Centre de gestion
de la fonction publique
territoriale de la Charente

v. 10/09/2025

CHARTE INFORMATIQUE / TÉLÉPHONIE

TABLE DES MATIERES

PRÉAMBULE

La présente charte définit les règles d'utilisation des systèmes d'information, des outils informatiques et de communication mis à disposition par le Centre de Gestion de la Fonction Publique Territoriale de la Charente.
Elle s'impose à toute personne accédant aux ressources informatiques de l'établissement, qu'il s'agisse d'agents, d'élus ou de prestataires extérieurs.
Son objectif est d'assurer la sécurité, la confidentialité et la bonne utilisation des moyens numériques, dans le respect des obligations légales et réglementaires en vigueur.

Chaque utilisateur est responsable du respect des règles énoncées dans cette charte et peut voir sa responsabilité engagée en cas de manquement.

En cas d'infraction :

- Un rappel à l'ordre peut être effectué par l'autorité hiérarchique,
- Une procédure disciplinaire peut être engagée en cas de manquement grave ou répétés, par l'autorité territoriale,
- Des sanctions pénales sont également applicables en cas de violation de la réglementation légale.

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

1. INTRODUCTION

Le Centre de Gestion de la Fonction Publique Territoriale de la Charente (ci-après dénommé "l'établissement" ou « CDG ») met en œuvre un système d'information et de communication indispensable à l'exercice de ses missions et à l'accompagnement des collectivités locales.
Dans ce cadre, des outils informatiques et de communication sont mis à disposition des agents, des élus et, sous conditions, de prestataires ou d'intervenants extérieurs.
La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources de communication de l'établissement.
Elle a également pour objet de sensibiliser les utilisateurs aux risques inhérents à l'usage des systèmes d'information, notamment en matière :

- d'intégrité,
- de confidentialité,
- de disponibilité des informations traitées.

Le non-respect des règles de sécurité, l'imprudence, la négligence ou un comportement malveillant peuvent entraîner des conséquences graves, engageant à la fois :

- la responsabilité civile et/ou pénale de l'utilisateur,
- celle de l'établissement.

1.1. Protection des données à caractère personnel

Conformément au Règlement Général sur la Protection des Données (RGPD) 2016/679 et à la loi Informatique et Libertés (n°78-17 du 6 janvier 1978 modifiée), « *l'établissement est responsable de la protection des données personnelles qu'elle traite ».*

Un Délégué à la Protection des Données (DPO) a été désigné pour :

- Veiller au respect des obligations légales en matière de protection des données,
- Conseiller et accompagner les responsables de traitement,
- Assurer l'information et l'exercice des droits des personnes (droit d'accès, de rectification, d'effacement, d'opposition, ...).

Le DPO doit être consulté préalablement à la mise en œuvre de tout nouveau traitement de données.
Il peut être contacté par courriel à l'adresse suivante : dpo@cdg16.fr
Le DPO tient à jour un registre des traitements que l'établissement réalise.
Ce registre est accessible à toute personne en faisant la demande.
En matière de communication externe, tout document, donnée ou information issue du système d'information ne peut être diffusé qu'après autorisation préalable de la direction ou selon des règles fixées par les services.

Attention :
Tout message électronique envoyé depuis une adresse professionnelle portant l'identité de l'établissement engage l'image de celle-ci. Il appartient donc à chaque utilisateur de veiller au respect du formalisme, de la confidentialité et des procédures de validation définies par l'autorité territoriale.

1.2. Respect des droits de propriété intellectuelle

Le principe de propriété intellectuelle s'applique à toutes les données et contenus manipulés dans le système d'information : textes, documents, images, sons, vidéos, logiciels,…

Chaque utilisateur s'engage à respecter :

- Les droits de propriété intellectuelle de l'établissement
- Les droits des partenaires et tiers titulaires de droits sur les ressources utilisées.

Toute reproduction, diffusion, altération ou usage non autorisé expose l'agent à des sanctions disciplinaires et/ou pénales.

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

1.3. Champ d'application de la charte

La présente charte s'applique à toute personne ayant accès au système d'information de l'établissement et notamment :

- agents (quel que soit leur statut, droit public ou privé),
- élus,
- invités (prestataires, stagiaires, intervenants extérieurs dûment autorisés).

Les obligations définies par la charte s'appliquent de manière identique à tous les utilisateurs.

La charte est applicable dans le cadre des activités professionnelles et, de manière exceptionnelle et encadrée pour un usage personnel, à condition que celui-ci :

- ne perturbe pas le bon fonctionnement des services,
- ne compromette pas la sécurité des systèmes,
- ne porte pas atteinte à l'image ou aux intérêts de l'établissement.

La charte est diffusée à l'ensemble des utilisateurs par mise à disposition dans l'intranet.

Des actions de communication internes sont organisées autant que nécessaire afin d'informer les utilisateurs des pratiques recommandées.

Quelques définitions :

- « U*tilisateur* » : toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de l'établissement et à les utiliser : agents, stagiaires, personnels de sociétés prestataires...
- "O*utils informatiques et de communication*" : recouvrent tous les équipements informatiques, les outils de télécommunications et les outils de reprographie de l'établissement.
- « *Le service informatique* » : est assuré par un agent dédié du Centre de Gestion, en charge de l'ensemble de l'infrastructure informatique et téléphonique, ainsi que de l'intervention sur les postes de travail. Il assure également la coordination avec des prestataires extérieurs lorsque des besoins spécifiques le nécessitent.

2. LES RÈGLES D'UTILISATION DU SYSTÈME D'INFORMATION DE L'ÉTABLISSEMENT

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par l'établissement.

2.1. Les modalités d'intervention du service informatique

L'administrateur du système informatique, est responsable de son bon fonctionnement et du contrôle de son utilisation. Il veille à l'application des règles de la présente charte afin de garantir la sécurité et à la continuité des systèmes d'information, réseaux et moyens de communication du Centre de Gestion. Dans ce cadre, il dispose des outils techniques nécessaires à l'administration, à l'investigation et au contrôle de l'usage des ressources informatiques.
Le responsable du service informatique a accès à l'ensemble des données techniques, dans le strict respect des règles de confidentialité applicables au contenu des documents traités, y compris les données à caractère personnel.
Il est soumis à une obligation de secret professionnel et de réserve, et s'engage à garantir la confidentialité, l'intégrité et la sécurité des données, conformément aux exigences du Règlement Général sur la Protection des Données (RGPD).
Les opérations de contrôle ou d'analyse des usages informatiques ne sont réalisées que dans le cadre de besoins légitimes, tels que la maintenance, la sécurité, la prévention ou la résolution d'incidents. Elles excluent toute surveillance systématique ou permanente des utilisateurs.

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

2.2. L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un identifiant individuel attribué à chaque utilisateur lors de son arrivée au Centre de Gestion, associé à un mot de passe strictement personnel.
Les moyens d'authentification sont personnels, confidentiels et intransmissibles. Il est strictement interdit de les partager ou de les divulguer, sous quelque forme que ce soit.
Le mot de passe doit comporter au minimum 13 caractères, incluant obligatoirement des lettres majuscules, des lettres minuscules, des chiffres et des caractères spéciaux.
L'utilisation d'informations personnelles (nom, prénom, date de naissance, nom de l'établissement, ...), de suites logiques ou de répétitions est proscrite.
La réutilisation d'anciens mots de passe est déconseillée. Il n'est plus demandé de renouveler le mot de passe à intervalles réguliers. Toutefois, un changement immédiat est requis en cas de suspicion de compromission.
Le Centre de Gestion se réserve le droit d'adapter ces règles en fonction de l'évolution des exigences de sécurité ou des recommandations officielles (ex. : ANSSI, CNIL).

2.3. Les règles de sécurité

Tout utilisateur s'engage à respecter les règles élémentaires de sécurité informatique suivantes :

- Signaler immédiatement au service informatique toute anomalie, dysfonctionnement, suspicion de compromission ou tentative d'intrusion relative à son compte ou à un équipement.
- Ne jamais communiquer son identifiant ou son mot de passe à un tiers, et ne jamais demander ceux d'un autre utilisateur.
- Ne jamais dissimuler sa véritable identité numérique ou usurper celle d'autrui.
- Ne pas modifier les paramètres techniques du poste de travail sans autorisation du service informatique.
- Ne pas installer de logiciels ou extensions sans validation préalable du service informatique.
- Ne pas copier, modifier ou supprimer les logiciels appartenant à l'établissement sans autorisation expresse.
- Verrouiller sa session ou son poste de travail dès qu'il s'absente, même brièvement.
- Ne pas accéder, tenter d'accéder, modifier ou supprimer des données qui ne relèvent pas de ses fonctions, sauf autorisation.
- Toute copie de données sur un support externe (clé USB, disque dur, etc.) doit être préalablement validée par le service informatique et respecter les règles internes en vigueur.
- Il est interdit de connecter un périphérique amovible privé. En cas de doute, l'utilisateur doit consulter le service informatique.

Par ailleurs :

- Les visiteurs ne sont autorisés à accéder au système d'information qu'avec l'accord explicite du service informatique.
- Les prestataires et intervenants extérieurs doivent s'engager à respecter les règles de sécurité de l'établissement. Il leur appartient également de les faire appliquer à leurs collaborateurs et éventuels sous-traitants.
- Les contrats conclus avec des tiers ayant accès aux données, aux logiciels ou aux équipements informatiques de l'établissement doivent comporter une clause rappelant ces obligations.

Toutes les actions réalisées sur les systèmes d'information font l'objet d'une traçabilité. Chaque utilisateur est personnellement responsable de l'usage de son compte et des données auxquelles il accède.

Tout manquement aux présentes règles peut entraîner des sanctions disciplinaires (conformément au Code général de la fonction publique), voire des poursuites pénales en cas d'infractions (usurpation d'identité, atteinte aux systèmes de traitement automatisé de données, etc.), ainsi que des sanctions administratives prévues par le Règlement Général sur la Protection des Données (RGPD).

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

3. LES MOYENS INFORMATIQUES

3.1. Configuration du poste de travail

L'établissement met à disposition de chaque utilisateur un poste de travail équipé des outils informatiques et logiciels nécessaires à l'exercice de ses fonctions.
Ces équipements, configurés et maintenus par le service informatique interne, doivent être utilisés conformément aux règles établies.
À ce titre, il est interdit à l'utilisateur, sauf autorisation préalable du service informatique :

- De modifier la configuration matérielle ou logicielle des équipements, ainsi que leurs paramètres de fonctionnement.
- De connecter ou déconnecter du réseau tout équipement informatique ou de communication sans validation.
- De déplacer un équipement (hors matériel nomade expressément prévu à cet effet) sans accord formel.
- D'installer des logiciels ou extensions non fournis par le service informatique.
- De porter atteinte, volontairement ou non, au bon fonctionnement des dispositifs informatiques ou de communication mis à disposition.

Toute demande de modification, d'ajout de logiciel ou de déplacement de matériel doit faire l'objet d'une validation préalable par le service informatique.

3.2. Équipements nomades

Sont considérés comme équipements nomades tous les moyens techniques mobiles tels que les ordinateurs portables, imprimantes portables, téléphones mobiles ou smartphones, supports amovibles (clé USB, disques externes), CD/DVD, ...
Ces équipements peuvent contenir des données sensibles ou confidentielles. À ce titre, ils doivent être sécurisés de manière appropriée, notamment par des dispositifs de chiffrement lorsque cela est techniquement possible.
Avant de stocker des données sensibles ou à caractère personnel sur un support mobile (par exemple une clé USB), l'utilisateur doit en informer le service informatique afin que les mesures de sécurisation nécessaires — telles que le chiffrement — soient mises en place.
En cas de perte, vol ou compromission d'un équipement nomade ou d'un support de données externe, l'utilisateur doit en informer immédiatement le service informatique. Celui-ci réalisera, en lien avec l'utilisateur, un inventaire des données potentiellement concernées et décidera des mesures à prendre, notamment en matière de notification à la CNIL si nécessaire (conformément au RGPD).
L'usage des smartphones personnels ou professionnels pour consulter la messagerie électronique de l'établissement expose à des risques particuliers de perte de confidentialité, notamment en cas de perte ou de vol. Ces appareils doivent donc être protégés par un verrouillage automatique (code, biométrie ou mot de passe) dès qu'ils ne sont pas utilisés pendant quelques minutes, afin de prévenir tout accès non autorisé.

3.3. Internet

L'utilisation d'Internet depuis les équipements de l'établissement est autorisée dans le cadre de l'activité professionnelle. Les utilisateurs peuvent consulter les sites web présentant un lien direct et nécessaire avec leurs missions, quels que soient leur nature ou leur domaine.
Une utilisation ponctuelle, raisonnable et modérée à des fins personnelles est tolérée en dehors des heures de travail, sous réserve que :

- les contenus consultés ne soient ni contraires à la loi, ni à l'ordre public,
- ils ne portent pas atteinte à la réputation ou aux intérêts de l'établissement.

Un système de filtrage automatique des sites web est mis en œuvre pour prévenir les risques de sécurité, de contenus illicites ou inappropriés.
Si un site requis dans le cadre d'une activité professionnelle est bloqué, l'agent peut en faire la demande auprès du service informatique via une demande d'intervention, en précisant :

- l'adresse exacte du site concerné,
- la justification professionnelle de la demande

Attention :
Toute requête vers un site web externe peut exposer publiquement l'identité de l'établissement. Une vigilance particulière est donc requise dans l'utilisation des services en ligne.
La consultation de contenus illicites (images, vidéos, écrits), le téléchargement illégal ou l'accès à des sites frauduleux sont strictement interdits et peuvent exposer l'utilisateur à des sanctions disciplinaires et pénales.

Dans le cadre de leur activité professionnelle, les agents du CDG peuvent être amenés à consulter divers sites internet (CDG33, CIG Grande Couronne, CIG Petite Couronne, INTERSTIS…) dont les espaces privés sont soumis à des codes d'accès. Ceux-ci sont créés et gérés par le service informatique.

3.4. Wifi

Trois réseaux Wi-Fi distincts sont disponibles au sein du Centre de Gestion :
- CDG16 Private : réservé aux équipements professionnels gérés par le service informatique et pour les agents.
- CDG16 Public : destiné aux visiteurs ou prestataires, avec accès restreint et isolé du réseau principal.
- CDG16 VIP : destinés aux personnes extérieures au CDG mais avec un accès récurent (Conseil Medical, élus …)

Il est **formellement interdit** de connecter un appareil personnel (téléphone, tablette, ordinateur portable, ...) au réseau CDG16 Private, y compris pour la consultation de courriels professionnels.
L'utilisation du réseau Wifi CDG16 Public devra faire l'objet d'une demande préalable auprès du service informatique, qui générera des coupons à usage personnel et unique. Chaque utilisateur de coupon devra être impérativement recensé par l'agent qui les distribuera. La validité d'un coupon peut varier à la demande (1h à plusieurs jours).
L'usage de ces réseaux est soumis à traçabilité et à contrôle, conformément aux obligations de sécurité et de protection des données. Tout usage abusif ou non autorisé pourra donner lieu à des mesures correctives.

3.5. Messagerie électronique

3.5.1. Usage professionnel et personnel

La messagerie électronique mise à disposition par l'établissement est destinée à un usage professionnel. L'utilisation à des fins privées de l'adresse professionnelle ne saurait être qu'exceptionnelle et ne porter atteinte au bon fonctionnement du service, ni à la sécurité du système d'information.
Seuls les messages identifiés comme personnels (par une mention explicite dans l'objet, tel que « Personnel ») bénéficient du secret des correspondances et du droit au respect de la vie privée.
À défaut de mention claire, les messages sont présumés professionnels.
L'établissement ne peut accéder aux messages marqués comme personnels, sauf en cas de circonstances exceptionnelles prévues par la loi.

3.5.2. Consultation et accès à distance

Les agents peuvent consulter leur messagerie professionnelle à distance, via un navigateur, à l'adresse suivante : https://messagerie.cdg16.fr
En cas d'utilisation d'un ordinateur personnel, les fichiers téléchargés doivent être effacés dès que possible.
En cas d'absence pour raison de santé, la direction peut, par mesure de précaution et afin de favoriser le rétablissement de l'agent, décider de suspendre temporairement l'accès à distance à la messagerie.

3.5.3. Gestion des absences et continuité du service

En cas d'absence ponctuelle non prévisible, la continuité de service doit obligatoirement être assurée.
Aussi, la messagerie pourra être consultée ou transférée vers une autre boîte fonctionnelle du service et traitée par un autre agent.
Si l'agent n'a pas activé de message d'absence, le service informatique s'en chargera, en précisant que la correspondance est redirigée vers un collègue identifié.

3.5.4. Comportements et vigilance

L'envoi ou la réception de contenus illicites, diffamatoires, injurieux, racistes, sexistes, xénophobes, homophobes, ou contraires à l'ordre public et aux bonnes mœurs est formellement interdit.
Les propos injurieux transmis via la messagerie ou publiés sur des forums électroniques constituent une atteinte au respect des personnes et peuvent entraîner des sanctions disciplinaires et/ou pénales.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et leur qualité à recevoir communication des informations transmises.
La vigilance des expéditeurs doit redoubler en présence d'informations à caractère personnel et/ou confidentiel.

- Spams, chaînes et abonnements :

L'établissement dispose d'un dispositif de filtrage anti-spam pour limiter les messages indésirables.
Les utilisateurs sont invités à :

- ne pas multiplier les abonnements à des newsletters ou listes de diffusion non professionnelles,
- ne pas donner suite aux messages incitant à rediffuser des chaînes de mails ou contenus douteux.

- Taille et gestion de la messagerie :

- L'envoi de pièces jointes est soumis à une limite de taille automatique de 20Go maximum.
- La messagerie disposant d'un espace de stockage limité, il revient à l'utilisateur de procéder régulièrement à la suppression des messages inutiles et l'archivage des courriels professionnels importants.

- Sécurité, phishing et virus :

Les utilisateurs doivent faire preuve de vigilance face aux tentatives de hameçonnage (*phishing*) ou aux virus :

- Vérifier la cohérence de l'adresse de l'expéditeur,
- Vérifier l'identité de l'expéditeur avant d'ouvrir un message ou une pièce jointe,
- En cas de doute, ne pas ouvrir les pièces jointes, ne pas cliquer sur les liens qu'il comporte et prévenir immédiatement le service informatique via une demande d'intervention,
- Le service informatique analysera le message suspect et informera l'agent des suites à donner.

Attention :
Le service informatique ne demande jamais d'identifiants ou de mots de passe par courriel.
Tout message de ce type doit être ignoré et déplacé dans les courriers indésirables.

3.6. Téléphones

L'établissement met à disposition des agents, dans le cadre de leurs missions, des téléphones fixes et/ou mobiles professionnels. Ces moyens de communication sont attribués en fonction des besoins de service.

Le Centre de Gestion utilise un système de téléphonie sur IP permettant la transmission des communications vocales via le réseau informatique. Cette technologie offre une meilleure intégration avec les outils numériques de travail et une gestion centralisée des communications.
Fonctionnalités disponibles :

- Transfert d'appels et mise en attente

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

- Conférences téléphoniques
- Présentation du numéro appelant
- Intégration avec les outils collaboratifs (selon configuration)

Sécurité et continuité de service : Les communications VoIP transitent par l'infrastructure réseau sécurisée de l'établissement. En cas de panne réseau ou électrique, des mesures de continuité de service peuvent être mises en œuvre, notamment le renvoi automatique vers les téléphones mobiles professionnels.

Qualité de service : La qualité des communications VoIP dépend de la bande passante disponible. Les agents sont invités à signaler tout problème de qualité audio au service informatique pour optimisation du réseau.

Compatibilité : Le système VoIP est compatible avec différents terminaux (postes fixes IP, logiciels sur ordinateur, applications mobiles) selon les besoins du service et les autorisations accordées.

3.6.1. Usages

L'utilisation des téléphones fixes à des fins personnelles est tolérée, à condition qu'elle reste ponctuelle, modérée et sans incidence sur l'activité professionnelle.

Les téléphones mobiles mis à disposition de certains agents nomades sont à usage professionnel uniquement. Les agents sont tenus d'en prendre soin et d'informer immédiatement le service informatique en cas de perte, vol ou dégradation.

Les agents utilisant leur téléphone mobile personnel à des fins professionnelles s'engagent à prendre toutes les mesures de sécurité et de confidentialité pour protéger les intérêts de l'établissement et sa responsabilité.

3.6.2. Restrictions techniques

Des restrictions peuvent être mises en place selon les fonctions des utilisateurs. Par exemple :
- certains postes sont limités aux appels nationaux,
- d'autres peuvent permettre les appels internationaux ou vers des numéros surtaxés.

Ces restrictions sont définies par le service informatique en lien avec les responsables hiérarchiques.

3.6.3. Suivi et confidentialité des communications

Conformément aux recommandations de la CNIL, l'établissement ne met pas en œuvre de suivi individuel permanent de l'utilisation des services de téléphonie. Seules des statistiques globales sont collectées pour assurer le suivi général des consommations (entrants/sortants), dans le but de vérifier leur conformité avec les contrats opérateurs et pour suivre l'activité du service (de la journée à l'évolution annuelle).
L'établissement n'a pas accès, par défaut, à l'intégralité des numéros appelés via le serveur de téléphonie ou les téléphones mobiles professionnels.
Toutefois, en cas de consommation manifestement excessive ou anormale, le service informatique peut, sur demande expresse de l'autorité territoriale, accéder aux relevés détaillés d'appels (y compris les numéros complets), dans le respect des principes de nécessité, de proportionnalité et de confidentialité.

3.7. Tablettes numériques

Des tablettes numériques peuvent être mises à disposition d'agents ou d'élus pour un usage professionnel. Les règles définies pour les postes informatiques et les mobiles s'appliquent à ces équipements.

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

3.8. Utilisation des plateformes NUAGE et NIMBUS

L'établissement met à disposition des agents une plateforme sécurisée de stockage et de collaboration appelée NUAGE, basée sur Nextcloud, ainsi qu'une seconde plateforme NIMBUS destinée notamment aux services de Paie à Façon et GeRHi, basé sur la même technologie.

- NUAGE permet aux utilisateurs de :
- Stocker et organiser leurs documents professionnels de manière sécurisée,
- Partager des fichiers ou des dossiers avec des collègues internes ou, sous conditions, avec des partenaires externes. Aussi, l'usage de plateformes de partage (WeTransfert, DropBox…) est proscrit.
- Collaborer en temps réel sur des documents,
- Organiser ou rejoindre des visioconférences sécurisées dans le cadre professionnel.

- NIMBUS permet aux utilisateurs et aux collectivités adhérentes de :
- Stocker et organiser leurs documents professionnels de manière sécurisée,
- Partager des fichiers ou des dossiers avec des collègues internes et/ou les collectivités

- Accès à NUAGE et NIMBUS :
- Par navigateur, via l'adresse sécurisée :

https://NUAGE.cdg16.fr pour l'accès au NUAGE
https://NIMBUS.cdg16.fr pour l'accès à NIMBUS

- Par l'explorateur de fichiers Windows, en utilisant l'outil RaiDrive, qui permet de monter NUAGE et NIMBUS comme un lecteur réseau.

- Règles d'utilisation :
- L'accès est strictement réservé à un usage professionnel.
- Le partage de fichiers vers l'extérieur doit être limité aux besoins du service et sécurisé par mot de passe et durée de validité.
- Il est interdit d'utiliser NUAGE ainsi que NIMBUS pour stocker ou partager des fichiers personnels ou non liés aux missions professionnelles.
- En cas de collaboration externe, les agents doivent appliquer systématiquement les options de sécurisation proposées (protection par mot de passe, expiration automatique des liens).
- Les visioconférences doivent être utilisées uniquement à des fins professionnelles, dans le respect de la confidentialité des échanges.

L'utilisateur est responsable des données qu'il partage ou transfère par l'intermédiaire de NUAGE ou NIMBUS, et doit veiller à respecter les règles de confidentialité et de sécurité définies par l'établissement.

4. UTILISATION DE L'INTELLIGENCE ARTIFICIELLE

Le Centre de Gestion explore l'utilisation et l'intégration de l'intelligence artificielle (IA) afin d'optimiser certaines tâches et d'améliorer l'efficience de ses services.
L'intelligence artificielle générative permet de produire de nouveaux contenus (textes, images, sons, ...) à partir de modèles entraînés sur de vastes ensembles de données. Toutefois, son usage comporte des risques, notamment en matière de fiabilité des contenus générés, de confidentialité des données et de biais algorithmiques.

L'usage de l'IA doit s'inscrire dans un cadre garantissant une utilisation responsable, sécurisée et conforme aux réglementations en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD), en minimisant les risques liés à la confidentialité, à l'exactitude des informations et aux droits des tiers.

- **Accès et utilisation des outils d'IA**

L'accès aux outils d'IA est strictement réservé aux comptes professionnels fournis par le CDG.

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

L'usage de comptes personnels est interdit afin de garantir la traçabilité et la conformité des traitements effectués.
Les outils d'IA doivent être utilisés exclusivement à des fins professionnelles et en cohérence avec les missions du CDG.

- **Bonnes pratiques et interdictions**

Les comptes professionnels étant partagés, chaque utilisateur veille à la gestion de son historique.
Aucune donnée à caractère personnel, sensible ou confidentielle ne doit être saisie ou transférée dans un outil d'IA, même si l'outil est approuvé par le CDG.
Les utilisateurs doivent vérifier la fiabilité et la conformité des contenus générés avant toute diffusion.
Toute utilisation visant à produire, partager ou encourager des contenus illicites, discriminatoires, erronés ou contraires aux valeurs du service public est strictement interdite.

- **Protection des données et conformité RGPD**

Les outils d'IA ne doivent pas être utilisés pour traiter des données personnelles ou sensibles (RSU, identité d'agents, données médicales, documents internes…).
Toute donnée exploitée dans un cadre professionnel doit respecter les principes de minimisation, de confidentialité et de finalité définis par le RGPD.
Certains traitements de données peuvent être soumis à des obligations légales ou réglementaires spécifiques, imposant leur conservation pour une durée déterminée ou limitant leur transmission.
En cas de doute sur la conformité d'un usage, les agents doivent consulter le Délégué à la Protection des Données (DPO)

- **Contrôle et sanctions**

Le CDG16 se réserve le droit de superviser et de contrôler l'usage des outils d'IA afin de s'assurer du respect du présent règlement.
Tout manquement aux règles peut donner lieu à des sanctions disciplinaires.
En cas de constatation d'un usage abusif ou d'une faille de sécurité, l'utilisateur concerné doit immédiatement signaler l'incident à sa hiérarchie ou au DPO.

- **Responsabilités des utilisateurs**

Les agents restent pleinement responsables des contenus générés et diffusés par les outils d'IA, y compris en cas d'erreur ou d'information trompeuse.
Ils doivent faire preuve de vigilance et d'esprit critique face aux réponses fournies par les modèles d'IA.
Toute utilisation contraire aux missions du CDG ou aux règles de déontologie du service public pourra engager la responsabilité individuelle de l'agent concerné.

5. TÉLÉTRAVAIL

Le télétravail constitue une modalité d'organisation du travail autorisée par l'établissement dans des conditions encadrées par la réglementation en vigueur et par la charte du CDG. Les agents exerçant leur activité à distance doivent se conformer aux mêmes obligations de sécurité, de confidentialité et de bon usage des outils informatiques que lorsqu'ils sont présents sur site.
Dans ce cadre, les règles suivantes s'appliquent :

- **L'équipement utilisé doit être sécurisé** : poste de travail fourni par l'établissement ou équipement personnel préalablement validé par le service informatique.
- **L'accès aux ressources professionnelles** (messagerie, NUAGE, logiciels métiers, etc.) s'effectue via des connexions sécurisées (HTTPS, VPN, authentification forte si nécessaire).
- L'agent s'engage à **ne pas stocker localement de données sensibles ou professionnelles** sur un équipement personnel, sauf autorisation expresse.
- Toute anomalie, incident ou suspicion de compromission survenant en situation de télétravail doit être immédiatement signalée au service informatique.

- L'usage du réseau Wi-Fi personnel doit être protégé par mot de passe et chiffré (au minimum WPA2).
- Les échanges à distance (visioconférences, partages de fichiers) doivent être réalisés uniquement via les outils validés par le responsable informatique.

6. DROIT A LA DÉCONNEXION ET CONTINUITÉ DE SERVICE

Le droit à la déconnexion s'applique pleinement aux agents du CDG16 en congé et en dehors des horaires de travail, y compris en télétravail.

En dehors des horaires habituels, aucune réponse aux courriels, appels ou messages (SMS, messagerie) professionnels ne peut être exigée. Ce droit vise à garantir le respect des temps de repos, prévenir les risques de surcharge mentale et préserver l'équilibre entre vie professionnelle et vie personnelle. Les responsables de service doivent veiller à une organisation du travail respectueuse de ce principe, y compris en évitant l'envoi de sollicitations hors temps de travail, sauf cas exceptionnel.

Toutefois, l'absence de l'agent ne doit pas compromettre la continuité de service. Pour ce faire, il doit veiller à permettre l'accès aux documents, applicatifs et informations dont il dispose et nécessaire au bon fonctionnement du service en son absence.
Dans le cas d'une absence imprévue, il pourra être demandé à l'agent l'accès à un espace de travail ou la transmission d'éléments (mot de passe de sites internet, applicatifs…). A défaut, le service informatique pourra ouvrir les accès.
En cas d'absence prolongée, il pourra être demandé à l'agent de restituer ses équipements nomades (PC, téléphone portable…).

7. ADMINISTRATION DU SYSTEME D'INFORMATION

Afin d'assurer la sécurité, la continuité de service et la protection des données, plusieurs dispositifs techniques et organisationnels sont mis en place au sein du Centre de Gestion.

7.1. Systèmes de filtrage et de traçabilité

Des systèmes automatiques sont déployés à titre préventif pour :
- Filtrer l'accès aux sites web non autorisés,
- Éliminer les courriels non sollicités (spam),
- Bloquer certains protocoles non autorisés (peer-to-peer, messageries instantanées...).

Le service informatique est habilité à réaliser, sans avertissement préalable, les investigations techniques nécessaires pour résoudre les dysfonctionnements ou garantir l'intégrité du système d'information.
La journalisation des accès (logs) est utilisée pour assurer la traçabilité des événements informatiques. Les fichiers de journalisation enregistrent :
- Les dates et heures de connexion,
- Les identifiants utilisés,
- Les postes de travail concernés,
- La nature de l'événement.

Ces données sont exclusivement accessibles au service informatique et sont conservées pour une durée maximale de 12 mois.

En cas de suspicion de manquement à la présente charte, la direction pourra solliciter la communication de données de journalisation (site internet, connexion, téléphonie…). L'agent concerné en sera avisé.
Ces données peuvent en outre être fournies aux autorités compétentes selon les dispositions légales et réglementaires en vigueur.

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

Elles peuvent enfin être communiquées à l'utilisateur pour les seules données qui le concernent directement et individuellement en application de son droit d'accès.

7.2. Gestion du poste de travail

Le service informatique peut intervenir à distance sur les postes de travail pour des besoins de maintenance ou de mise à jour.
Toute intervention se réalise avec l'accord exprès de l'utilisateur, après validation d'un mot de passe à usage unique.
Seul le service informatique est habilité à initier ou autoriser des accès distants.
En l'absence de l'utilisateur (poste inoccupé), des interventions techniques peuvent être réalisées sans notification préalable pour assurer le bon fonctionnement du système d'information.

7.3. Stockage des données

L'établissement met à disposition des agents une plateforme sécurisée de stockage et de collaboration appelée NUAGE, basée sur Nextcloud.

Règles d'utilisation :

- Tous les documents professionnels doivent être stockés sur NUAGE.
- NUAGE permet un accès sécurisé aux documents, notamment en mobilité ou en télétravail.
- Le partage de documents doit être réalisé en limitant les droits d'accès aux seules personnes habilitées.
- Lors d'un partage externe, il est obligatoire de sécuriser les accès (mot de passe, date d'expiration, permissions spécifiques).
- L'utilisation de NUAGE est strictement réservée à un usage professionnel.

Les données présentes sur NUAGE font l'objet d'une sauvegarde quotidienne, avec une rétention de 14 jours ouvrés.

Important : Tout stockage local sur les disques durs des postes de travail est proscrit, sauf dérogation expresse accordée par le service informatique. Aucune sauvegarde n'est assurée.

7.4. Procédure applicable lors du départ d'un utilisateur

Lors du départ d'un agent :

- le matériel informatique mis à disposition doit être intégralement restitué.
- les données et fichiers personnels doivent être effacés de l'environnement professionnel.
- les documents professionnels doivent être laissés intacts afin d'assurer la continuité du service. Toute destruction de données non autorisée pourra être sanctionnée même après le départ de l'agent.
- les mails de l'agent sont conservés durant 4 ans. L'agent dispose d'un droit à consultation, même après son départ, en cas de poursuites.

Les accès aux comptes informatiques, à NUAGE, à NIMBUS et à tout site professionnel en lien avec l'activité du CDG sont supprimés dès le départ effectif de l'agent.

7.5. Mesures d'urgence par le service Informatique

En cas d'urgence, le service informatique peut :

- déconnecter immédiatement un utilisateur,
- isoler ou neutraliser un fichier ou des données manifestement dangereuses,
- imposer temporairement des limitations techniques (réduction de débit, restriction d'impression…),
- suspendre des services pour protéger l'intégrité du système d'information,

- interrompre toute activité suspecte menaçant la sécurité.

Ces actions peuvent être réalisées avec ou sans préavis, selon la gravité de la situation.

8. SOBRIÉTÉ NUMÉRIQUE

- **Stockage et gestion des données**

Afin de limiter l'impact du stockage des données ainsi que pour faciliter la gestion, il est recommandé aux agents d'utiliser les dossiers partagés dans le but de limiter les copies et doublons de fichiers.
De même, il est demandé d'utiliser le NUAGE pour communiquer des fichiers par mail (lien de partage) et éviter d'envoyer les fichiers en pièce jointe.

- **Usage des mails**

Le mail est un outil incontournable car il apporte de nombreux avantages tels qu'une communication instantanée, la possibilité d'inclure plusieurs destinataires, une transmission des documents numériques ainsi que l'assurance d'une traçabilité et d'un suivi des échanges.
Malgré tout, l'excès de mails peut générer une surcharge d'informations puis un stress lié au devoir de traiter cette masse d'informations, parfois dans l'urgence.
La facilité d'utilisation du mail en fait l'outil de communication privilégié au détriment des autres canaux. Cela peut cependant aller jusqu'à l'excès. Il est donc conseillé de cadrer cette pratique :

- ✓ Lorsque la réponse est immédiate ou le sujet nécessite une succession d'échanges, les conversations doivent privilégier le face-à-face ou le téléphone ;
- ✓ Lorsque la réponse peut être différée, les sujets peuvent être formalisés dans un court message, et il est souhaitable de conserver une traçabilité, le message doit favoriser l'utilisation du mail.

Voici quelques bonnes pratiques :

❖ Quand je reçois un mail :

- Ne pas lire ou traiter ses mails pendant une autre activité
- Eviter de croire que tout est urgent et/ou prioritaire à traiter
- Utiliser la fonction de réponse automatique ou de réponse différée
- Instaurer des créneaux réguliers de consultation des mails
- Trier, supprimer et archiver régulièrement ses mails
- Faciliter le tri en utilisant : les règles de diffusion, les systèmes de répertoire pour le classement, et des règles d'archivage (en fonction de la date par exemple)
- Ne pas laisser sa boite mail ouverte en permanence (risque d'interruption de tâches) supprimer les notifications pendant certaines périodes
- Penser systématiquement à décrocher les cases autorisant la réception de newsletters ou publicités des sites internet où l'on s'inscrit.

❖ Quand j'envisage d'envoyer un mail :

- Toujours adapter le canal de diffusion en fonction du message et du contexte
- Ne pas répondre en dehors des heures du bureau et par conséquent ne pas mélanger les boites mails professionnelles et personnelles
- Limiter et réduire le nombre de destinataires
- Limiter l'utilisation du bouton « répondre à tous » et « transférer » en fonction du contexte
- L'objet du mail doit être clair concis et compréhensible
- Lors de la formulation d'une demande, préciser une échéance de réponse, pour permettre au destinataire de s'organiser en conséquence
- Limiter chaque mail à 7 idées-clés maximum pour permettre au récepteur du mail de retenir l'essentiel
- Utiliser les outils de mise en forme pour faciliter la lecture, mettre en valeur et améliorer la compréhension (éviter les majuscules, points de suspension et points d'exclamation).

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

- **Sobriété énergétique**

Les équipements informatiques représentent une part non négligeable de la consommation électrique des entreprises et collectivités.
Quelques gestes simples permettent de réduire l'impact et les coûts :

- Eteindre le poste de travail et les périphériques associés en cas d'absence. Même en veille, un ordinateur consomme de l'énergie,
- Désactiver les fonctions wifi, bluetooth quand elles ne servent pas,
- Réduire la luminosité des écrans et éteindre les doubles écrans lorsqu'ils ne sont pas utilisés,

- **Gestion des impressions**

Les copieurs consomment de l'énergie même en veille. C'est pourquoi ils doivent être éteints durant la nuit.
Les utilisateurs sont en outre invités à :

- Privilégier l'impression recto/verso,
- Privilégier les impressions en noir et limiter les impressions en couleurs aux seuls documents le nécessitant.

Ces paramètres doivent être pris en compte sur chacun des postes informatiques au niveau de la configuration par défaut des impressions sur les copieurs.

9. ENTRÉE EN VIGUEUR

La présente charte a été adoptée par le Conseil d'Administration du Centre de Gestion le ……2025, après avis du Comité Social Territorial du 6 octobre 2025.

Elle entre en vigueur à compter du 1er novembre 2025.

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr

ANNEXE I
DISPOSITIONS LEGALES ET REGLEMENTAIRES APPLICABLES

Protection des données personnelles

- Règlement (UE) 2016/679 du 27 avril 2016, dit Règlement Général sur la Protection des Données (RGPD), applicable depuis le 25 mai 2018.
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par :
- la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles,
- et l'ordonnance n°2018-1125 du 12 décembre 2018 pour l'adaptation au RGPD.

Sécurité des systèmes d'information

- Directive (UE) 2022/2555 du 14 décembre 2022, dite directive NIS2, relative aux mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'Union européenne.
- Loi n°2018-133 du 26 février 2018 renforçant la sécurité des réseaux et systèmes d'information.
- Code de la fonction publique (partie législative applicable aux agents publics) – Obligation de discrétion, de confidentialité et de sécurité des systèmes d'information (articles L121-1 et suivants).

Dispositions pénales applicables

- Code pénal :
- Articles 226-16 à 226-24 relatifs à la protection des données personnelles.
- Articles 323-1 à 323-7 relatifs aux atteintes aux systèmes de traitement automatisé de données (loi Godfrain sur la fraude informatique).
- Article L.335-2 relatif aux infractions en matière de propriété intellectuelle (contrefaçon de logiciels).
- Code pénal – partie réglementaire :
- Articles R.625-10 à R.625-13 (infractions aux obligations de déclaration ou de sécurité des données personnelles).
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

Propriété intellectuelle

- Loi n°94-361 du 10 mai 1994 transposant la directive européenne sur la protection juridique des logiciels.
- Code de la propriété intellectuelle, notamment les articles relatifs aux droits d'auteur sur les logiciels.

Remarques importantes

- Le non-respect des règles de sécurité informatique, de protection des données ou de confidentialité engage la responsabilité disciplinaire, civile et pénale des utilisateurs.
- Les obligations décrites sont susceptibles d'évoluer en fonction des modifications législatives, réglementaires ou des recommandations des autorités compétentes (CNIL, ANSSI, ENISA…).

30, rue Denis Papin – CS 12213 – 16022 ANGOULÊME Cedex – 05.45.69.70.02 – cdg16@cdg16.fr