Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

PONT-L'ABBÉ
Pont-'n-Abad

CHARTE INFORMATIQUE

Charte d'utilisation des ressources informatiques au sein de la commune de Pont-L'Abbé

Préambule

Au sein de la commune de Pont-L'Abbé, ci-après dénommée « **la Collectivité** », les agents utilisent quotidiennement des outils informatiques et de communications nécessaires au bon déroulement de leur mission.

En raison de l'importance centrale que l'outil informatique prend dans le travail quotidien, la collectivité a décidé de se doter de la présente charte qui a pour objet de fixer les règles d'utilisation des moyens informatiques et de communication électronique au sein des services.

La présente charte informatique est destinée aux utilisateurs des outils informatiques et de communications de la collectivité au regard du développement de la gestion informatisée des données personnelles au sens du Règlement Général sur la Protection des Données, issu des instances européennes (RGPD, règlement nº 2016/679 mis en vigueur le 25 mai 2018 en France). Puis, la cybersécurité invite les employeurs et les utilisateurs à faire preuve de plus en plus de vigilance dans l'utilisation des nouvelles techniques de communication et d'information.

La charte informatique teint compte notamment des recommandations de la Commission nationale de l'Informatique et des Libertés (CNIL) ou celle de l'agence nationale de la sécurité des systèmes d'information (Anssi).

Cette charte s'applique à l'ensemble du personnel, titulaires et contractuels, ainsi qu'aux intérimaires, stagiaires et apprentis ayant un droit d'accès aux ressources informatiques, aux services internet, de messageries et téléphoniques, ainsi que tout moyen de connexion à distance (ordinateurs, tablettes, téléphones, portables, imprimantes, logiciels) dans le cadre de leur travail.

Elle a pour finalité d'informer les agents des modalités d'utilisation de ces outils, des risques et des failles, d'en préconiser leur utilisation et d'assurer une transparence. Elle pourra évoluer en fonction du contexte légal et, le cas échéant, de la politique de sécurité de la collectivité.

Cette charte informatique est adoptée après consultation du Comité Social Territorial. Elle permet à **la Collectivité** d'assurer de manière optimum et efficace la sécurité de ses systèmes d'information et de garantir un usage loyal, respectueux et responsable des moyens informatiques et de communication électronique, ainsi que de protéger le patrimoine et l'image de la collectivité.

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

Chaque agent se doit de respecter les règles déontologiques et professionnelles, les procédures de travail, l'organisation et les règles de délégation, la communication d'informations et l'utilisation de ces moyens informatiques.

La charte est décomposée en quatre parties :

I/ Données à caractère personnel

II/ Missions des administrateurs

III/ Mesures de sécurité et modalités d'utilisations

IV/ Responsabilités et sanctions

Lexique

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

PONT-L'ABBÉ
Pont-'n-Abad

I/ Données à caractère personnel

Les données à caractère personnel sont toute(s) information(s) désignant directement ou indirectement une personne physique. Le Règlement Général sur la Protection des Données (RGPD, règlement nº 2016/679 mis en vigueur le 25 mai 2018) encadre les traitements qui sont réalisés sur ces données et renforce les droits individuels.

- Quelles sont mes garanties concernant mes données nominatives au sein de la Collectivité dans le cadre des utilisations des outils informatiques ?

- Je suis informé(e) que l'utilisation des données à caractère personnel me concernant (adresse IP, adresse MAC, date, heure de connexion, durée de connexion, trace de navigation, etc.) sera effectuée dans l'intérêt légitime poursuivi par **la Collectivité** (désignée Responsable de traitement), qui est de sécuriser les services, les outils et les réseaux et d'éviter toutes fuites externes (risques juridiques, économiques et techniques), et d'assurer une organisation interne correspondant aux règles déontologiques et professionnelles, en respectant les droits individuels.
- Je suis informé(e) que les finalités poursuivies sont d'assurer la sécurité des réseaux et des outils informatiques, de limiter les risques d'abus d'une utilisation trop personnelle d'internet, du téléphone ou de la messagerie.
- Je suis informé(e) que mes données sont à destination des administrateurs désignés (service informatique).
- Je suis informé(e) que la durée de conservation des données est limitée à ce qui est nécessaire au fonctionnement des outils informatiques ou de communication et de mes missions, soit 6 mois maximum pour les logs de connexion (système de journalisation).
- Je bénéficie de droits (accès, rectification, effacement, limitation, portabilité, opposition) relatifs à l'utilisation de mes données.
- J'ai le droit d'introduire des réclamations auprès de l'autorité de contrôle qu'est la Commission nationale de l'Informatique et des Libertés (CNIL).

Lorsque je suis amené(e) à collecter des données à caractère personnel dans le cadre de mes missions, je dois m'assurer que la collecte soit loyale, licite et transparente.
En cas de doutes, vous pouvez consulter le délégué à la protection des données de la collectivité (Centre de Gestion du Finistère, mail : protection.donnees@cdg29.bzh).

- Quelles sont les clauses spécifiques concernant le traitement des données sensibles et le renforcement de l'obligation de confidentialité ?

Chaque agent est responsable de l'utilisation des informations auxquelles il accède dans le cadre de ses fonctions. L'accès aux dossiers, fichiers et applications doit être strictement limité aux besoins liés à l'exercice des missions confiées.

Il est formellement interdit de consulter, modifier ou extraire des informations sans motif professionnel légitime, même en l'absence de diffusion de ces informations.

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

Les agents sont tenus à une obligation de discrétion et de confidentialité absolue concernant les données dont ils ont connaissance, en particulier lorsque celles-ci présentent un caractère sensible, notamment dans le domaine social.

Tout manquement à ces obligations est susceptible d'engager la responsabilité disciplinaire de l'agent, sans préjudice d'éventuelles poursuites civiles ou pénales prévues par les textes en vigueur.

- Quelle Quelles sont mes garanties concernant mes données nominatives au sein de la Collectivité s sont les sanctions encourues en cas de non-respect sur les données à caractère personnel ?

Les sanctions de la CNIL visent la personne physique ou morale (l'employeur) dont la responsabilité pénale et civile peut être engagée.
La **Collectivité** en sa qualité de Responsable de traitement, se réserve le droit de sanctionner disciplinairement l'agent en infraction, et peut l'exposer à des poursuites judiciaires.

II/ Missions des administrateurs

La **Collectivité** met à disposition des agents les moyens techniques (informatique et communication) et humains (administrateurs) nécessaires au bon déroulement de leur mission.
La **Collectivité** assure donc la sécurité technique et le fonctionnement des moyens techniques, par les missions de ses administrateurs.

➡ Ils assurent et maintiennent la sécurité du système

Notamment par l'installation du système d'exploitation de mon ordinateur et des mises à jour nécessaires (mission exclusive des administrateurs). Ils sécurisent les postes de travail par des procédures de verrouillage automatique de sessions au bout de 5 minutes d'inactivité. Ils surveillent les systèmes d'information par des logiciels régulièrement mis à jour et des pares-feux, ils sécurisent l'informatique mobile par des codes de déverrouillage, ils limitent les flux du réseau au strict nécessaire, sécurisent les serveurs et les sauvegardent régulièrement.

➡ Ils m'accompagnent dans l'utilisation de mes moyens informatiques et de communication

Notamment par la formation, l'assistance pour résolution de problèmes techniques, et l'information des contraintes de service liées au maintien du bon fonctionnement des moyens informatiques et de communication (ex : interruption de service, maintenance, ...).

➡ Ils interviennent sur mes outils en cas de force majeure

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

Ils peuvent avoir momentanément accès aux ressources informatiques indispensables à la poursuite de l'activité du service, si possible après m'avoir informé(e), et à l'exclusion de l'accès à mes répertoires, fichiers et messages clairement identifiés ou expressément signalés comme lieu de stockage privé (indiquer : personnel ou privé et nom prénom).

➡ Ils analysent les éléments sources de problèmes techniques

La prévention et la résolution de problèmes techniques autorisent les administrateurs à analyser un certain nombre d'éléments relatifs aux flux de trafic et aux volumes stockés et notamment :

- les fichiers stockés (format, taille, date...)
- les ressources matérielles et logicielles
- les connexions au réseau (identifiants, dates et heures de connexions...)
- les échanges via le réseau
- les connexions internet (identifiants de connexion, volumes de données transférées, date et heures de connexion...)
- les messages stockés (fréquence, taille des fichiers transmis...)

Dans ce cadre la confidentialité des données sera respectée (devoir de réserve et de secret professionnel des administrateurs). C'est un contrôle individuel des agents dans le but de protéger les réseaux et de garantir le bon usage de ces outils.

De plus, l'ensemble des informations sera conservé sur un dispositif de sauvegarde, dans la limite de la durée légale de conservation.

III/ Mesures de sécurité et modalités d'utilisations

La **Collectivité** s'assure des moyens de sécurité mis en place pour le bon fonctionnement des outils et des services. L'agent doit également s'assurer de respecter ces mesures et d'en informer les administrateurs s'il y a des failles dans les plus brefs délais.

➡ Outils informatiques

- Comment protéger les données professionnelles ?

Le login et le mot de passe : clés de l'accès aux outils informatiques
Les personnes qui ont accès au réseau informatique bénéficient d'un droit d'accès par l'utilisation d'un login et d'un mot de passe. Ceux-ci ont pour objectif de préserver la confidentialité des informations professionnelles.
Pour une efficacité optimale, il est obligatoire d'avoir un mot de passe complexe de 14 caractères.
Les login et mot de passe sont par définition personnels ; ils ne pourront être cédés que par la volonté de son bénéficiaire qui en assume alors toute la responsabilité. Pourra dès lors être sanctionnée l'usurpation d'identité d'un autre utilisateur, ou l'obtention d'un mot de passe d'un autre utilisateur sans son autorisation.

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

La **Collectivité** peut néanmoins demander à l'utilisateur de communiquer aux administrateurs ses mots de passe, s'il est absent et nécessaire à la continuité du service public. Les agents du Centre Communal d'Action Sociale ne doivent pas communiquer leur mot de passe aux administrateurs.
Enfin, afin de protéger les données professionnelles, il est demandé à tout utilisateur de verrouiller son ordinateur (touche windows + L) dès qu'il quitte son poste de travail.

Le réseau : un outil partagé
Pour une préservation des données professionnelles, tout utilisateur s'engage :
- à ne pas altérer les données ou accéder à des informations appartenant à d'autres utilisateurs, sans leur autorisation,
- à ne pas modifier ou détruire des ressources connectées au réseau sans autorisation des administrateurs ou d'un supérieur hiérarchique ou a minima sans s'être assuré que ces ressources ne sont pas utilisées par d'autres utilisateurs.

- Comment protéger mes données privées ?

Tous les fichiers ou dossiers enregistrés sur les outils informatiques sont présumés professionnels. Néanmoins, une utilisation à titre privé des outils informatiques est admise, dès lors qu'elle est raisonnable et qu'elle ne nuit pas au bon fonctionnement du service.
Les dossiers doivent être identifiés comme « privé » ou « personnel » dans leur nom pour pouvoir être protégés par le droit au respect de la vie privée des utilisateurs.

- Comment protéger le fonctionnement de mes outils informatiques ?

Afin de permettre un fonctionnement optimal du poste de travail et d'éviter tout dysfonctionnement technique, tout utilisateur s'engage :
- à ne pas interrompre, sans y être autorisé, le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau.

➡ Outils de communication

- Comment protéger mes messages professionnels ?

Les échanges électroniques avec des tiers ont la même valeur juridique que les échanges écrits. Un message électronique peut donc être une preuve ou un début de preuve, engageant l'utilisateur ou la **Collectivité**, au même titre qu'un courrier écrit.
Il est donc conseillé de conserver tous les messages, envoyés ou reçus, qui peuvent avoir une valeur contractuelle ou une valeur juridique pertinente (exemples : engagement sur une prestation, conseil statutaire sur un dossier sensible, procédure marché public...). Si les messages n'ont pas ces types de valeurs, évitez d'encombrer vos boîtes mails en les conservant.
Par ailleurs, tout utilisateur s'engage à ne pas masquer son identité, ni diffuser des informations confidentielles relatives à la **Collectivité** à ses usagers, cocontractants

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

et partenaires ou aux agents sauf si la conduite des dossiers ou le droit à l'information le requiert.
En son absence, tout utilisateur est censé avoir pris les dispositions nécessaires pour assurer la continuité du service public (ex : gestionnaire d'absence de messagerie indiquant les contacts des suppléants). Néanmoins, de façon exceptionnelle, la **Collectivité** peut être amené à accéder à la messagerie de l'utilisateur en son absence, lorsque cela est nécessaire à la continuité du service public. Ces dispositions sont également à prendre pour les messages téléphoniques.

- Comment protéger mes messages privés ?

Toute utilisation des moyens de communication est présumée professionnelle. Néanmoins, une utilisation à titre privé des moyens de communication est admise, dès lors qu'elle est raisonnable et qu'elle ne nuit pas au bon fonctionnement du service.
Les messages doivent être identifiés comme « privé » ou « personnel » dans leur objet et, si besoin, stockés dans un répertoire identifié « privé » ou « personnel » pour pouvoir être protégés par le droit au respect de la vie privée des agents et du secret des correspondances.

- Comment protéger le fonctionnement de mes outils de communication ?

Afin de ne pas provoquer de dysfonctionnements de sa messagerie, et plus globalement, de l'ensemble des messageries des agents de la **Collectivité** tout utilisateur s'engage :

- à supprimer rapidement tous les messages volumineux et sans valeur juridique pertinente, le volume des boites et des messages échangés étant limité.
- à ne pas ouvrir les fichiers exécutables rattachés des courriels (.exe, .msi,...). Il convient d'en informer rapidement l'administrateur, puis de procéder à leur suppression.
- à ne pas ouvrir les messages suspects (objet douteux, provenance d'un émetteur inconnu, pièce jointe non habituelle...). Il convient d'en informer rapidement l'administrateur, puis de procéder à leur suppression.

De plus, la prévention et la résolution de problèmes techniques autorisent les administrateurs à analyser un certain nombre d'éléments relatifs aux flux de trafic et aux volumes stockés

➡ Informatique nomade (téléphones portables, ordinateurs portables etc.) et télétravail

En cas d'utilisation hors du réseau, vous devez protéger tous vos outils. En cas de besoin d'accès au réseau à distance, vous devez demander l'autorisation de votre hiérarchie demander un outil de sécurisation de type VPN (*virtual private network*).

Lors du fonctionnement du service en télétravail, toutes les règles et recommandations citées dans ce document sont applicables.

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

- Comment protéger ces outils informatiques mobiles ?

  Afin de protéger un maximum ces outils mis à disposition lors de déplacements, il serait préférable entre autres, de ne pas les laisser à la vue de tous dans la voiture si vous n'êtes pas à l'intérieur.
  Le but est de les protéger physiquement du vol et de toute malveillance ou intrusion.

- Comment protéger l'utilisation du VPN ?

  Le VPN vous permettra d'avoir accès au réseau de partage de la **Collectivité** lors de vos déplacements. Pour se faire, vous devez vous connecter à l'internet.
  Si l'ordinateur doit rester dans la salle lors de pauses, veillez à verrouiller votre ordinateur. Si le temps d'absence est plus long, veillez à vous déconnecter du réseau partagé et à verrouiller ensuite votre ordinateur.

- Comment protéger l'usage d'un moyen de stockage externe (clé USB, disque dur externe) ?

  Dans le cadre de vos missions, vous êtes susceptible d'utiliser un moyen de stockage que vous pourrez avoir sur vous lors de vos déplacements. Il est recommandé que ce moyen soit utilisé exclusivement sur votre ordinateur ou celui d'un autre utilisateur de la **Collectivité.** Cela éviterait les virus et les intrusions malveillantes, principalement lorsque vous êtes en déplacement et que vous utilisez un ordinateur autre que celui de la **Collectivité.**

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

PONT-L'ABBÉ
Pont-'n-Abad

IV/ Responsabilités et sanctions

Comme tout employeur, **la Collectivité** est responsable des faits commis par ses agents au moyen de ses outils informatiques et de communication.

Pour une utilisation légale de ces outils, il est donc exclu que ceux-ci soient le moyen de réalisation de manquements aux obligations statutaires ou d'infractions de droit commun, l'utilisateur s'exposant dans ce cas à des sanctions disciplinaires et/ou des poursuites judiciaires.

Dans le cadre de cette responsabilité, et lorsque la **Collectivité** détient des présomptions sérieuses d'infraction aux règles de la charte, il peut être amené à contrôler la légalité de l'utilisation de ces outils par :

- une analyse du contenu des messages et fichiers professionnels,
- une analyse des connexions internet par les logs de connexion dont la durée de conservation ne dépassera pas 6 mois,
- un blocage de l'accès à certains sites considérés comme dangereux ou interdits au regard de leur contenu présumé,
- une analyse du contenu des messages privés en cas d'enquête judiciaire, ou si l'employeur a reçu une décision d'un juge l'autorisant à accéder à ces documents,
- un accès aux fichiers identifiés comme personnels ou privés en présence de l'agent ou après l'avoir appelé ou en cas de risque ou évènement particulier qu'il appartient aux juridictions d'apprécier.

Annexe unique : l'attestation de prise de connaissance et de respect des règles fixées par la présente charte informatique.

Envoyé en préfecture le 26/06/2026
Reçu en préfecture le 26/06/2026
Publié le
ID : 029-212902209-20260626-20260626_AL2-DE

PONT-L'ABBÉ
Pont-'n-Abad

LEXIQUE

Il est désigné sous le terme « la collectivité » le maire, employeur des agents. La direction pourra être dépositaire de l'autorité publique, pour exercer le rôle d'employeur. Les administrateurs pourront les assister dans le rôle qui leur est dévolu dans la présente charte.

Il est désigné sous le terme **« utilisateur »** toute personne (élu, agent, prestataire externe, stagiaire, temporaire...) ayant accès ou utilisant les ressources informatiques mises à disposition par la **Collectivité**.

Il est désigné sous le terme de **« outils informatiques »** :

- Le poste de travail
- Le réseau
- Internet et extranet
- Les badges électroniques
- Les outils communicants (Smartphone, tablette ...)

Il est désigné sous le terme de **« outils de communication »** :

- La messagerie
- Le téléphone
- Le télécopieur
- Les outils communicants (Smartphone, tablette ...)

Il est désigné sous le terme **« administrateurs »** les membres de l'équipe informatique, stagiaires compris.

Il est désigné sous le terme **« administrateurs d'application »** les utilisateurs ayant des droits avancés autres que ceux strictement nécessaires à l'utilisation basique d'un logiciel (exemple : gestion des droits des utilisateurs...).

Il est désigné sous le terme de **« données à caractère personnel »** : toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

Avis favorable du Comité Social Territorial du 20/02/2026

Délibération du Conseil Municipal du 28/04/2026

Le Maire

Stéphane LE DOARÉ

VILLE DE PONT-L'ABBÉ (Finistère)

HÔTEL DE VILLE - Square de l'Europe -29120 Pont-l'Abbé