiques, ou tout autre élément étranger au dossier traité (ex : plaques d'immatriculations, enseignes, etc…) qui doivent, le cas échéant, être floutés.
Les photos, enregistrements vidéo ou sonores pris dans le cadre des activités de la collectivité ou dans ses locaux ne peuvent pas être utilisés à des fins personnelles, et sont interdits à la diffusion externe sans le consentement écrit de la direction.

4. DISPOSITIONS PARTICULIERES

4.1. Image de marque de la collectivité

Les utilisateurs de moyens informatiques ne doivent pas nuire à l'image de marque de la collectivité en utilisant des moyens, que ce soit en interne ou en externe, à travers des communications d'informations à l'extérieur de la collectivité ou du fait de leurs accès à Internet.

4.2. Télétravail et mobilité

Les agents autorisés à télétravailler ou en déplacement professionnel doivent respecter des règles de sécurité renforcées :

- Utiliser exclusivement le matériel fourni par la commune
- Se connecter au réseau de la collectivité via VPN sécurisé
- Ne jamais laisser le matériel sans surveillance dans un lieu public
- Verrouiller systématiquement l'écran lors des absences
- Ne pas connecter de support amovible personnel non autorisé
- Signaler immédiatement toute perte ou vol de matériel

Les équipements nomades doivent être chiffrés et protégés par un mot de passe fort.

4.3. Réseaux sociaux et communication numérique

- **Usage professionnel :**

Seules les personnes habilitées peuvent communiquer au nom de la commune sur les réseaux sociaux. Toute publication doit respecter la charte de communication de la collectivité.

Envoyé en préfecture le 21/07/2026
Reçu en préfecture le 21/07/2026
Publié le 21/07/2026
ID : 074-200054138-20260708-DEL_2026_100-DE

- **Usage personnel :**

Les agents peuvent s'exprimer librement sur les réseaux sociaux dans le respect de leurs obligations de réserve et de discrétion professionnelle. Ils ne doivent pas :
Divulguer d'informations confidentielles ou sensibles
Tenir des propos portant atteinte à l'image de la commune
Utiliser le logo ou les éléments graphiques de la commune sans autorisation

4.4. Accès aux données informatiques en cas d'absence d'un agent

L'obligation de loyauté impose à l'agent public, absent de son poste de travail en raison d'un congé ou d'un « arrêt maladie », de communiquer à la collectivité qui en fait la demande tout document nécessaire à la poursuite de l'activité du service concerné.

Récemment appliquée dans le domaine des technologies de l'information et de la communication, cette jurisprudence impose à l'agent de communiquer son mot de passe ou les fichiers en sa possession lorsque le bon fonctionnement de son service dépend des données détenues par cet agent.
Les modalités d'accès de la collectivité aux données stockées sur l'environnement informatique d'un agent absent (messagerie, fichiers, supports de stockage) sont les suivantes :

- Un tel accès ne peut avoir lieu que dans le cas où il s'avère nécessaire à la poursuite de l'activité du service concerné
- Seul le Chef de service dont dépend l'agent absent peut demander l'accès à son environnement informatique. Il doit pour cela motiver sa demande auprès du responsable du service informatique qui doit en vérifier le caractère professionnel

4.5. Gestion des incidents et violations de données

Notre collectivité peut faire l'objet d'attaques virales qui utilisent la messagerie au travers d'emails piégés qui ne peuvent pas être filtrés par les dispositifs de sécurité habituels.
La seule protection réside dans le respect le plus strict des consignes suivantes :

- Tout email non sollicité ou inattendu est suspect, particulièrement s'il comporte une pièce jointe ou demande des informations personnelles. Il faut impérativement le supprimer
- En aucune circonstance, ne doit être exécuté un logiciel reçu en pièce jointe d'un email, ou suivre un lien reçu dans un email qui demande des informations personnelles ou propose l'exécution d'un logiciel
- En aucune circonstance, ne doit être téléchargé sur un poste informatique de la collectivité un logiciel provenant d'Internet pour ensuite l'installer sur votre poste. Seuls les agents du service informatique sont habilités à procéder à des installations de logiciels sur les postes de travail.

Mesures d'urgence à appliquer en cas d'infection avérée ou supposée par un virus :

- Ne pas suivre les instructions qui s'affichent à l'écran
- Déconnecter l'ordinateur du réseau en enlevant le câble RJ45 et/ou désactiver le WIFI
- Ne pas éteindre le poste et ne plus l'utiliser
- Avertir le service informatique par téléphone au 06.19.45.85.93 qui prendra contact avec vous dans les meilleurs délais. Laisser un message en cas de répondeur.

Tout incident de sécurité (perte de données, accès non autorisé, infection virale, vol de matériel) doit être signalé immédiatement au service informatique et au responsable hiérarchique.
En cas de violation de données personnelles susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, la commune notifiera la CNIL dans un délai de 72 heures conformément au RGPD.

Envoyé en préfecture le 21/07/2026
Reçu en préfecture le 21/07/2026
Publié le 21/07/2026
ID : 074-200054138-20260708-DEL_2026_100-DE

4.6. Sensibilisation et formation

La commune s'engage à former et sensibiliser régulièrement les utilisateurs aux enjeux de sécurité informatique et de protection des données personnelles.
Les utilisateurs sont encouragés à solliciter le service informatique pour toute question relative à la sécurité ou à l'usage des outils numériques.

5. ENTRÉE EN VIGUEUR

5.1. Date d'entrée en vigueur

La présente charte entre en vigueur dès sa signature.

5.2. Publicité

La présente charte sera transmise au personnel.
Les utilisateurs devront obligatoirement signer le récépissé ci-dessous.

6. EVOLUTION DE LA CHARTE

La présente charte pourra être modifiée pour s'adapter aux évolutions technologiques, réglementaires ou organisationnelles. Les utilisateurs seront informés de toute modification.
Cette charte a été élaborée en concertation avec les instances représentatives du personnel et validée par délibération du conseil municipal.

- Fait à Faverges Seythenex le ……

Engagement de l'utilisateur

Je soussigné (e)

Nom et Prénom : ……

Direction/Service : ……
En tant qu'utilisateur du système d'information et de communication de la commune de Faverges Seythenex, déclare :

- Avoir pris connaissance de la charte qui m'a été remise
- M'engage à la respecter pendant toute la durée de mes fonctions, et sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

Fait à …… Le ……

Signature, précédée de la mention « Lu et approuvé »

Principaux textes de références

- Le règlement (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données,
- La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et libertés,
- La loi n°78-17 du 06/01/78 dite « Informatique et liberté » modifiée par la loi n°2018-493,
- La loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques,
- La loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,
- La législation relative à la propriété intellectuelle,
- La législation relative à la fraude informatique,
- La législation en matière de transmission d'informations à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine et à la diffusion de contenus illicites à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste et sexiste (articles 227-23 et 227-24 du code pénal et loi du 29 juillet 1881),
- Le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques,
- La 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,
- Les dispositions du code pénal relatives à la fraude informatique et aux atteintes aux droits de la personne et notamment les articles 226-1, 226-15 à 226-24, 321-1 à 323-7,
- L'ensemble des dispositions statutaires et notamment la 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,
- La circulaire du 12 mars 1993 relative aux modalités de l'application de la loi "informatique et libertés" au secteur public,
- Le guide d'hygiène informatique -Agence nationale de la sécurité des systèmes d'information –Janvier 2017

Envoyé en préfecture le 21/07/2026
Reçu en préfecture le 21/07/2026
Publié le 21/07/2026
ID : 074-200054138-20260708-DEL_2026_100-DE

🗝 *6 points clés à retenir*

- **Puis-je utiliser les moyens mis à ma disposition à titre privé ?**

Avant tout professionnel, un usage privé est cependant toléré s'il est modéré, loyal, non lucratif et qu'il ne nuit pas à l'accomplissement des missions de service public de l'utilisateur. Tout usage privé doit-être identifié comme tel (répertoire nommé « Privé », mention « Privé » dans l'objet des messages ou en cochant la case privée pour l'agenda). L'utilisation de matériels et supports de stockage personnels est quant à elle proscrite.

- **Données à Caractère Personnel (DCP) :**

La constitution de fichiers de DCP est obligatoirement soumise à l'avis du Délégué à la Protection des Données (DPD) et ne doit pas être réalisée sans sa sollicitation.

- **Mot de passe :**

Il est strictement individuel, confidentiel et doit être robuste.
Vos identifiants et mots de passe personnels ne doivent jamais être écrits, partagés ou révélés, c'est votre responsabilité qui est en jeu.

- **Poste de travail :**

Les utilisateurs doivent systématiquement verrouiller la session lorsqu'ils s'absentent ou quittent leur poste de travail, même pour une durée très courte.

- **Stockage des documents professionnels :**

Il ne doit pas être réalisé sur le disque « C : » ou « D : » mais sur une ressource partagée du réseau afin qu'ils puissent être sauvegardés.

- **Avec mes mails :**

Je n'ouvre pas un message d'un expéditeur inconnu.
Je n'ouvre pas de pièce jointe sans être sûr du contenu.