Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

CHARTE D'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Champ d'application

La Commune de Gardanne a la volonté politique de développer l'utilisation des technologies de l'information et de la communication dans les services municipaux afin d'améliorer le service rendu au public et de permettre à ses agents de travailler dans les meilleures conditions.

La présente charte a pour objectifs la définition des conditions d'usages des outils mis à votre disposition afin de développer les bonnes pratiques, de sensibiliser les utilisateurs de la commune aux responsabilités engagées, d'identifier les règles qui s'appliquent quelle que soit la situation de travail : dans les locaux de la collectivité, en situation de mobilité ou en situation de télétravail.
Elle s'applique à l'ensemble des utilisateurs de la Commune tous statuts confondus (élus, agents, apprentis, stagiaires…), et plus généralement à l'ensemble des personnes (prestataires, partenaires, délégataires, public), utilisant les moyens informatiques ou de communication de la Commune.
Enfin, dans un contexte où la protection des données constitue un enjeu majeur pour les libertés individuelles, le respect de la charte constitue un engagement individuel permettant de diminuer les risques de fuites, de pertes, d'altération des données face notamment aux cyberattaques.

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

Table des matières

Champ d'application 1
Principes Généraux 3
1. Matériel informatique et logiciels 4
a. Les droits d'usage 4
b. Personnalisation de la connexion 4
c. Les fichiers 5
2. Protection des données personnelles 6
a. Définition 6
b. Secret professionnel 6
c. En cas de manquement à ces règles il s'expose à des risques 6
d. Le droit à la déconnexion 7
e. Journalisation des accès utilisateur et sécurité du système d'information 7
f. Les droits sur les données à caractère personnel concernant l'agent 7
g. Altération et/ou violations de données 7
3. La messagerie électronique 8
a. Les messages : 8
b. Envoi de gros fichiers 9
c. Adresse de messagerie 9
d. En cas d'absence 9
e. Piratage de compte de messagerie 9
4. La navigation sur Internet 10
5. La téléphonie, smartphones, tablettes, Internet et transmission de données 10
6. Accès externe 11
7. Sensibilisation - Action - Formation 11
8. L'administrateur 11
a. Missions 11
b. Contrôle, surveillance et archivage 11
c. Actions 12
9. Administrateur fonctionnel 12
10. Mise en application 13
11. Annexe 14
Cadre Légal (Rappel non exhaustif) 14

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

Principes Généraux

La présente Charte concerne les ressources informatiques et leurs usages, les services internet et téléphoniques de la mairie de Gardanne, 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.
Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau ;
- Ordinateurs portables ;
- Terminaux portables ;
- Copieurs, fax, téléphones ;
- Imprimantes simples ou multifonctions ;
- Tablettes ;
- Smartphones ;
- Byod (bring your own device) utilisation de matériels personnels
- Réseaux locaux et WiFi (Le WiFi est considéré comme une extension du réseau local et doit à ce titre être traité comme tel.).

La présente charte a pour but de rappeler les règles d'une bonne utilisation de ces outils dans l'intérêt des utilisateurs et de la collectivité.
Celles-ci concernent notamment : l'utilisation des matériels, les logiciels de messagerie et la navigation sur l'internet.

La mise à disposition des équipements est attribuée par l'autorité hiérarchique en accord avec la Direction Générale en fonction des besoins des agents et peut être retirée en cas de nécessité et de non-respect des clauses de cette charte.

Tout utilisateur est responsable de l'usage des ressources informatiques, téléphoniques et du réseau auxquels il a accès, il s'engage à prendre soin des matériels et des installations informatiques mis à sa disposition.
On désignera par « **administrateur** » la (ou les) personne(s) chargée(s) de la gestion du réseau informatique, et de la téléphonie.

On désignera de façon générale sous le terme « **ressources informatiques** » les moyens téléphoniques, informatiques, bureautiques ou de gestion ainsi que les données elles-mêmes, auxquelles il est possible d'accéder via le réseau local ou par WiFi ou par un accès distant (VPN).

En qualité d'utilisateur des ressources informatiques, chaque utilisateur s'engage à connaître et à appliquer l'ensemble des dispositions de la présente charte.

La collectivité s'engage pour sa part à mettre en œuvre tous les moyens pertinents et utiles, afin de garantir la meilleure sécurité possible des installations, de la protection des données et du bon fonctionnement des systèmes et logiciels mis à la disposition des utilisateurs.

1. Matériel informatique et logiciels

a. Les droits d'usage

Seuls les utilisateurs ont le droit d'accéder aux ressources informatiques.
Les postes mis à disposition sont équipés des logiciels nécessaires aux tâches professionnelles de l'agent. L'utilisateur reste responsable du matériel qui lui a été confié.

Il est interdit :

Pour le matériel :

- De le déplacer. Tout déplacement de matériel ne peut être fait que par le service informatique selon la procédure de demande d'intervention.
- De modifier ou supprimer des paramétrages systèmes et des configurations.
- De connecter un matériel sur le réseau.
- D'ajouter des périphériques.

Avant toute utilisation de support amovible (clé USB, disque numérique…), il faudra l'analyser avec les outils anti-virus installés et accepter les consignes données par ces outils (refus de lecture ou destruction des fichiers infectés).

Pour les logiciels :

- D'installer ou d'exécuter de sa propre initiative de nouveaux logiciels. Les besoins nouveaux sont à adresser au service informatique par le chef de service.
- De faire une copie d'un logiciel[7] ou de sa clé de licence.
- De contourner les restrictions d'utilisation d'un logiciel.
- D'en modifier les configurations.
- De développer ou de diffuser des virus informatiques ou programmes malveillants.
- D'utiliser des outils d'analyse et de scan du réseau.

En cas d'installation de logiciels ou matériels supplémentaires, une demande devra être faite par mail à sav-informatique@ville-gardanne.fr **ou en utilisant GLPI** https://srvsupervision/glpi/

b. Personnalisation de la connexion

Un identifiant de connexion (login) et un mot de passe (password) sont mis à disposition par le service informatique à chaque agent. **Il est nominatif donc personnel**. Des identifiants et mots de passe peuvent également être attribués pour l'accès à certaines applications. Chaque utilisateur dispose de privilèges qui lui sont propres selon ses attributions et ses responsabilités.
Aussi, afin de se conformer aux dernières préconisations en la matière, les mots de passe devront être composés à minima :
Exemple 1 : les mots de passe doivent être composés d'au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles.

Exemple 2 : les mots de passe doivent être composés d'au minimum 14 caractères comprenant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire.

Exemple 3 : une phrase de passe doit être utilisée et elle doit être composée d'au minimum 7 mots.
Cf. Recommandations de la Commission Nationale de l'Informatique et des Libertés

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

Pour des raisons tenant à la fois de la responsabilité, de la confidentialité et surtout de la sécurité, il est interdit :

- **De communiquer son identifiant et son mot de passe à toute autre personne (collaborateur, supérieur hiérarchique, et à plus forte raison à toute personne étrangère à la mairie, comme un stagiaire ou un prestataire extérieur par exemple).**
- **D'utiliser l'identifiant d'une autre personne (usurpation d'identité).**

Toutes les connexions réalisées à l'aide du mot de passe de l'utilisateur engagent la responsabilité de son propriétaire. En cas d'absence prolongée d'un agent, les utilisateurs autorisés du même service ont accès à ses documents, au sein d'un dossier partagé sur le serveur de bureautique et n'ont donc pas besoin qu'on leur transmette les identifiants de connexion de l'agent absent.

L'utilisateur prendra soin de verrouiller son poste ou de se déconnecter du poste libre- service lors d'une absence prolongée de son bureau.

c. Les fichiers

Certains logiciels permettent un traitement automatique de données. C'est le cas, notamment, des logiciels de traitement de texte dans leur module publipostage. Certains agents peuvent ainsi être amenés à constituer des bases de données nominatives. Celles-ci sont généralement soumises aux dispositions de la loi informatique et libertés et nécessitent l'information des personnes concernées, la déclaration du traitement dans le registre des traitements de la commune préalablement à la collecte des données. Aussi, l'utilisateur prendra soin d'avertir préalablement le Délégué à la Protection des Données (Mail: dpo@ville-gardanne.fr) de toute constitution de base de données ou de fichiers nominatifs quelle qu'en soit sa taille.

L'ensemble des données que l'utilisateur souhaite garder confidentiel et dont il assume la pleine et entière responsabilité doit être rassemblé dans un dossier personnel unique et clairement identifié *(personnel ou privé)*, qui ne seront pas mis sur le réseau de la ville (G: ou X:), et ces derniers ne seront pas sauvegardés.

Tous les fichiers de l'utilisateur, hors son dossier « privé » ou « personnel », doivent donc être partagés dans le cadre de l'organisation de la collectivité afin d'assurer la continuité du service public et mis dans les dossiers prévus à cet effet.

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

2. Protection des données personnelles

a. Définition

La loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, renforcée par le Règlement Général sur la Protection des Données Personnelles (RGPD) du 27 avril 2016 définissent les conditions dans lesquelles des données à caractère personnel peuvent être traitées.

Au sens de ces textes :

- une donnée à caractère personnel est constituée par toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;
- un traitement représente toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

A titre d'exemple, constituent des traitements de données à caractère personnel :

- Le classement et le traitement de dossiers papier de demande de subventions,
- La mise en œuvre d'un système de billettique de transport ou de piscines,
- Les enquêtes sur les ménages,
- La gestion du personnel ou de la paye…

b. Secret professionnel

En tant qu'agent de la fonction publique, chaque personnel est tenu au secret professionnel et à la confidentialité au regard du grand nombre d'informations notamment sensibles et nominatives auxquelles il puisse avoir accès.

Il s'engage, dans le respect de la déclaration faite dans le registre des traitements (RGPD) à :

- Ne pas utiliser les données à caractère personnel à des fins autres que celles prévues par ses attributions ;
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- Ne faire aucune copie de ces données sauf si c'est nécessaire à l'exécution de la finalité du traitement ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- S'assurer dans la limite de ses attributions, que seuls des moyens de communications sécurisés seront utilisés pour transférer ces données.

c. En cas de manquement à ces règles il s'expose à des risques

S'il ne respecte pas les dispositions des présentes règles il pourrait voir ses droits d'accès restreints ou suspendus et, le cas échéant, être passible de sanctions administratives et/ou de poursuites civiles ou pénales.

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

d. Le droit à la déconnexion

En tant qu'agent de la collectivité, il dispose d'un « droit à la déconnexion », c'est-à-dire de la possibilité de ne pas se connecter aux outils numériques de la ville (outils collaboratifs, applications métier) et de ne pas être contacté par son employeur en-dehors de son temps de travail (téléphone, courriel).
Ce droit s'exerce en dehors des heures correspondant à sa formule de travail hebdomadaire, définie avec sa hiérarchie.
S'il estime que ce droit n'est pas respecté, il peut évoquer en premier lieu la situation avec sa hiérarchie.

e. Journalisation des accès utilisateur et sécurité du système d'information

La ville doit être en mesure de suivre tous les accès au système d'information à des fins de sécurité, de statistique et de maintenance.
Lorsqu'un poste de travail accède au système d'information de la commune, les données suivantes sont enregistrées :
- L'identifiant de l'utilisateur,
- La date et l'heure de connexion,
- L'adresse IP et le nom du poste de travail,
- Les applications auxquelles il a accédé,
- Le nombre de sessions ouvertes par l'utilisateur,
- La durée totale de l'activité de l'utilisateur.

f. Les droits sur les données à caractère personnel concernant l'agent

La ville, qui est l'employeur, collecte et traite des données à caractère personnel concernant les agents.
L'agent dispose, dans certaines conditions, de droits sur ces données à caractère personnel : accès, rectification, effacement, limitation, portabilité et opposition.
Pour tout renseignement sur les modalités d'exercice de ces droits, il peut saisir le délégué à la protection des données (DPO – Data Protect Officer) de la ville (dpo@ville-gardanne.fr).
S'il estime que ses droits ne sont pas respectés, il peut également introduire une réclamation auprès de la CNIL (www.cnil.fr).

g. Altération et/ou violations de données

En cas suspicion de vol, altération, suppression de données, il est nécessaire de prévenir dans les plus brefs délais :
- Le responsable de la sécurité des systèmes d'information rssi@ville-gardanne.fr
- le délégué à la protection des données dpo@ville-gardanne.fr

Voir procédures sur commun X:\20_RGPD\Violation de données

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

3. La messagerie électronique

La messagerie électronique est un outil permettant l'envoi et la réception de message est avant tout d'un outil professionnel réservé à un usage professionnel.
L'utilisateur doit ouvrir sa correspondance électronique et y répondre. Il doit porter une attention particulière à la rédaction de ses messages qui doivent être clairs et précis.

a. Les messages :

- doivent être le plus concis possible (taille maximum d'un message : 10 mégaoctets, pièce jointe comprise, révisable selon l'évolution des technologies).

- sont soumis aux règles qui régissent les droits et obligations des agents publics : notamment la discrétion, la réserve et la neutralité.

- ne doivent pas porter atteinte à l'image de l'institution municipale.

- ne doivent pas contenir des éléments de nature offensante, diffamatoire, injurieuse ou à connotation pornographique, sexiste ou raciste.

- n'engagent que leur auteur et ne peuvent être opposables à la Ville.

L'envoi en nombre de messages à des utilisateurs qui sont sans rapport avec leur mission et qui ne l'ont pas explicitement souhaité est interdit.

Si le message a un caractère privé, l'expéditeur y fait figurer la mention privé ou personnel et demande à son correspondant d'agir de même.

Toute transmission de documents informatiques requiert de la part de l'expéditeur un certain nombre de vérifications :
- La transmission ne doit pas contrevenir au respect de la confidentialité des informations.
- Le fichier doit être compatible avec les logiciels à disposition du destinataire.
- Le fichier doit être sain de tout virus.

Pour des raisons de sécurité (intrusion, virus, pertes de données, ...) il est fortement déconseillé de lire (et à plus forte raison d'exécuter les pièces jointes) les messages provenant d'expéditeurs inconnus ou suspects.
Au même titre, il est déconseillé d'exécuter les programmes transmis par messagerie (particulièrement ceux ayant le suffixe .EXE).

Il est interdit de relayer des messages de type canular (hoax), carte de vœux, chaîne, ...

Les données circulant sur l'internet « en clair » ne sont pas protégées contre les indiscrétions et les détournements éventuels. La vigilance s'impose donc quant au contenu diffusé.

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

b. Envoi de gros fichiers

Dans le cadre d'envoi vers l'extérieur de fichiers conséquents (plus de 10 mégaoctets) les utilisateurs doivent privilégier l'utilisation de plateformes d'échange de documents qui sont ou seront mises à leur disposition. La DSI recommande d'utiliser gratuitement :
https://send.transfertpro.com/?c=TSENDFREE

c. Adresse de messagerie

Les comptes et mots de passe de messagerie sont incessibles. Chaque utilisateur est responsable de l'utilisation qu'il en fait.

La diffusion des adresses électroniques d'autres utilisateurs est interdite sans leur autorisation.

L'usage de la cci (copie carbone invisible) est à favoriser lors d'envois multiples vers l'extérieur.

L'usurpation de l'adresse d'un autre utilisateur est strictement interdite et peut être punie par la loi française (usurpation d'identité).

d. En cas d'absence

Vous êtes invité à paramétrer une réponse automatique lors de vos absences pour congés. Vous trouverez une explication de la procédure dans le dossier commun X :

file:///X:/2_Informatique/Procedure_info_agent_absent.pdf

Accès à ma messagerie en cas d'absence ou de départ :

En cas de nécessité et pour des raisons de continuité de service, et via une demande expresse écrite du Directeur Général des Services, un accès à la messagerie électronique de l'agent absent peut être autorisé pour le chef de service ou le supérieur hiérarchique, sans toutefois accéder aux dossiers dits "personnels".

Pour plus d'informations, vous trouverez ci-après les recommandations de la CNIL :
https://www.cnil.fr/fr/lacces-la-messagerie-dun-salarie-en-son-absence

e. Piratage de compte de messagerie

L'utilisateur préviendra l'administrateur s'il ne peut plus se connecter ou s'il soupçonne que son compte est violé (cf. 1.4 Compromission et violation de données).

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

4. La navigation sur Internet

La navigation doit se faire exclusivement à partir du logiciel mis à disposition par le service informatique. Seul ce dernier sera à même d'afficher l'intégralité du contenu mis à disposition par la commune (intranet, portail applicatif).

Internet recueille une masse importante d'informations de qualité et de fiabilité très variable. L'utilisateur s'assurera que le site visité est suffisamment sérieux pour pouvoir exploiter les informations qu'il comprend. Bien entendu, l'utilisation et la transmission des informations trouvées sur Internet sont soumises aux lois sur la propriété intellectuelle et au droit d'auteur.
L'accès à des sites connus pour leur caractère strictement commercial doit être exceptionnel.

Sont interdits :
- les actes commerciaux d'achat en ligne.
- les transactions de type bancaire.
- les téléchargements, notamment de logiciels ou d'autres œuvres protégées (livre, musique, photo, vidéo).
- la connexion à des sites à caractère xénophobe, raciste, licencieux ou pornographique.
- l'accès à certains sites illégaux (pédophiles par exemple) peut même revêtir le caractère d'une infraction pénale.
- le dialogue en ligne (chat).
- la participation à des forums de discussion *(exception faite des webinaires et des visioconférences)*.
- l'accès à des sites offrant de la messagerie instantanée[11].

5. La téléphonie, smartphones, tablettes, Internet et transmission de données

En termes de services de téléphonie, sont interdits :
- Le téléchargement des logos et des sonneries sur les téléphones mobiles, que ce soit à usage professionnel ou privé.
- L'envoi de MMS ou de FAX par Internet ou par GSM.
- L'utilisation de la téléphonie à travers internet (type SIP, P2P VoIP...).
- Les appels téléphoniques ne concernant pas le cadre du travail.
- Appels vers et depuis l'étranger est proscrit, tout comme les appels vers les numéros surtaxés.

À noter que l'envoi de SMS par Internet ou par GSM doit demeurer exceptionnel et dans un cadre purement professionnel.

Ne sont pas autorisés (sauf autorisation écrite pour connexion au réseau de la Ville):
- L'utilisation de la navigation Internet, du WAP, de la messagerie (courriel) à partir de téléphones mobiles GSM.
- L'utilisation des GSM comme Point d'accès internet.
- L'utilisation de Modem.
- L'installation d'applications sans l'accord de l'informatique.
- L'appel à des numéros surtaxés.

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

6. Accès externe

Pour les prestataires :
Tout matériel autre que les matériels mis à disposition par la mairie accédant au réseau de la mairie via le réseau local ou via internet (messagerie ou accès réseau privé virtuel VPN), devra être à jour de son antivirus et des mises à jour de son système d'exploitation et de ses logiciels, afin de ne pas introduire de virus ou de logiciels malveillants (chevaux de Troie, vers etc..) sous peine de se voir bloquer l'accès.

Pour les agents :
Seuls les matériels fournis par la mairie pourront avoir accès via VPN au réseau et applications de la ville.

7. Sensibilisation - Action - Formation

Des actions de sensibilisations à la protection des données et à la sécurité informatique auront lieux lors des formations internes, ou par mail ou lors des interventions de la DSI ou du DPO.

8. L'administrateur

a. Missions

L'administrateur est responsable du bon fonctionnement du système d'information et de son intégrité, pour cela :
Il dimensionne les installations et les réseaux aussi bien que les volumes des fichiers transmis et les durées de connexions.
Il alloue à chaque utilisateur les ressources nécessaires à l'exercice de ses fonctions.
Il a accès à toutes les informations en transit (données ou voix) ou stockées dans le réseau.
Il est tenu à un strict respect du secret professionnel.
Il peut prendre la main à distance sur l'ordinateur afin d'aider l'agent à résoudre un problème ou d'installer un logiciel, faisant suite à une demande.
Il pourra bloquer l'accès d'un ordinateur et ou d'un matériel au réseau, si la sécurité des systèmes d'information est compromise cela afin de garantir la sécurité des systèmes d'information.
Il pourra supprimer des messages mails, fichiers, documents compromis sans accéder à la messagerie ou aux données de l'utilisateur ou des utilisateurs, via un script automatique, si ces mails, fichiers, documents peuvent porter atteintes à la sécurité des systèmes d'information, et ainsi éviter la propagation de virus ou phishing.
Il met en place les outils pour protéger le système d'information de toute intrusion, pollution ou acte hostile.
Il peut temporairement capturer et analyser en détail les communications téléphoniques, de vidéo ou de données afin de résoudre d'éventuels problèmes techniques, qui seront supprimés après utilisation.

b. Contrôle, surveillance et archivage

A la fois pour assurer un bon fonctionnement et une protection du réseau, l'administrateur doit veiller au bon usage des ressources par les utilisateurs. Il analyse, contrôle et archive les temps de connexions, les sites visités, ainsi que toute activité relative à l'usage des ressources informatiques dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.

Seul le Monsieur le Maire ou le Directeur Général des Services peut demander à l'administrateur des relevés (journaux de navigation) non nominatifs.

En cas de détection de comportements non conformes à la Charte, l'administrateur peut, après en avoir informé personnellement et par écrit l'utilisateur, réaliser une surveillance personnelle dont les résultats sont communiqués uniquement au Directeur Général des Services.
Cette surveillance ne s'exerce pas sur les dossiers informatiques portant le nom « privés » ou « personnels ».
Dans tous les cas l'administrateur se garde le droit d'effacer, ou d'isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des ressources informatiques.

Des contrôles réguliers des communications téléphoniques passées sont effectués. Le numéro appelant, le numéro appelé, la date, la durée et l'heure de la communication sont accessibles à l'administrateur.

c. Actions

L'administrateur se réserve le droit de suspendre à tout moment, et sans avertissement, l'accès au système d'information (sites Internet notamment), en cas de non-respect de la charte par l'utilisateur.

L'administrateur se réserve en outre le droit de bloquer à tout moment, sans avertissement préalable, l'accès aux sites dont le contenu est jugé illégal ou offensant.

Sans préjudice de la confidentialité des correspondances, l'administrateur est tenu de dénoncer au Procureur de la République les usages illégaux (tels que pédophilie, incitation à la haine raciale, terrorisme) qu'il constaterait dans l'usage des outils T.I.C.

L'administrateur peut interrompre l'accès, notamment pour des raisons de maintenance et de mise à niveau, sans que celui-ci puisse être tenu pour responsable des conséquences de ces interruptions aussi bien pour l'utilisateur que pour tout tiers.

Toutefois, l'administrateur s'engage dans la mesure du possible à faire connaître aux utilisateurs, par avance, via le courrier électronique et Intranet les plages d'interruptions de service lorsque celles-ci correspondent à des maintenances ou des interventions programmées.

9. Administrateur fonctionnel

L'administrateur(trice) fonctionnel logiciel a en charge la gestion fonctionnelle du logiciel, en tant que référent(e) technique, a pour mission d'accompagner les utilisateurs du service à la fois sur de l'assistance de 1er niveau, mais également sur le pilotage de projets faisant intervenir le département numérique et les éditeurs de logiciels.

En plus des missions habituelles décrites ci-dessous, l'administrateur(trice) fonctionnel logiciel (H/F) a un rôle de coordonnateur et de facilitateur, il/elle travaillera en lien étroit avec l'ensemble des services et sera chargé/e de faire évoluer les pratiques et sera force de proposition terme d'outils.
L'administrateur(trice) fonctionnel logiciel se charge de créer les comptes utilisateurs, leur affecter les droits et des déclarations d'incident vers les éditeurs de logiciels et vers la DSI via les plateformes dédiées : GLPI ou mail (sav-informatique@ville-gardanne.fr)

En tant que correspondant Informatique : il doit gérer les droits d'accès aux différents outils, définir un plan informatique annuel ou pluriannuel sur la base d'un état des lieux des outils informatiques et numériques et d'une analyse des besoins en partenariat avec la DSI, assurer le dépannage sur la partie logicielle et matérielle en lien avec la DSI.

Envoyé en préfecture le 12/01/2026
Reçu en préfecture le 12/01/2026
Publié le 12/01/2026
ID : 013-211300413-20260108-DEL_2026_20-DE

10. Mise en application

Cette charte remplace et annule toutes dispositions contraires contenues dans les notes de service et autres réglementations existantes en vigueur relatives au fonctionnement et l'utilisation du système d'information, qu'elles soient écrites ou orales.
La charte est présentée à la première connexion de l'utilisateur à un équipement informatique appartenant à la ville, celui-ci doit la valider afin de pouvoir accéder aux ressources, sinon il sera déconnecté.

Elle est présentée et remise par le supérieur hiérarchique à l'agent fonctionnaire au moment de sa prise de fonction, de même qu'aux agents contractuels ou vacataires.

Elle sera communiquée aux fournisseurs titulaires de marchés dont les salariés ou sous-traitants sont amenés, dans le cadre de leur prestation, à avoir accès aux systèmes d'information de la Ville de Gardanne. A charge pour eux de la communiquer aux personnes intervenant de leur fait.

La charte et toutes les explications techniques nécessaires à sa bonne compréhension, ainsi que des liens vers les sites juridiques officiels, constitueront des rubriques permanentes présentes sur l'Intranet.

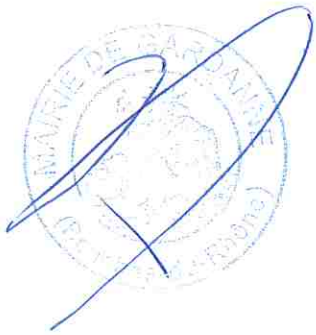
Le non-respect des règles établies ou rappelées par la charte pourra donner lieu à des sanctions de nature disciplinaires mais aussi selon le cas, la gravité et la nature, à des sanctions prises au titre du code pénal, les unes n'étant pas exclusives des autres.

Cette charte peut connaître des modifications dues aux évolutions législatives ainsi qu'à celle des ressources informatiques. Dans tous les cas, une note de service sera rédigée indiquant les modifications.

La présente charte a été soumise et validée par le Comité Social Territorial le 13 novembre 2025.

La présente charte a été approuvée par délibération n°2026-20 du Conseil municipal en date du 08 janvier 2026.

Fait à Gardanne, le 08 janvier 2026



11. Annexe

Cadre Légal (Rappel non exhaustif)

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

La loi n°78-17 du 6 janvier 1978 « informatique, fichiers et libertés » modifiée ;
Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;
La loi n°85-660 du 3 juillet 1985 relative aux droits d'auteur et à la protection des Logiciels (Titre V) ;
La loi n°88-19 du 5 Janvier 1988 relative aux systèmes de traitement automatisé de données ;
La loi n°91-246 du 10 juillet 1991 relative au secret des correspondances (art 226-15) ;
La loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs ;
La loi n°2004-575 du 21 Juin 2004 relative à l'économie numérique ;
La loi n°2006-358 du 24 Mars 2006 relative à la conservation des données des communications électroniques ;
La loi n°2006-961 du 1 août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information ;
La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.