CHARTE INFORMATIQUE DE SÈTE AGGLOPÔLE MEDITERRANÉE

Sète agglopôle méditerranée
ARCHIPEL DE THAU

Table des matières

VERSION

Ce tableau gère les modifications apportées au document au-delà de sa version initiale. Les petites modifications de type erreurs de frappe ou changements de syntaxe ne font pas l'objet d'un suivi.

VERSION	DATE	AUTEUR(S)	OBJET DE LA RÉVISION
V 1.0	20/10/2025	Service informatique	Version initiale
V 1.1	17/02/2026	Service informatique	Regroupement des informations relatives à l'opposabilité au sein du paragraphe « Diffusion – Opposabilité – Mise à jour » et suppression de la section « OPPOSABILITÉ DE LA CHARTE » Ajout d'une section « Annexes IA et SIG» précisant que les annexes jointes à la charte en constituent une partie intégrante et qu'elles ont la même valeur normative que la charte principale.
V 1.2			

PRÉAMBULE

La **charte informatique** de la collectivité définit les **règles** encadrant l'usage des **outils numériques** mis à disposition des usagers.

Ces **technologies** permettent une **ouverture maîtrisée** vers l'extérieur et peuvent renforcer les **performances**, sous réserve d'un usage **responsable** et **sécurisé**.

L'objectif est de **protéger le système d'information**, assurer le **bon fonctionnement** de la collectivité et **respecter les droits et devoirs** de chacun.

Une mauvaise utilisation peut entraîner des **conséquences graves** (atteinte à la **confidentialité**, vols de données, etc.).

Chaque utilisateur est **responsable** et doit s'engager à **respecter cette charte**.

CHAMP D'APPLICATION DE LA CHARTE

La présente **charte** concerne l'ensemble des **utilisateurs** de la collectivité, qu'il s'agisse du **personnel**, quel que soit leur statut, des **élus** ou de toute autre personne **ayant accès au système d'information**.

Elle s'applique également à tout **prestataire extérieur** amené à utiliser les **outils informatiques** ou à accéder aux **données** de la collectivité. Tout contrat conclu avec un prestataire devra explicitement faire référence à cette charte et **l'inclure en annexe**.

Intégrée au **règlement intérieur** du personnel, cette charte s'impose à chaque **agent** travaillant au sein de la collectivité.

Des annexes thématiques (SIG et IA), viennent la compléter afin de traiter plus précisément certains domaines tout en assurant une cohérence d'ensemble.

DIFFUSION – OPPOSABILITÉ – MISE À JOUR

La **charte** est disponible sur l'**intranet** de la collectivité pour l'ensemble des **utilisateurs**. Chaque utilisateur doit remettre à la Direction des Systèmes d'Information (DSI) un **accusé de réception signé**, attestant de la bonne compréhension de ses **droits et devoirs**.

La présente **charte** est rendue **opposable** dès son **annexion au règlement intérieur** de la collectivité. Elle est par ailleurs **notifiée à l'ensemble des élus** du **conseil communautaire**.

Elle s'impose à toute personne utilisant un équipement informatique mis à disposition par la collectivité, ainsi qu'à celles disposant d'un accès, **permanent** ou **occasionnel**, au **système d'information** de l'organisation.

Enfin, la charte est accessible et tenue à jour sur **l'intranet** ; **la version en vigueur publiée en ligne fait foi**.

ANNEXES IA et SIG

Les annexes jointes à la présente charte en constituent une partie intégrante.
Elles ont la même valeur normative et s'imposent dans les mêmes conditions que la charte principale.

POSTES INFORMATIQUES

Toute personne, qu'il s'agisse d'un **agent**, d'un **élu** ou d'un **collaborateur** intervenant au sein ou pour le compte de la collectivité, peut bénéficier d'un **droit d'accès au système d'information**.

Ce droit d'accès est :

✓ **Strictement personnel**
✓ **Non transférable**

Chaque utilisateur reçoit un **équipement informatique** qu'il doit utiliser avec **soin**, dans le respect des **consignes d'usage**.

Règles d'usage impératives

Les **règles suivantes** s'appliquent à l'ensemble des utilisateurs du **système d'information** :

- En cas d'**absence** même de courte durée, l'utilisateur doit **verrouiller sa session** afin de sécuriser son poste de travail.
- À la fin de la journée, l'utilisateur doit **fermer ses applications** et **éteindre son ordinateur** (sauf cas spécifique validé par la DSI). Cette procédure permet notamment l'**installation automatique des mises à jour** nécessaires.
- L'utilisateur doit régulièrement **supprimer les fichiers devenus inutiles** et **archiver les documents**, afin d'optimiser **l'espace de stockage** et de maintenir **les performances** des systèmes informatiques.
- L'utilisateur doit **prendre soin de son matériel**, le transporter dans la pochette prévue à cet effet et le stocker en lieu sûr. L'agent doit le faire **ramener au bureau en cas d'absence prolongée** afin de pouvoir gérer les mises à jour nécessaires à la sécurité. Il n'est pas autorisé à conserver son matériel (PC portable, tablette ou téléphone professionnel) à la maison en cas d'absence prolongée.
- L'usage des **supports amovibles** est strictement limité aux **besoins professionnels justifiés**. L'usage de supports **personnels ou non sécurisés est interdit**. La DSI peut en restreindre l'accès.
- Les équipements sont fournis avec une **configuration standardisée** gérée par la DSI, incluant **le système**, les **mises à jour de sécurité**, un **antivirus/EDR** actif, un **pare-feu** et des **règles de filtrage**. Il est interdit de modifier ces réglages et de désactiver les protections.

De manière générale, tout **dysfonctionnement** ou **anomalie** constaté doit être **signalé sans délai à la DSI**.

ACCÈS WIFI

Les **réseaux internes sécurisés** doivent être **privilégiés** ; l'utilisation de **points d'accès Wi-Fi** publics est déconseillée. En cas de besoin, le **partage de connexion mobile** reste **la solution recommandée**.

Il est **interdit de créer un pont** entre ces connexions mobiles et le réseau interne, par exemple en connectant un appareil à la fois au **réseau filaire** et au **Wi-Fi**.

De même, l'accès au réseau par **câble** (RJ45) est strictement réservé aux **postes référencés**. Tout **branchement filaire non autorisé** est **interdit**.

GESTION DES IDENTIFIANTS ET MOTS DE PASSE

Chaque utilisateur du **réseau informatique** dispose d'un **compte personnel**, protégé par un **identifiant (login)** et un **mot de passe**. Il est seul responsable de l'usage de ce compte et, à ce titre, doit veiller à la **confidentialité** de son mot de passe. Ce dernier ne doit en aucun cas être **communiqué à un tiers**,

ni être noté sur un support quel qu'il soit. Par nature, le mot de passe est **strictement personnel, incessible et intransmissible**.

Cas particulier : dans certaines situations spécifiques, un même poste peut être utilisé par un groupe d'utilisateurs pour des usages ciblés. Ces exceptions doivent être **encadrées**.

Les mots de passe permettant l'accès à des **données sensibles ou stratégiques** (y compris ceux permettant l'accès à une session) doivent être **renouvelés au minimum tous les six mois**, conformément aux recommandations de l'ANSSI en matière de sécurité informatique

Pour garantir leur efficacité, les mots de passe doivent respecter les **critères suivants** :

- Longueur ≥ 12 caractères ;
- Au moins 1 majuscule ;
- Au moins 1 chiffre ;
- Au moins 1 caractère spécial ;
- Bannir toute référence personnelle (nom, date, service).

Le **stockage des mots de passe** doit être sécurisé : l'utilisation d'un **gestionnaire de mots de passe validé par la DSI** est obligatoire pour conserver et organiser ses mots de passe. Ce gestionnaire assure leur chiffrement, permet de générer des mots de passe robustes, et limite les risques liés à l'oubli ou à la réutilisation.

MESSAGERIE ÉLECTRONIQUE

La **messagerie électronique** constitue l'un des principaux vecteurs de propagation de **virus informatiques** et de tentatives de « **Phishing** » (hameçonnage), une méthode utilisée par des fraudeurs pour récupérer des **données personnelles**. Il est en effet très facile de diffuser, par email, un fichier infecté en pièce jointe ou un **lien menant vers un programme malveillant**.

Comme pour tout autre moyen de communication (courrier postal, téléphone, etc.), **chaque utilisateur est personnellement responsable** des messages qu'il envoie ou reçoit.

Utilisation privée de la messagerie :

L'usage de la messagerie **@agglopole.fr** est prioritairement réservé à l'exercice des **missions de service public**. Un usage personnel, à condition qu'il soit **ponctuel** et **raisonnable**, peut être toléré s'il ne perturbe pas le service, ne contrevient pas à la charte d'utilisation et ne compromet pas la sécurité des systèmes. Les messages à caractère privé doivent cependant être clairement identifiés par la mention « personnel ».

Les **redirections automatiques** vers des **adresses externes personnelles** sont interdites.

La **signature** utilisée dans les courriels doit respecter le **modèle normalisé de la collectivité**, incluant le nom, la fonction, le service, les coordonnées et le logo officiel. L'ajout de **slogans**, d'**images non approuvées** ou de mentions engageant la collectivité est interdit sans validation préalable des services **RH**, **Communication** ou **DSI**.

Règles d'usage :

L'utilisateur doit faire preuve de **vigilance** dans l'utilisation de la **messagerie électronique** et respecter les règles suivantes :

- Il ne doit pas **ouvrir de courriels** dont le **sujet paraît suspect**, notamment ceux comportant des pièces **jointes** ou des **liens douteux**.

- En cas d'**absence prévisible** (congés, formation, déplacement, mission extérieure), l'utilisateur doit activer un message d'**absence clair et factuel**. Ce message mentionnera uniquement :
    - La **période d'absence** ;
    - un **contact de relais générique** (ex. : accueil@agglopole.fr, urbanisme@agglopole.fr) , ou le **numéro du standard**.
- Pour l'**envoi ou la réception de fichiers volumineux**, l'agent est invité à **privilégier l'utilisation** de l'outil "**GrosFichiers**", mis à disposition sur l'intranet par la **DSI**.

UTILISATION D'INTERNET

L'accès à **Internet** est strictement réservé à des **usages professionnels**. Toutefois, un usage personnel modéré peut être toléré en **dehors des heures de travail**, à condition qu'il n'entrave pas le **bon fonctionnement** des activités professionnelles, notamment en termes de bande passante ou de sécurité.

Chaque utilisateur doit être conscient que certaines pratiques présentent des **risques importants** pour la collectivité. Il est notamment **interdit de** :

- **Communiquer à des tiers** des informations techniques sur le matériel ou les systèmes utilisés
- **Diffuser des informations** relatives à la collectivité sur des sites Internet, forums ou réseaux sociaux sans **autorisation préalable**.

L'utilisateur s'engage également à respecter les règles suivantes lors de l'utilisation d'Internet :

- Ne pas consulter de sites **contraires aux lois en vigueur** ou portant atteinte à la **dignité humaine**, notamment ceux faisant l'apologie de la pédopornographie, des crimes contre l'humanité, ou incitant à la discrimination, à la haine ou à la violence envers une personne ou un groupe en raison de son origine, de sa nationalité, de sa race, de sa religion ou de toute autre appartenance.
- Ne pas **télécharger ou partager** des contenus protégés par des **droits d'auteur** ou la législation sur le copyright (tels que logiciels propriétaires, fichiers musicaux ou audiovisuels, etc.).
- Ne pas télécharger de fichiers (logiciels, vidéos, images, etc.) n'ayant **aucun lien avec les fonctions ou missions professionnelles**.

Pour garantir la **sécurité** et prévenir les abus, la collectivité peut, à tout moment et conformément à la réglementation en vigueur, **contrôler les connexions** entrantes et sortantes réalisées depuis ses équipements.

TÉLÉPHONIE ET TABLETTE

L'usage des **téléphones fixes et mobiles** mis à disposition est réservé aux **besoins professionnels**. Toutefois, un usage **ponctuel à des fins personnelles**, limité aux **communications locales**, peut être toléré, à condition de ne pas nuire au bon déroulement des **activités professionnelles**.

La collectivité se réserve le droit de **contrôler les appels et messages** émis ou reçus, dans le respect de la **législation en vigueur**.

Les **smartphones** et **tablettes** sont des **outils professionnels**. Leur usage à des fins personnelles peut être **exceptionnellement autorisé**, à condition que les messages à caractère privé soient clairement identifiés par la mention « **personnel** ».

Il est rappelé que les **agents ne sont pas tenus de répondre** aux appels ou aux messages **en dehors de leur temps de travail** (soirs, week-ends, congés), sauf en cas d'**astreinte**.

MOBILITÉ ET TÉLÉTRAVAIL

L'accès au **système d'information depuis l'extérieur** se fait uniquement via **les solutions approuvées par la DSI** : **VPN** et **authentification forte**, depuis un **poste conforme**. Lors de l'utilisation en mobilité, il convient de **protéger les écrans des regards indiscrets** et d'**éviter les conversations confidentielles** dans les lieux publics.

DEPART D'UN UTILISATEUR

Lorsqu'un **utilisateur met fin à son activité** au sein de la collectivité, son **accès aux systèmes d'information internes** est automatiquement **révoqué**.

À ce titre, il lui incombe de :

- **Restituer** l'ensemble du **matériel** (informatique, téléphonique, etc.) mis à sa disposition,
- **Supprimer** de son poste de travail tous les **fichiers ou données à caractère personnel** qu'il aurait pu y stocker.

Toute **copie de documents ou de données professionnels** n'est autorisée qu'après **validation écrite** de son **supérieur hiérarchique dûment habilité**.

Par ailleurs, les **répertoires personnels** ainsi que les **données de messagerie** conservés sur les serveurs seront automatiquement **supprimés par la DSI**, et ce **au plus tard un mois après le départ** de l'agent.

SURVEILLANCE, CONTRÔLE ET RESPECT DE LA VIE PRIVÉE

Le système d'information utilise des **fichiers journaux** ("logs") pour **surveiller** les activités, garantir la **sécurité** et détecter d'éventuelles **erreurs**. Ces fichiers consignent les **accès**, les **modifications de fichiers**, ainsi que les **connexions** au réseau, à la messagerie et à Internet. Les utilisateurs sont informés que leurs **actions peuvent être surveillées**. Seule la **DSI** a accès à ces informations, qui sont conservées pendant une période maximale d'un an. En cas de problème, de suspicion de **virus** ou de **comportement suspect**, un **contrôle manuel** peut être effectué, y compris sur les dossiers identifiés comme **personnels**, tout en garantissant le **respect de la vie privée** des utilisateurs. De plus, les agents du **service informatique**, en vertu de leur rôle, signent une **charte** et sont soumis à une **obligation de confidentialité renforcée**, assurant ainsi un traitement conforme aux exigences **légales** et **éthiques**.

PSSI

Les **utilisateurs du système d'information** de la collectivité sont tenus de respecter les **principes** et **mesures** définis dans la **Politique de Sécurité des Systèmes d'Information** (PSSI), document cadre précisant les **règles de protection des ressources numériques**.

La **PSSI** est disponible sur l'**intranet** et doit être **consultée régulièrement** afin de garantir une **utilisation conforme et sécurisée** des outils informatiques.

MANQUEMENT À LA CHARTE ET À LA PSSI

Le **non-respect** des dispositions de la présente **charte**, ainsi que celles définies dans la **Politique de Sécurité des Systèmes d'Information** (PSSI), peut entraîner la **suspension** voire **la suppression de l'accès** aux **outils informatiques et de communication** mis à disposition.

Selon la **gravité des manquements constatés**, des **sanctions disciplinaires** pourront être appliquées, conformément à la **réglementation en vigueur** dans la **fonction publique territoriale**. Le cas échéant, des **poursuites pénales** pourront également être engagées.

OPPOSABILITÉ DE LA CHARTE

La présente **charte** est rendue **opposable** dès son **annexion au règlement intérieur** de la collectivité. Elle est par ailleurs **notifiée à l'ensemble des élus** du **conseil communautaire**.

GLOSSAIRE

- **Antivirus/EDR** : logiciel conçu pour détecter, neutraliser et supprimer les logiciels malveillants.
- **Mise à jour** : opération consistant à installer une nouvelle version d'un logiciel.
- **Pare-feu** (firewall) : logiciel et/ou matériel protégeant un réseau en filtrant les accès entrants et sortants selon des règles définies.
- **Phishing** (hameçonnage) : technique frauduleuse qui consiste à imiter l'apparence d'une institution (banque, administration) pour obtenir des informations personnelles.
- **Système d'information** : ensemble organisé de ressources permettant de collecter, stocker, traiter et diffuser des informations, généralement via un réseau informatique.
- **Télétravail** : organisation du travail où un salarié effectue, hors des locaux de l'employeur, des tâches réalisables sur site, en utilisant les technologies de l'information (article L. 1222-9 du code du travail). Le télétravail est une forme de nomadisme numérique.
- **DSI :** Direction des Systèmes d'Information

BASES LEGALES

L'utilisateur est tenu de respecter les obligations de réserve, de discrétion et de secret professionnel, conformément aux droits et devoirs des agents publics tels que définis par la loi du 13 juillet 1983 relative aux droits et obligations des fonctionnaires, ainsi que par la loi n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale.

Par ailleurs, il doit se conformer aux dispositions suivantes :

Loi n° 78-17 du 6 janvier 1978 sur l'informatique, les fichiers et les libertés, visant à protéger les libertés individuelles face aux risques liés à l'utilisation des technologies informatiques.

Loi n° 78-753 du 17 juillet 1978 et l'ordonnance n° 2015-1341 du 23 octobre 2015, relatives aux règles régissant les relations entre le public et l'administration.

Loi n° 2000-230 du 13 mars 2000, adaptant le droit de la preuve aux technologies de l'information et encadrant la signature électronique.

Loi n° 2004-575 du 21 juin 2004, dite loi pour la confiance dans l'économie numérique, visant notamment à encourager le développement des nouvelles technologies au sein des collectivités.

DROIT DISCIPLINAIRE

- Loi n° 83-634 du 13 juillet 1983, modifiée, relative aux droits et obligations des fonctionnaires.
- Loi n° 84-53 du 26 janvier 1984, modifiée, portant dispositions statutaires relatives à la fonction publique territoriale.
- Décret n° 89-677 du 18 septembre 1989, modifié, concernant la procédure disciplinaire applicable aux fonctionnaires territoriaux.

- Décret n° 92-1194 du 4 novembre 1992, modifié, fixant les règles communes applicables aux fonctionnaires stagiaires de la fonction publique territoriale.
- Décret n° 88-145 du 15 février 1988, modifié, pris pour l'application de l'article 138 de la loi du 28 janvier 1984, relatif aux agents non titulaires de la fonction publique territoriale.
- Décret n° 91-298 du 20 mars 1991, modifié, portant dispositions statutaires applicables aux fonctionnaires territoriaux nommés dans des emplois permanents à temps non complet.