



Centre de gestion  
de Seine-et-Marne  
Fonction Publique Territoriale



# CHARTRE INFORMATIQUE

Direction des systèmes d'information et du numérique | Septembre 2022

**10, Points de Vue – CS 40056 – 77564 LIEUSAIN CEDEX**  
Tél. 01 64 14 17 00 - [cdg77.fr](http://cdg77.fr)

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## TABLE DES MATIÈRES

1. Objectif de la charte .....	3
2. Champ d'application .....	3
3. Application et diffusion de la charte .....	4
4. Principes généraux sur l'usage des ressources informatiques .....	4
5. Protection des données .....	5
6. Définitions .....	6
7. Les interlocuteurs .....	8
8. Utilisation des moyens mis à disposition .....	8
9. Création de répertoires privés et organisation des documents .....	11
10. Droits et devoirs des utilisateurs .....	12
11. Précisions relatives à l'application de la charte aux délégués ou représentants du personnel .....	16
12. Utilisation des supports de stockage de données externes .....	17
13. Utilisation des équipements personnels (BOYD) .....	17
14. Accès à distance .....	18
15. Stockage des données .....	18
16. Mise a disposition des équipements .....	19
17. Procédures spécifiques au matériel de prêt .....	19
18. Cas particulier de vol ou de perte de matériel .....	20
19. Utilisation des moyens d'impression .....	20
20. Utilisation de la messagerie .....	20
21. Messages : modalités d'archivage et de destruction des messages .....	23
22. Délégation de la boîte mail .....	23
23. Départ d'un agent .....	24
24. Cas de l'absence ou de l'absence prolongée de l'agent .....	24
25. Cas particulier du décès d'un agent .....	26
26. Gestion des spams .....	26
27. Règles de sécurité .....	26
28. Droit à la déconnexion .....	27
29. Sanctions .....	29
30. Réglementation applicable .....	29
31. Signature de l'agent .....	33

# 1. OBJECTIF DE LA CHARTE

Le Centre de Gestion de Seine-et-Marne (CDG 77) met à disposition des agents un ensemble de moyens informatiques et de communication nécessaires à l'exercice de leurs missions. La présente charte a pour objet de définir les conditions d'utilisation et les règles de bon usage de ces moyens informatiques, mais également d'assurer le développement de l'utilisation du système d'information dans le respect des lois et des règlements.

La charte définit les conditions d'accès et les règles d'utilisation des ressources informatiques, des services internet, de messagerie et téléphonique, des matériels nomades, 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, ainsi que les supports de données.

**Les supports de données concernent notamment :** ordinateurs portables et fixes, tablettes tactiles, téléphones portables et fixes, imprimantes, logiciels, clés USB, disques durs externes ...).

Elle vise à sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle du CDG 77.

**Ainsi, la charte :**

- précise les principaux droits, devoirs et responsabilités des utilisateurs en accord avec la législation en vigueur ;
- informe chaque utilisateur sur la conduite à tenir vis-à-vis du système d'information ;
- instaure un usage correct des ressources informatiques et des services internet, selon des règles minimales de courtoisie et de respect d'autrui.

Ces règles ont une valeur contraignante liée à la référence légale ou réglementaire auxquelles elles se réfèrent.

Certains documents peuvent renforcer ou compléter les règles générales de la présente charte, il appartient à l'utilisateur de prendre connaissance de ces textes dans le cadre de ses missions.

## 2. CHAMP D'APPLICATION

La charte concerne tous les agents du CDG 77 ainsi que l'ensemble des personnes habilitées par un donneur d'ordre du Centre de gestion de Seine-et-Marne qui utilise les ressources informatiques et les moyens de communication dans l'exercice de ses missions (prestataires, élus, partenaires, vacataires, stagiaires, sous-traitants etc.).



**Cette charte s'applique à l'ensemble du personnel du Centre de gestion de Seine-et-Marne ainsi qu'aux stagiaires, alternants et salariés d'entreprises extérieures exécutant un travail au sein du CDG 77.**

**L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service. Elle suit des règles strictes présentées ci-après.**

Accusé de réception en préfecture  
N° : 22-0233  
Date de télétransmission : 28/09/2022  
Date de réception en préfecture : 28/09/2022

### 3. APPLICATION ET DIFFUSION DE LA CHARTE

La charte a été approuvée lors du Conseil d'administration du 23 septembre 2022.

Elle fait l'objet d'une publicité garantissant sa diffusion et sa prise de connaissance par tous les utilisateurs auxquels elle s'adresse.

Elle est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur demande. Elle est systématiquement remise à tout nouvel arrivant contre récépissé.

**En fonction du statut de l'utilisateur, elle fait l'objet d'une acceptation expresse :**

- soit par l'apposition de la signature manuscrite du nouvel agent, lors de sa prise de fonction ;
- soit par le biais d'une case à cocher (« j'ai bien pris connaissance de la charte informatique du CDG 77 et en accepte l'ensemble des dispositions »), lors de sa première connexion (et des différents rappels) au système d'information. Soit par le biais d'une annexe aux contrats conclus avec les utilisateurs.

Elle est rattachée en tant que pièce contractuelle, aux contrats ou conventions conclus avec les prestataires du CDG77, et ce quel que soit leur statut.

Les règles édictées dans la présente charte sont susceptibles d'être complétées ou modifiées compte tenu de la variété et de l'évolution permanente des outils informatiques et de communication ou des législations applicables. Dans de telles circonstances, le présent document fera l'objet d'un avenant.

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

### 4. PRINCIPES GÉNÉRAUX SUR L'USAGE DES RESSOURCES INFORMATIQUES

L'usage des ressources informatiques et des services internet ainsi que les informations auxquelles un utilisateur a accès sont réservés au cadre de l'activité professionnelle. L'activité professionnelle représente toute l'activité administrative, technique et de gestion effectuée dans le cadre des fonctions de chacun des utilisateurs. L'utilisation des ressources informatiques partagées et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers.

Les dossiers et fichiers créés par un utilisateur grâce à l'outil informatique mis à sa disposition par le CDG 77 sont présumés, avoir un caractère professionnel.

**Chaque utilisateur s'engage à :**

- ne pas modifier la configuration des ressources (matériel, réseaux, etc.) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées au sein du CDG 77 ;
- ne pas faire de copies des logiciels commerciaux acquis par le CDG 77 ;
- ne pas installer, télécharger ou utiliser sur le matériel des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne pas divulguer des informations dignes de confiance, et sans autorisation des personnes habilitées au sein du CDG 77 ;

Versant région crépitac  
077-287708326-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 29/09/2022

- ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites (virus, malware, chevaux de Troie, etc.) ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés ;
- informer immédiatement sa hiérarchie et le service informatique de toute perte, anomalie ou tentative de violation de ses codes d'accès personnels ;
- effectuer une utilisation rationnelle et loyale des services et notamment du réseau, de la messagerie, des ressources informatiques, afin d'en éviter la saturation ou l'abus de leur usage à des fins personnelles ;
- récupérer sur les matériels d'impression (imprimantes, télécopieurs) les documents sensibles envoyés, reçus, imprimés ou photocopiés ;
- ne pas quitter son poste de travail en laissant accessible une session en cours et à ne pas se connecter sur plusieurs postes à la fois.

#### Chaque utilisateur est :

- responsable du matériel qui lui est confié et doit en respecter l'intégrité ;
- responsable du bon usage de son identifiant, de son mot de passe et des droits d'accès et doit respecter les consignes de sécurité énoncées dans la présente charte ;
- responsable de l'information qui lui est confiée et doit prendre toutes les précautions nécessaires afin de préserver l'intégrité et la confidentialité des données qu'il traite ou échange.

## 5. PROTECTION DES DONNÉES

Un recours croissant à l'usage des technologies de l'information exige que chacun respecte les principes du droit à la protection des données personnelles. La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et le Règlement Général sur la Protection des Données définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent et doivent être effectués. Ces réglementations ouvrent aux personnes concernées par les traitements différents droits des données collectées et enregistrées sur leur compte.

Il est obligatoire de consulter au préalable le Délégué à la Protection des Données (DPO) avant la création d'un nouveau traitement de données à caractère personnel. Ainsi, **toute création, modification ou suppression de fichier comportant des données à caractère personnel doit, préalablement à sa mise en œuvre, être déclarée auprès du Délégué à la Protection des Données**, qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévues, les destinataires des données, le moyen d'information des personnes concernées et les mesures de sécurité à déployer pour protéger les données.

Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel du CDG 77 au fur et à mesure de leur mise en œuvre. Ce registre est tenu à disposition de toute personne en faisant la demande.

Le Délégué à la Protection des Données veille au respect des droits des personnes. En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le Délégué aux coordonnées suivantes :

- nom, prénom ;
- direction, service ;
- adresse électronique ;
- téléphone.

## 6. DÉFINITIONS

### Utilisateur

Toute personne autorisée qui accède et utilise les outils informatiques et les moyens de communication du CDG 77 : agents, salariés, stagiaires, personnels de sociétés prestataires, visiteurs occasionnels, pour un usage professionnel.

### Ressources informatiques

Moyens informatiques de calcul ou de gestion locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau informatique administré par la Direction des Systèmes d'Information et du numérique (smartphone, ordinateur fixe ou portable, tablette, clé USB, disque externe, équipements de reprographie). Les moyens de télécommunication (téléphones fixes, sans fil, ou GSM).

### Services Internet

La mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : web, messagerie, webmail, forums, chat, SFTP.

### Compte

Le moyen d'accès (nom d'utilisateur, mot de passe) qui permet à un utilisateur de se connecter aux ressources informatiques et aux services Internet du CDG 77.

### BYOD

Expression anglaise « Bring Your Own Device » (en français : « Apportez Votre Equipement personnel de Communication » ou AVEC l'usage d'équipements informatiques personnels dans le contexte professionnel. Il peut s'agir par exemple d'un utilisateur qui, pour se connecter au réseau du CDG 77 utilise un ordinateur, une tablette ou son smartphone personnel.

### Équipements nomades

Tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB, etc.).



#### Pour aller plus loin

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par le biais d'un procédé de chiffrement suffisant. On applique [la recommandation de l'ANSSI sur le nomadisme numérique](#) dont la dernière version date de 2018.

Service Informatique de la Préfecture  
077-287708325-20220923-22-33-DE  
Date de transmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## **Système d'information (SI)**

Il recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par le CDG 77. Il est aussi constitué des dispositifs numériques nomades personnels ou professionnels connectés au CDG 77 (tablettes, ordinateurs portables, téléphones portables, etc.). Il s'agit également de tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure, ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

## **Donnée utilisateur ou administré**

Toute les information circulant ou accessible depuis les systèmes d'information du CDG 77 ou transitant sur ces systèmes d'information, et/ou générée par les utilisateurs.

## **Donnée professionnelle**

Toute information liée directement ou indirectement à l'activité professionnelle, notamment par exemple numéro de matricule, téléphone professionnel.

## **Donnée à caractère personnel**

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.

## **Code malveillant, virus, malware**

Un code malveillant est un logiciel qui a pour effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, la messagerie, mais aussi les cédéroms, les supports de stockage externes (clef USB, disque dur externe, mémoire flash).

## **Confidentialité**

Fait d'assurer que l'information n'est accessible qu'aux personnes autorisées. La confidentialité est une obligation légale pour les données personnelles.

## **Demande d'accès**

Dans le cas où un agent ne disposerait pas des informations nécessaires à ses fonctions, il doit en faire la demande à son responsable hiérarchique selon une procédure définie au sein du CDG 77.

## **Service des systèmes d'Information et du numérique**

Le Service des Systèmes d'Information est le service responsable du fonctionnement et de la sécurité des Systèmes d'Information. Il dispose des droits les plus étendus pour contrôler l'utilisation faite du Système Informatique par les Utilisateurs.

## **Disponibilité**

Fait d'assurer que les ressources nécessaires à la fourniture d'un service du Système Informatique soient accessibles lorsqu'elles sont sollicitées.

## **Droits d'accès**

Les droits d'accès définissent ce à quoi il est possible d'accéder avec le nom d'utilisateur et le mot de passe. Ils sont différents d'un utilisateur à l'autre en fonction de sa position dans la hiérarchie ou de ses fonctions.

Accusé de réception en préfecture  
107720825-P0210920-22-02-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## 7. LES INTERLOCUTEURS

### 7.1 Le service informatique

Le « support utilisateur » répond aux questions générales relatives à cette charte de bon usage des systèmes d'information, ce service peut apporter un conseil sur les usages numériques préconisés.

### 7.2 L'encadrement direct de l'agent

L'encadrement s'assure de l'adéquation entre les exigences des missions dévolues à l'agent (notamment précisées dans la fiche de poste) et les moyens à déployer pour leur réalisation ainsi que les méthodes à utiliser. Toute demande d'équipements et de moyens doit être soumise et validée par la hiérarchie directe de l'agent avant d'être adressée au service informatique.

## 8. UTILISATION DES MOYENS MIS À DISPOSITION

### 8.1 Configuration des postes de travail

Le poste de travail est la propriété du CDG 77 et est confié aux utilisateurs afin de leur permettre d'assurer leurs tâches professionnelles. Il s'agit d'un outil de travail dont l'agent est responsable et pour lequel celui-ci doit respecter les règles d'usage décrites ci-après.

**Le poste de travail** (PC fixe, ordinateur portable, tablette ou smartphone) représente l'ensemble des moyens matériels affectés à un utilisateur pour réaliser les missions qui lui sont confiées.

**L'environnement de travail** désigne ici l'ensemble des moyens logiciels (systèmes d'exploitation, applications métier) ou immatériels (espaces de stockage ou d'archivage, documents numériques) nécessaires à la réalisation des tâches professionnelles.

Chaque utilisateur s'engage à :

- ne pas modifier la configuration des ressources (matériel, réseaux, etc.) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées au sein du CDG 77 ;
- ne pas connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par le service informatique interne ;
- ne pas déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade ») ;
- ne pas brutaliser le matériel ou le détourner de son usage initial ;
- ne pas nuire au fonctionnement des outils informatiques et de communications.

**Toute installation de logiciels supplémentaires (logiciels de consultation de fichiers multimédia) est subordonnée à l'accord du service des systèmes d'information.**

## 8.2 Responsabilité de l'information confiée

Les données numériques et l'information en général constituent le patrimoine immatériel du CDG 77 et sa principale richesse. Chaque agent est responsable de l'information qui lui est confiée et doit prendre toutes les précautions nécessaires afin de préserver l'intégrité et la confidentialité des données qu'il traite ou échange.

L'utilisateur est responsable des droits qu'il donne aux autres utilisateurs ; il lui appartient de protéger les données qui lui sont confiées en utilisant les différents moyens de sauvegarde mis à sa disposition.

### Accès aux données

Dans le cadre de ses missions un agent peut avoir accès à des données sensibles (RH, données sociales ou, données financières, de santé, etc.). Dans ce cadre, l'agent doit :

- veiller à ce que leur intégrité et leur confidentialité soient strictement respectées et qu'elles ne soient pas détournées de l'usage et de la finalité prévus ;
- prendre toutes les précautions de sécurité requises lors du transit d'informations confidentielles au sein du CDG 77 et à l'extérieur (chiffrer les données au moment de leur envoi par mail).

### Les agents ne doivent pas :

- tenter d'accéder à des informations ou à des applications en dehors des droits qui leur sont attribués. En cas de détection d'une faille, chaque agent doit le signaler immédiatement à la Direction des systèmes d'information et du numérique (DSIN) et en informer la hiérarchie ;
- utiliser de données professionnelles à des fins personnelles ;
- laisser l'accès à son environnement de travail à des personnes non habilitées ;
- tenter de lire, modifier, copier ou détruire des données autres que celles qui appartiennent en propre à l'agent ;

**Pour rappel les logiciels métier sont désormais munis d'une fonction de journalisation permettant de tracer les actions effectuées par les utilisateurs en lecture, écriture, modification, suppression.**

Chaque agent doit procéder à la protection des informations professionnelles qui lui sont confiées en veillant à leur enregistrement sur des emplacements protégés et sauvegardés (serveurs, réseaux de stockage de données, arborescence bureautique du service).

**L'enregistrement de données sur le poste en local doit rester une exception et ne saurait constituer une règle de classement et de gestion de ces informations.**

## 8.3 Utilisation des moyens informatiques et des moyens nomades

L'utilisateur s'interdit de prêter les outils informatiques, notamment les équipements portables, mis à sa disposition à tout tiers du CDG 77. Il doit prendre soin des matériels qui sont mis à sa disposition par l'administration et informer le service informatique dans les plus brefs délais, de toute détérioration, perte ou vol. Il doit également signaler tout fonctionnement anormal des matériels ou logiciels mis à sa disposition.

Dans l'hypothèse d'une utilisation des moyens informatiques non conforme à la charte informatique, la responsabilité personnelle de l'utilisateur pourrait être engagée.

Le CDG 77 se réserve le droit de restreindre ou suspendre temporairement l'utilisation privée des moyens informatiques sans préavis en cas de danger pour le système d'information : accès à des sites réputés dangereux, attaques virales, intrusions, et de prendre les mesures nécessaires pour rétablir les ressources informatiques à un niveau compatible avec l'activité du CDG 77 (interruption de flux réseaux sur consommateurs de bande passante, déplacement ou suppression de fichiers volumineux, par exemple).

Les équipements informatiques nomades (PC portables, tablettes et smartphones notamment) mis à disposition par le CDG 77 sont équipés de dispositifs de protection permettant de les connecter à Internet depuis un accès domestique ou autre dans les meilleures conditions de sécurité.

Les équipements nomades munis d'accès directs à Internet (par carte 3G/4G par exemple) ne doivent pas être connectés simultanément au système d'information du CDG 77 et à un autre réseau externe (Internet par exemple).

Les dispositifs de protection de ces équipements peuvent évoluer sans préavis en fonction de l'évolution des technologies, des risques et d'autres paramètres. Le CDG 77 peut faire évoluer ces dispositifs à sa convenance.

**Il est strictement interdit aux utilisateurs de retirer les protections des ressources mises à leur disposition sous peine de sanction.**

## 8.4 Utilisation du poste de travail à des fins privées

L'utilisation du courrier électronique et des moyens informatiques à des fins personnelles est autorisée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels.

Concernant la messagerie, les messages personnels doivent être marqués « PERSONNEL » ou « PRIVÉ » et être stockés dans un répertoire portant le même nom. Le CDG 77 n'assume aucune responsabilité quant à la sauvegarde des données privées des agents.



### Pour aller plus loin

#### L'accès au poste informatique ou à la messagerie

L'employeur doit respecter le secret des correspondances privées. Une communication électronique émise ou reçue par un employé peut avoir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles L.226-15 (pour le secteur privé) et L.432-9 (pour le secteur public) du Code pénal.

La Cour de cassation a affirmé, dans un arrêt du 2 octobre 2001 (arrêt « Nikon »), qu'un employeur ne saurait prendre connaissance de messages personnels d'un employé sans porter atteinte à la vie privée de celui-ci (article 9 du code civil) et au principe du secret des correspondances (article 226-15 du code pénal), quand bien même une utilisation à des fins privées aurait été proscrite par l'employeur.

Pour autant, le principe du secret des correspondances connaît des limites dans la sphère professionnelle. Il peut également être levé dans le cadre d'une instruction pénale ou par une décision de justice.

#### **Tout ce qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'employeur peut y accéder librement.**

La Cour de cassation considère qu'un message envoyé ou reçu depuis le poste de travail mis à disposition par l'employeur revêt un caractère professionnel, sauf s'il est identifié comme étant « personnel », dans l'objet du message (Cour de cassation, 30 mai 2007).

#### **Il appartient à l'employé d'identifier les messages qui sont personnels. À défaut d'une telle identification, les messages sont présumés être professionnels.**

La nature personnelle d'un message peut figurer dans l'objet du message ou dans le nom du répertoire dans lequel il est stocké.

Source CNIL Juin 2017

## 9. CRÉATION DE RÉPERTOIRES PRIVÉS ET ORGANISATION DES DOCUMENTS

De la même manière que pour les messages, les documents personnels doivent être marqués « PERSONNEL » ou « PRIVÉ » et être classés **dans un dossier du même nom prévu à cet effet.**

**En outre, il est formellement interdit de sauvegarder des fichiers personnels sur les serveurs du CDG 77.**

Les documents professionnels doivent être gérés conformément aux consignes liées aux usages et missions de la direction dans le cadre de l'organisation générale du CDG 77. Le nommage des documents doit être conforme aux conventions du CDG 77 (noms explicites, sans caractères spéciaux ou accentués).

Il est recommandé de supprimer régulièrement les versions obsolètes des documents et de ne conserver que celles qui sont nécessaires et suffisantes, pour ne pas surcharger les espaces de stockage.

La suppression de documents nativement numériques doit se faire conformément à la politique d'archivage du CDG 77.

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## 10. DROITS ET DEVOIRS DES UTILISATEURS

### 10.1 Utilisation des postes de travail et des équipements mobiles

#### 10.1.1 Postes de travail

La Direction des systèmes d'information et du numérique (DSIN) est la seule entité habilitée à donner l'autorisation d'installer une application ou un périphérique sur le poste de travail. Sans autorisation de cette entité, aucun utilisateur ne doit installer de lui-même un périphérique ou un logiciel. De même, l'Utilisateur n'est pas autorisé à exécuter un logiciel non référencé par la DSIN du CDG 77. Le fond d'écran ou de l'écran de veille du poste de travail peut être personnalisé mais ne doit pas porter atteinte à l'image du CDG 77. D'autre part, sans autorisation du service informatique du CDG 77, il est interdit de relier les ordinateurs portables fournis par la DSIN à une autre connexion Internet que celle fournie par celui-ci.

#### Par ailleurs, l'Utilisateur doit :

- signaler à sa hiérarchie et au service informatique tout incident de sécurité avéré ou soupçonné dans les plus brefs délais ;
- éteindre quotidiennement son poste de travail et le verrouiller obligatoirement (Ctrl+Alt+Supp) en cas d'absence, même brève. Il mettra hors-tension son poste de travail en cas d'absence prolongée (plusieurs heures ou durant la nuit et les Week-end ou lors de ses congés) afin de minimiser les risques d'accès frauduleux, de limiter la consommation électrique, et faciliter les mises à jour s'effectuant au démarrage ou à l'arrêt du poste.

#### L'Utilisateur ne doit pas :

- profiter des privilèges exceptionnels pouvant lui être accordés sur le système d'information à des fins non légitimes ou en les détournant de leur finalité.
- masquer son identité ou usurper l'identité d'autrui par quelque moyen que ce soit ;
- désactiver ou désinstaller volontairement la solution antivirus ou toute application installée par défaut sur son poste.

#### 10.1.2 Équipement mobile

- Il est obligatoire de protéger son téléphone mobile ou sa tablette par un système de verrouillage (mot de passe, code PIN, schéma de déverrouillage).
- Ces équipements ne doivent pas être « débridés ».
- Les applications de confiance doivent être téléchargées à partir des plateformes officielles de téléchargement (Google Play Store, AppStore, plateformes internes de type Intranet applicatif).
- L'Utilisateur doit être le seul à utiliser son équipement si des données professionnelles sont stockées (messagerie, fichiers). Il lui est interdit de prêter ou de donner à un tiers son matériel.

- L'Utilisateur doit signaler au plus tôt à la DSIN, la casse, la perte ou le vol d'un terminal mobile contenant des données professionnelles ou y donnant accès. L'Utilisateur a par ailleurs l'obligation de porter plainte en cas de vol et de contacter l'opérateur téléphonique correspondant pour suspendre la ligne en cas de perte ou de vol (une grande vigilance est à observer quant au vol ou à la perte des équipements mobiles : notamment lors des déplacements).
- L'Utilisateur a l'obligation de prévenir la DSIN en cas de déplacement à l'étranger afin d'obtenir l'autorisation d'utiliser ses équipements mobiles dans le pays concerné.

## 10.2 Utilisation d'internet et filtrage

Le CDG 77 est fournisseur d'accès internet (FAI) lorsqu'il fournit un accès à internet quel que soit le biais (filaire ou wifi). La navigation sur internet s'effectue avec les adresses IP publiques du CDG 77, engageant ainsi la responsabilité de sa présidente en cas d'usage délictueux.

De ce fait, le CDG 77 est tenu au respect d'un certain nombre d'obligations parmi lesquelles :

- l'identification et la journalisation des informations de connexion et de navigation (durée, sites visités, téléchargements) ainsi que leur conservation sur une année ;
- le filtrage de la navigation, par le blocage de sites dont la consultation est illicite et punie par la loi ;
- le constat de toute utilisation illégale pourra donner lieu, après décision actée de l'autorité administrative ou judiciaire, à la suppression des accès et/ou à des sanctions disciplinaires ;

L'utilisation d'Internet doit se faire en respectant la réglementation en vigueur, les consignes de sécurité du réseau et les procédures définies le cas échéant à cette fin par le CDG 77.

Un usage exceptionnel dans le cadre de la nécessité de la vie courante est toléré pendant les heures de pause à condition que cette utilisation n'affecte ni les performances du système ni la bonne exécution des missions professionnelles. Cela inclut l'usage des réseaux sociaux et des forums de discussion.

Les informations enregistrées peuvent être examinées en réponse à une demande actée d'une autorité administrative ou judiciaire compétente.

le CDG 77 se réserve le droit de bloquer l'accès aux sites dont le contenu est jugé illégal, offensant ou sans rapport avec les missions de l'agent.



### Pour aller plus loin

Tout utilisateur se connectant sur des réseaux sociaux, blogs, ou forums, s'engage au respect de son obligation du secret professionnel. La présence des agents sur ces réseaux, blogs, ou forums, engage leur stricte responsabilité à titre privé, et ne saurait engager sur quelque motif que ce soit la responsabilité du CDG 77. Chaque agent, s'engage au respect de ses obligations déontologiques que sont la discrétion professionnelle, même dans un cadre d'usage privé. Ainsi :

- l'agent ne doit pas diffuser d'informations ou de documents dont il a connaissance dans le cadre de l'exercice de ses fonctions ;
- l'agent doit éviter toute manifestation de nature à dénigrer ou à porter atteinte à l'image du CDG 77.

Un agent doit être prudent quant à l'expression publique de ses opinions, qu'elles soient d'ordre politique, juridique ou religieux, même exprimées sous son seul nom, en particulier si les propos permettent de faire le lien avec l'employeur.

D'autre part, afin de prévenir l'accès à certains sites non autorisés en raison de leur caractère immoral, illicite, illégal (pornographie, pédophilie, racisme, incitation à la haine raciale, révisionnisme, etc.) ou sans utilité professionnelle, un dispositif de filtrage et de contrôle est mis en œuvre. Les données de connexion des utilisateurs de ce dispositif de contrôle seront conservées un an, conformément à la réglementation en vigueur. L'outil de filtrage ne dispense pas les utilisateurs d'une juste déontologie individuelle. Chaque utilisateur est seul responsable de la décision d'accéder à un site Internet. Le fait que l'accès à un site en particulier ne soit pas interdit ne signifie pas que l'accès à ce site est autorisé et conforme à la réglementation applicable. Si certains sites non accessibles s'avéraient présenter un intérêt professionnel, il convient d'avertir le service informatique sous couvert de la voie hiérarchique par écrit en fournissant tous les éléments d'étude nécessaires.

#### L'Utilisateur doit :

- consulter et utiliser les sites Internet, les forums de discussion ou autres outils de communication présentant un lien direct avec l'activité professionnelle ;
- faire preuve de vigilance vis-à-vis des informations en provenance d'Internet et de vérifier leur exactitude.

#### L'Utilisateur ne doit pas :

- accéder à des flux multimédias n'ayant pas de liens avec l'activité (streaming, webradios, etc.) ;
- consulter, télécharger ou propager des informations (textes, images, sons) à caractère illégal ; injurieux, harcelant, obscène, menaçant ou n'ayant aucun lien direct avec l'activité ;
- installer et participer à des jeux en ligne ;
- accéder à des contenus pouvant porter préjudice à la ~~sécurité du Système~~ d'Information du CDG 77 ;
- tenter de contourner le dispositif de filtrage.

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## 10.3 Utilisation du téléphone

Le CDG 77 met à disposition de tous les agents des moyens téléphoniques fixes adaptés à ses missions. Certains agents peuvent disposer de téléphones mobiles. Dans ce cadre chaque utilisateur est responsable du matériel qui lui est confié et de l'utilisation qui en est faite notamment en termes de consommation.

L'administration se réserve le droit d'effectuer des contrôles sur les consommations : il s'agit de contrôles globaux non nominatifs sur les téléphones fixes et de contrôles individualisés pour les consommations réalisées à partir des matériels de mobilité (6 premiers numéros des numéros appelés, numéros surtaxés dates, heures et durées des appels, nombre de sms).

En cas d'utilisation abusive, un relevé des consommations de téléphonie (type de numéro appelé, date, heure, durée) par utilisateur peut être édité, et communiqué au responsable hiérarchique qui donne un avis sur l'opportunité professionnelle des appels après explication de l'agent.

En cas d'abus constaté, la ligne pourra être suspendue ou le matériel mobile repris sur demande de la Directrice Générale des Services ou d'une personne faisant autorité avec une refacturation possible des communications abusives auprès de l'utilisateur concerné.



### Pour aller plus loin

La téléphonie présente également des risques en termes de sécurité (vol ou perte de téléphone portable, prise de contrôle de poste fixe sur IP, etc.). Il est obligatoire de configurer un code de verrouillage sur votre appareil.

## 11. PRÉCISIONS RELATIVES À L'APPLICATION DE LA CHARTE AUX DÉLÉGUÉS OU REPRÉSENTANTS DU PERSONNEL

Les représentants du personnel utilisent, dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l'exercice de leur activité professionnelle. Ils disposent d'une adresse électronique dédiée, ils doivent également disposer d'un répertoire dédié à leur activité.

Les délégués ou représentants syndicaux gèreront leur répertoire de manière autonome.

Les délégués ou représentants syndicaux devront dans leur communication au personnel du CDG 77 :

- veiller au respect des dispositions de la loi sur la liberté de la presse ;
- se limiter quant à l'objet de la communication à ce qui rentre dans le cadre de leurs attributions ;
- respecter les consignes du CDG 77 en termes de format, de taille, des messages ou de pages intranet.

Les délégués ou représentants du personnel ne pourront pas adresser de tracts par messagerie électronique.

Les délégués ou représentants du personnel établissent, sous leur seule responsabilité, des listes de diffusion avec l'accord préalable des agents concernés.

Ces derniers doivent à tout moment pouvoir en être radiés à leur demande. Les délégués ou représentants du personnel doivent à ce titre être respectueux de la législation informatique et libertés.

### Confidentialité des échanges

Le CDG 77 respecte la confidentialité des messages électroniques en provenance ou à destination des boîtes aux lettres des délégués ou représentants du personnel (contenu, auteurs et destinataires), du contenu des listes de diffusion élaborées par leurs soins et de l'identité des auteurs des messages.

Concernant l'envoi de mails aux agents, le référentiel RH de la CNIL dispose que le RGPD définit les destinataires comme « tout organisme qui reçoit la communication des données ».

Dans le domaine RH, peuvent notamment être destinataires « les instances représentatives du personnel, s'agissant des coordonnées professionnelles des employés après accord formalisé avec l'employeur **et recueil de l'accord express des intéressés**, et des données strictement nécessaires à la défense des intérêts des employés »

Il appartient donc aux délégués ou représentants du personnel de collecter l'accord des agents à qui elles souhaitent envoyer des mails.

## 12. UTILISATION DES SUPPORTS DE STOCKAGES EXTERNES

Les ports USB sont des sources d'infection potentielles du système d'information par le biais d'utilisation de supports de stockages externes (non contrôlés) infectés par des virus/programmes malveillants/rançongiciels.

Ainsi, il n'est pas recommandé d'utiliser des clefs USB, disques durs externes ou tout dispositif de stockage externe pour l'échange de fichiers. Le CDG 77 se réserve le droit de bloquer l'utilisation des ports USB en fonction du niveau de sécurité exigé par l'équipement concerné.

## 13. UTILISATION DES ÉQUIPEMENTS PERSONNELS (BOYD)

L'utilisation d'outils personnels (souvent désigné par BYOD pour « Bring Your Own Device ») n'intervient que de manière subsidiaire et exceptionnelle. Elle est subordonnée à une autorisation préalable la DSIN. Ce mode de travail n'est pas sans impact pour la sécurité du système d'information et engendre des risques tels que :

- la perte ou vol d'un équipement personnel contenant des données professionnelles ;
- un accès non autorisé à des données professionnelles par l'entourage du agent ;
- la dissémination de virus ou de programmes malveillants ;
- le risque d'intrusion frauduleuse dans le SI de l'administration ;
- le non-respect de la responsabilité civile du CDG 77 en tant que FAI (Fournisseur d'Accès à Internet).

Ainsi, ce mode de travail implique de la part de l'utilisateur le respect de toutes les règles de sécurité définies dans la présente charte et notamment, l'utilisateur prévoit le verrouillage du terminal avec un mot de passe répondant aux contraintes définies par la DSIN et l'utilisation d'un anti-virus à jour.

L'utilisation de terminaux personnels préalablement autorisée et déclarée auprès du Service Informatique n'entraînera pas l'application par le service informatique de mesures de sécurité entravant leur utilisation dans un cadre privé.

La panne ou la perte du terminal personnel oblige l'utilisateur à en informer immédiatement la DSIN puisque celui-ci contiendra potentiellement des données professionnelles.

Les connexions non explicitement autorisées de terminaux privés sur le réseau du CDG 77 sont strictement interdites.

En cas de nécessité d'effacement à distance par le service informatique, l'action portera uniquement sur les données professionnelles présentes sur le terminal de l'utilisateur.

Le CDG 77 ne pourra être tenu pour responsable des altérations voire des pertes d'informations à caractère privé survenues accidentellement lors de cette opération et ce malgré les précautions prises par le service informatique.

Dans tous les cas, les agents ne peuvent se prévaloir d'aucune indemnité, quelle qu'elle soit.

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## 14. ACCÈS À DISTANCE

Dans le cadre de l'ouverture des Systèmes d'Information, des services d'accès à distance à la messagerie ou à d'autres ressources du Système d'Information, les Utilisateurs peuvent être autorisés à utiliser leur matériel personnel (sous réserve de validation de la DSIN) ou professionnel pour accéder à distance aux Systèmes d'Information et se connecter à certaines ressources spécifiques.

Les services d'accès à distance sont restreints à certains usages. L'accès est soumis à une demande particulière qui sera validée par le supérieur hiérarchique, selon les règles en vigueur, puis adressée au service informatique. L'ensemble des règles décrites dans les articles précédents concernant l'utilisation des ressources restent applicables. Dans les cas d'utilisation des services d'accès à distance, afin de limiter le risque de divulgation d'information, des précautions particulières s'imposent :

- être particulièrement vigilant afin de ne pas divulguer d'information confidentielle lors d'une consultation à distance. (Regard indiscret d'un tiers, etc.) ;
- se déconnecter systématiquement et complètement du service d'accès à distance après utilisation ;
- protéger contre le vol les équipements mobiles et accessoires ;
- respecter les règles encadrant l'usage des équipements mobiles professionnels et personnels ;
- en tout état de cause, les Utilisateurs sont seuls responsables de la sécurité physique de leurs équipements personnels.

## 15. STOCKAGE DES DONNÉES

Dans le cas du stockage d'informations relatives à l'activité professionnelle des Utilisateurs, certaines règles sont à respecter. De manière générale, il n'est pas permis à l'Utilisateur d'utiliser des moyens de stockages externes au Système d'Information du CDG 77 (périphériques amovibles).

### **L'Utilisateur doit :**

- stocker les fichiers professionnels non partageables dans l'espace professionnel privé (dossier nominatif sur le serveur ou OneDrive) ;
- stocker les fichiers professionnels partageables dans les espaces de services ou sur les espaces de stockage cloud fourni par le CDG 77 (SharePoint, Teams, etc.) ;
- organiser et mettre en œuvre les moyens nécessaires à la conservation des données présentant un intérêt en matière de preuve, de suivi des dossiers ou d'archivage ;

### **Par ailleurs, l'Utilisateur de ne doit en aucun cas :**

- stocker des fichiers professionnels hors des espaces prévus par le service informatique ci-dessus mentionnés (bureau Windows, disques durs locaux, supports de stockage externe, cloud non autorisé). Le service informatique ne serait en aucun cas tenu responsable de la perte des fichiers (pas de sauvegarde).

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

- utiliser les dispositifs de stockage dans le nuage (Cloud) non autorisés. Sont concernées les solutions comme Dropbox, Google Drive, Hubic, Evernote, etc. Ces dispositifs sont non conformes aux règles de protection des données et ne sont pas autorisés par la DSIN ;
- utiliser des dispositifs de stockage de type FTP, sauf autorisation du Service Informatique.

## 16. MISE A DISPOSITION DES ÉQUIPEMENTS

Les ressources informatiques mises à disposition des Utilisateurs par le CDG 77 restent en tout temps propriété de celui-ci qui se réserve le droit de réclamer la restitution immédiate du matériel.

### En ce sens, l'Utilisateur doit :

- faire preuve de respect envers le matériel en tout temps en s'assurant par tous les moyens nécessaires de son entretien régulier, de son utilisation en accord avec les règles édictées dans ce document, de par le respect des notices d'utilisation ;
- retourner le matériel mis à disposition dès lors qu'il n'en a plus l'utilité, et ce dans les plus brefs délais.

### L'Utilisateur ne doit pas :

- utiliser le matériel mis à disposition dans des conditions ne respectant pas les règles émises dans ce document ou d'une manière pouvant causer des dommages au matériel ;
- prêter, vendre ou mettre à disposition d'un tiers le matériel professionnel. Toute dégradation volontaire ou manque d'attention vis-à-vis des équipements (laxisme) pourra se traduire par une sanction disciplinaire adaptée. Par ailleurs, en cas de dégradation involontaire répétée d'un équipement individuel, la mise à disposition de l'équipement concerné pourra être suspendue après avis du supérieur hiérarchique.

## 17. PROCÉDURES SPÉCIFIQUES AU MATÉRIELS DE PRÊT

Le CDG 77 met à disposition des agents du matériel de prêt comme des ordinateurs portables, des solutions de visioconférence, des vidéoprojecteurs, etc. L'utilisateur assure la garde et la responsabilité et doit informer le service informatique dès connaissance d'un risque sur le matériel et ses données (perte, vol, dégradation), afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont confiés et ne doit pas contourner la politique de sécurité mise en place sur ces derniers.

## 18. CAS PARTICULIER DE VOL OU DE PERTE DE MATÉRIEL

**L'agent ne doit pas stocker de documents professionnels sur le disque local du poste et en particulier sur les équipements mobiles susceptibles d'être égarés ou volés.**

Tout vol de matériel informatique doit être signalé immédiatement par l'agent à sa hiérarchie et au service informatique et doit faire l'objet d'un **dépôt de plainte à la police ou la gendarmerie dans les 24 heures suivant le constat des faits**. Le récépissé de plainte, qui est un document administratif obligatoire à conserver par le CDG 77, doit être adressé au Service de la Direction des Systèmes d'Information et du numérique, sans délai par l'utilisateur.

## 19. UTILISATION DES MOYENS D'IMPRESSION

L'impression de documents implique des risques de sécurité portant essentiellement sur leur confidentialité. Les règles suivantes permettent de réduire voire d'éliminer ces risques :

### Sur l'impression de vos documents :

- utiliser le mode « d'impression sécurisée » pour respecter la confidentialité des documents comportant des données à caractère personnel .

### Sur la numérisation des documents :

- il est recommandé de ne pas utiliser la fonctionnalité « numériser vers un courriel » pour un/ou plusieurs destinataire(s) à l'extérieur du CDG 77 ;
- préférer l'utilisation de la numérisation vers sa propre messagerie puis un envoi du document vers l'adresse électronique du destinataire à l'extérieur.

## 20. UTILISATION DE LA MESSAGERIE

Le CDG 77 met à disposition de chaque agent une boîte aux lettres électronique (BAL) ainsi qu'une adresse de messagerie électronique nominative.

### Chaque utilisateur est responsable :

- de l'utilisation de sa boîte aux lettres ; de même que l'est le gestionnaire (ou son suppléant) d'une boîte aux lettres d'unité (comme la boîte aux lettres de la direction par exemple) ;
- du contenu des messages envoyés sous son timbre.



#### **Pour aller plus loin**

La boîte aux lettres électronique relève du secret de la correspondance en ce qui concerne les messages dits « Personnel » ou « Privé » (Art 226-15 du nouveau code pénal).

L'adresse de messagerie qui a été remise à chaque agent demeure à usage professionnel exclusivement et ne doit être communiquée ou utilisée sur des sites sans rapport avec les missions de l'agent (mailings et différents services privés, etc.).

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

Un usage raisonnable dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique soit conforme aux dispositions de la présente charte et au droit informatique, qu'elle n'affecte pas le trafic normal des messages professionnels et qu'elle ne gêne en rien les activités du CDG 77.



#### Pour aller plus loin

Un message est considéré comme personnel dès lors qu'il contient dans son objet la mention « Personnel » ou « Privé ».

L'utilisation de la messagerie électronique est destinée principalement aux activités professionnelles, les messages professionnels sont soumis aux règles des écrits professionnels.

#### Avant de diffuser un message, l'utilisateur doit s'assurer que ce dernier :

- ne porte pas atteinte aux droits et à la dignité des agents du CDG 77 ;
- ne permet pas la propagation de virus.

#### Dans le cadre de l'usage de la messagerie professionnelle, l'Utilisateur doit :

- respecter les conseils et consignes indiquées pour structurer et organiser la gestion de sa messagerie ;
- signaler toute erreur ou correction à effectuer vis-à-vis de la constitution des groupes de distribution par défaut du CDG 77 ;
- respecter les consignes préconisées d'archivage, de conservation et de classement des courriers émis et reçus. Ces consignes doivent particulièrement être respectées dans le cas de messages présentant un intérêt en matière de preuve et de suivi des dossiers traités, d'autre part l'Utilisateur s'engage à respecter la taille allouée par le service informatique à sa messagerie ;
- activer le gestionnaire d'absence lorsqu'il est absent.

#### D'autre part, l'Utilisateur ne doit pas :

- ouvrir des messages dont l'origine, l'objet ou le contenu est douteux, ou exécuter les pièces jointes suspectes. En cas de réception d'un tel message, il avertit le service informatique et ne prend pas d'initiative sans la validation de celui-ci ;
- mettre en œuvre une redirection automatique ou réplique de messages vers une adresse électronique externe et notamment : **le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est interdit ;**
- utiliser la messagerie d'autrui sans l'autorisation expresse de la personne concernée et sans que la situation ne la réclame ;
- envoyer de messages à l'ensemble du personnel du CDG 77 (sauf autorisation de la hiérarchie) ou envoyer des messages en nombre ;
- relayer des chaînes ou tout canular, information non vérifiée ;
- promouvoir des événements n'ayant aucun lien avec l'activité du CDG 77 ;
- utiliser la messagerie afin de partager des annonces « commerciales » privées.

Accusé de réception en préfecture  
077-287709325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

Un système de filtrage des courriers électroniques non désirables est actif sur le Système Informatique. Lorsqu'un courrier électronique est identifié par le système comme étant non désirable car dangereux pour le système (adresse de l'expéditeur suspecte, contenu du message, etc.) : il est identifié comme tel et n'est pas transmis à son destinataire.

## Sur le traitement des messages

- Toute demande issue de particulier, d'entreprise, d'association ou autre organisme, émanant de personnes dûment identifiées (par un nom et une adresse postale) appelle une réponse des services du CDG 77.
- Le courrier électronique est une véritable correspondance qui doit être traité avec autant de rigueur qu'une lettre.
- Tout comme un courrier papier, le contenu des messages envoyés sous le timbre d'un utilisateur doit respecter les règles hiérarchiques et d'organisation des pouvoirs internes, notamment pour les délégations de signatures et les engagements pris au titre du CDG 77.
- Tout courrier électronique engageant le CDG 77 doit respecter les règles formelles de validation en vigueur. L'utilisateur a une obligation générale et permanente de confidentialité et de discrétion à l'égard des informations et documents électroniques disponibles sur le réseau interne. Ceci implique de s'assurer auprès de sa hiérarchie du niveau de confidentialité des documents avant de les diffuser.
- L'utilisateur doit être attentif aux destinataires des messages :
  - > en destinataire les personnes pour action (Dest) ;
  - > en copie les personnes pour information (CC).
- Le champ « copie cachée » (Cci:) est réservé à la protection de la vie privée (réglementation RGPD) des destinataires lorsqu'on ne désire pas divulguer leur adresse de messagerie. En dehors de ce cas de figure, l'utilisation du champ Cci est à utiliser avec parcimonie.
- L'utilisateur doit éviter l'envoi de copies (Cc: ou Cci:) à un nombre injustifié de destinataires.
- L'utilisation de la fonction « répondre à tous » ne doit pas être systématique pour ne pas encombrer les boîtes aux lettres des destinataires.
- Tout courrier électronique doit disposer d'un titre explicite.
- Tout courrier électronique doit indiquer les nom, prénom, fonctions et coordonnées de la personne en charge du dossier.
- Un message transféré d'un destinataire à un autre ne doit en aucun cas être modifié, par ailleurs, l'origine et la date du message doit être conservée.
- L'utilisateur doit utiliser les moyens de sécurisation des envois mis à disposition par le CDG 77 lors de l'envoi de données à caractère personnel sensibles.
- La loi interdit le stockage et la diffusion de messages ou documents de nature diffamatoire, discriminatoire, pédophile, incitant à la violence ou à la haine raciale. Toute réception de message de cette nature doit être signalé immédiatement à la hiérarchie et au Service Informatique.

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## Sur les potentielles escroqueries

Chaque utilisateur doit être vigilant face aux escroqueries potentielles qui se propagent par message électronique ou via des sites internet et suivre les consignes de sécurité, en particulier :

- ne pas ouvrir de documents ou cliquer sur un lien dont l'origine est inconnue ;
- ne jamais répondre à une demande d'informations personnelles par courriel quel qu'en soit l'expéditeur ;
- ne jamais communiquer de données sensibles (numéro de carte bancaire, mot de passe, numéro de sécurité sociale etc.).

Signaler immédiatement tout message suspect au Service Informatique.

## 21. MESSAGES : MODALITÉS D'ARCHIVAGE ET DE DESTRUCTION DES MESSAGES

Il convient de distinguer les nécessités d'archivage des messages au titre de la gestion de la capacité de stockage des boîtes de messagerie électronique, des nécessités de conservation des données telles que résultant des besoins des services et des obligations légales applicables en matière de conservation des archives.

Ainsi, il appartient au CDG 77 (et aux services concernés) de déterminer la durée à l'issue de laquelle d'anciens messages seront automatiquement archivés pour accorder la place nécessaire à la réception et à la conservation des messages plus récents.

En outre chaque service doit définir la durée de conservation des différents messages au regard des « nécessités de service » (la boîte de messagerie n'étant qu'un « réceptacle » d'informations pouvant se rattacher à différents traitements de données), que cette conservation intervienne en « base active » (donnée d'utilisation courante) ou dans le cadre d'un « archivage intermédiaire » (données présentant encore un intérêt administratif et conservées de façon « isolée » jusqu'à l'expiration de la durée d'utilité administrative).

## 22. DÉLÉGATION DE LA BOÎTE MAIL

Si la boîte mail est considérée comme professionnelle, les messages privés doivent impérativement être marqués « PERSONNEL » ou « PRIVE » si tel est le cas. En tout état de cause concernant la continuité de service, et en cas d'absence d'un agent, celui-ci peut déléguer sa boîte mail.

L'agent donne délégation à une ou plusieurs personnes, en choisissant la personne la plus adaptée de son point de vue sur les personnes pouvant prendre le relai sur son métier.

La délégation est donnée par l'agent pour une période limitée (pendant le temps d'absence) et non de manière illimitée.



### Pour aller plus loin

Il est contre-productif de donner délégation à plusieurs personnes, cela n'est pas effectif ni efficient. Un risque de non prise en charge des dossiers pouvant apparaître, tout le monde pouvant penser que l'autre s'en occupe

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## 23. DÉPART D'UN AGENT

En cas de départ d'un agent (démission, mutation, retraite, fin de contrat, etc.), ses autorisations seront retirées immédiatement par le CDG 77. Toute autorisation (compte, l'adresse électronique nominative et l'ensemble des accès aux systèmes, réseaux (dossiers partagés) et applications ou progiciels) prend fin lors de la cessation, même provisoire, de l'activité professionnelle.

Une fois le départ du agent devenu définitif, aucun document professionnel en possession de l'agent ne doit-être détruit par ce dernier. Toute copie de documents professionnels doit être préalablement autorisée par le supérieur hiérarchique.

Le agent devra supprimer toute donnée privée ou personnelle sur tout support (poste de travail, tablette, téléphone, supports amovibles, etc.), y compris sur sa messagerie avant de rendre son matériel au service DSIN.

Un accès aux données restantes pourra alors être consenti au responsable direct ou successeur de l'ancien utilisateur.

Lors de son départ, l'utilisateur doit remettre l'ensemble des moyens informatiques et de communication mis à sa disposition pour l'exercice de son activité professionnelle au service informatique du CDG 77. C'est avant le départ de l'agent, que son supérieur hiérarchique doit se préoccuper de la récupération des éventuelles données professionnelles que l'utilisateur est le seul à détenir. Ceci afin de pouvoir évaluer la pertinence de ce qui doit être récupéré et de ce qui peut être détruit.

## 24. CAS DE L'ABSENCE OU DE L'ABSENCE PROLONGÉE DE L'AGENT

Lorsque l'absence est prévue, l'agent peut utiliser le gestionnaire d'absence du bureau. Cette fonctionnalité de la messagerie permet une réponse automatique aux expéditeurs, notamment lorsque la continuité de service s'impose.

Il appartient à chaque agent de régler le gestionnaire d'absence du bureau de sa propre boîte aux lettres ou d'une boîte aux lettres sur laquelle il a délégation, avant toute période d'absence, et de s'assurer qu'il est bien désactivé à son retour.

De manière générale, les informations mises dans les mails envoyés par le gestionnaire d'absence sont :

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

En cas d'absence prolongée d'un agent et de l'incapacité à le joindre, et pour des raisons de continuité de service, les dossiers et mails professionnels pourront être consultés, l'agent étant censé avoir préalablement identifié les données « PERSONNELLES » ou « PRIVÉES » tel que précisé dans la présente charte.

Cette autorisation de consultation ponctuelle du poste de l'agent ou de l'espace de travail fera l'objet d'une demande de la hiérarchie de l'agent concerné auprès de la Direction Générale du CDG 77. A son retour, l'utilisateur sera informé de cette intervention par un message de la DRH.

En cas d'absence prolongée d'un agent (longue maladie), le responsable de service peut demander au service informatique, après accord de son directeur, le transfert des messages reçus.

Concernant les mails consultés : le supérieur hiérarchique n'aura pas accès aux autres messages de l'agent. L'agent concerné sera informé dès que possible de la liste des messages qui auront été transférés/consultés.



### Pour aller plus loin

**En cas de départ ou d'absence** prolongée prévue, chaque utilisateur prend, dans la mesure du possible et si nécessaire, les précautions propres à ce que la poursuite de l'activité puisse être assurée. Pour cela, il doit :

- privilégier le dépôt des fichiers de travail sur l'espace partagé, sur les serveurs du CDG 77 par les membres de son équipe ;
- informer sa hiérarchie des modalités d'accès aux ressources mises à sa disposition, étant ici rappelé que les données non situées dans un espace identifié comme « privé » ou « personnel », sont présumées être professionnelles ;
- informer ses interlocuteurs de son absence, en utilisant les fonctions de notification d'absence de la messagerie électronique.

Au moment de son départ et sous la responsabilité de son supérieur hiérarchique, l'agent peut signer une FICHE « DEPART AGENT », qui précise notamment que :  
«L'agent reconnaît avoir supprimé ses données à caractère personnel sur les matériels informatiques à remettre».

Et qui rappelle que

«Conformément à la charte informatique en vigueur au Centre de gestion de Seine-et-Marne, vous devez remettre à votre supérieur hiérarchique, les données informatiques à caractère professionnel présentes sur votre ordinateur et rédiger le message d'absence dans votre boîte à lettres professionnelle indiquant les coordonnées d'un contact au sein du CDG 77 (à défaut indiquer les coordonnées de votre supérieur hiérarchique) ».

## 25. CAS PARTICULIER DU DÉCÈS D'UN AGENT

En cas de décès d'un agent, les ayants-droit n'auront pas accès aux dossiers et mails y compris ceux dont le titre est « personnel » ou « privé » conformément à la réglementation en vigueur. En cas de demande écrite des ayant-droit, une réponse leur sera adressée le CDG 77 en fonction de la situation.

## 26. GESTION DES SPAMS

Le CDG 77 dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

## 27. RÈGLES DE SÉCURITÉ

Tout utilisateur est responsable de l'usage des informations, des ressources informatiques et des services internet auxquels il a accès. Il a aussi la responsabilité, à son niveau, de contribuer à la sécurité générale et aussi à celle de son service ou de sa direction. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

Il doit appliquer les mesures de sécurité du service ou de la Direction auquel il appartient et suivre les recommandations de la Politique de Sécurité des Systèmes d'Information du CDG 77.

Il doit signaler toute tentative de violation de son compte et, de façon générale toute anomalie ou irrespect de la politique de sécurité des systèmes d'information du CDG 77 qu'il peut constater.

Il doit suivre les règles en vigueur pour toute installation de logiciel. Ainsi, toute installation de logiciels supplémentaires est subordonnée à l'accord du service informatique du CDG 77.

Chaque utilisateur est responsable du bon usage de son identifiant, du mot de passe et des droits d'accès. Chaque utilisateur choisit des mots de passe conformément aux règles édictées par le CDG 77, ceux-ci sont conservés secrets selon les procédures en vigueur, en aucun cas ils ne doivent être communiqués à des tiers.

Les données et documents doivent être classés sur les arborescences bureautiques réseaux afin que ceux-ci soient sauvegardés régulièrement.

Il est interdit d'utiliser ou d'essayer d'utiliser des accès autres que les siens.

Chaque utilisateur a interdiction de masquer sa véritable identité, ou d'effacer ou modifier les données permettant la traçabilité de ses actions (logs d'application, enregistrements de base de données, systèmes d'horodatage).

Chaque utilisateur s'interdit de mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels, logiciels, accès dont il a l'usage.

## 28. DROIT À LA DÉCONNEXION

**Le droit à la déconnexion** peut être défini comme le droit de l'agent de ne pas être connecté aux outils numériques professionnels et ne pas être contacté, y compris sur ses outils de communication personnels, pour un motif professionnel en dehors de son temps de travail habituel.

### **Les outils numériques visés sont :**

- les outils numériques physiques : ordinateurs, tablettes, téléphones portables, réseaux filaires, etc. ;
- les outils numériques dématérialisés permettant d'être joint à distance : messagerie électronique, logiciels, connexion wifi, internet/intranet, etc.

Le temps de travail habituel correspond aux horaires de travail de l'agent durant lesquels il demeure à la disposition du CDG 77.

Ce temps comprend les heures normales de travail de l'agent et les éventuelles heures supplémentaires. En sont exclus les temps de repos quotidien et hebdomadaire, les temps de congés payés et autres congés exceptionnels ou non, les temps de jours fériés et de jours de repos, les temps d'absences autorisées, de quelque nature que ce soit (absence pour maladie, pour maternité, etc.).

### **Mesures visant à lutter contre l'utilisation des outils numériques et de communication professionnels hors temps de travail et mesures favorisant la communication.**

Aucun agent n'est tenu de répondre à des courriels, messages ou appels téléphoniques à caractère professionnel en dehors de ses heures habituelles de travail, pendant ses congés payés, ses temps de repos et ses absences, quelle qu'en soit la nature.

### **Afin d'éviter la surcharge informationnelle, il est recommandé à tous les agents de :**

- s'interroger sur le moment opportun pour adresser un courriel, un message ou joindre un collaborateur par téléphone ;
- ne pas solliciter de réponse immédiate si ce n'est pas nécessaire ;
- utiliser avec modération les fonctions « CC » ou « Cci » ;
- indiquer un objet précis permettant au destinataire d'identifier immédiatement le contenu du courriel ;
- privilégier les envois différés lors de la rédaction d'un courriel en dehors des horaires de travail ;
- pour les absences de moins de 5 jours, paramétrer le gestionnaire d'absence du bureau sur sa messagerie électronique et indiquer les modalités de contact d'un membre du CDG 77 en cas d'urgence ;
- pour les absences de plus de 5 jours, prévoir le transfert de ses courriels, de ses messages et de ses appels téléphoniques à un autre membre du CDG 77, avec son consentement exprès.

## Importance du respect du temps de travail

L'employeur doit s'assurer régulièrement par le biais des entretiens obligatoires notamment, que la charge de travail de l'agent est raisonnable et permet une bonne répartition dans le temps de son travail.

Il est rappelé l'obligation pour tous les agents quel que soit leur régime de travail, de respecter les durées maximales journalières de travail. Une amplitude horaire trop importante par jour ou par semaine peut cacher différents problèmes et potentiellement découler sur des situations d'atteinte à la santé de l'agent.

Afin de laisser le choix à tout un chacun d'organiser en toute autonomie la gestion de son temps pour répondre à sa mission professionnelle tout en conciliant sa vie personnelle, il a été convenu de ne pas opter pour une solution qui consisterait de bloquer les accès sur une période donnée. Par conséquent les accès resteront libres, toutefois chaque personne devra veiller à sa sécurité et à sa santé en respectant les durées de repos quotidiennes et hebdomadaires.

## Droit à la déconnexion en dehors du temps de travail effectif

Les périodes de repos, congé et suspension du contrat de travail doivent être respectées par l'ensemble des agents du CDG 77.

Sauf urgence avérée, les responsables hiérarchiques ne peuvent pas contacter leurs collaborateurs en dehors de leurs horaires de travail telles que définies au contrat de travail ou par l'horaire collectif applicable.

Concernant plus particulièrement l'usage de la messagerie électronique professionnelle, les agents ne sont pas tenus de prendre connaissance des courriels qui leurs sont adressés ou d'y répondre en dehors de leurs temps de travail.

Il en est de même des appels ou messages téléphoniques professionnels reçus pendant les temps de repos ou de congé. Toute dérogation doit être justifiée par la gravité, l'urgence et/ou l'importance du sujet en cause.

## Actions menées par le CDG 77

Pour s'assurer du respect du droit à la déconnexion et des mesures et recommandations prévues par le présent accord, le CDG 77 organisera des actions d'information et de sensibilisation à destination de l'ensemble du personnel. Ces actions d'information et de sensibilisation auront pour objectif d'aider les collaborateurs à avoir un usage raisonnable des outils numériques.

La Direction réaffirme le principe que toute personne qui pourrait rencontrer des difficultés à honorer sa mission en respectant ce droit à la déconnexion pourra demander un entretien avec son responsable hiérarchique et/ou avec la Directrice des Ressources Humaines afin de trouver une solution de rééquilibrage raisonnable de la charge de travail. Un accompagnement sur une meilleure gestion du temps et des priorités pourra être envisagé.

Si les mesures de suivi font apparaître des risques pour la santé des agents ou des difficultés, le CDG 77 s'engage à mettre en œuvre toutes les actions préventives et/ou correctives propres à faire cesser ce risque et lever ces difficultés.

## Révision de la charte

Les dispositions de la présente charte seront négociées et révisées au moins une fois par an.

Accusé de réception en préfecture  
077-28778623-20220930-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## 29. SANCTIONS

Dans le cas où un utilisateur contreviendrait à la présente charte, sa responsabilité pourrait être engagée, et le CDG 77 pourrait décider de mesures disciplinaires. Ces mesures internes pourraient être associées à des poursuites devant les juridictions judiciaires ou administratives dans le respect de la législation applicable.

## 30. RÉGLEMENTATION APPLICABLE

La charte informatique s'appuie sur la législation nationale et européenne et est également conforme aux différentes recommandations de la Commission Nationale Informatique et Libertés (CNIL). L'ensemble des articles ci-dessous sont accessibles sur [legifrance.gouv.fr](https://www.legifrance.gouv.fr) (choisir les codes en vigueur, et taper le numéro de l'article).

- Code civil : Article 9 du code civil : préservation de la vie privée et de l'image des salariés. « Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé ».
- Code du travail : Article L.120-2 du code du travail : principe de proportionnalité.
- Code du travail : Article L. 2142-6 du code du travail relatif à l'utilisation des technologies de l'information et de la communication par les instances représentatives du personnel et des syndicats.
- Code pénal : la législation relative au secret des correspondances (articles 226-15 et 432-9 du code pénal),
  - Dispositions Pénales :
    - o Code Pénal (partie législative) : articles 226-16 à 226-24,
    - o Code Pénal (partie réglementaire) : articles R. 625-10 à R. 625-13,
  - Dispositions pénales : articles 323-1 à 323-3 du Code pénal,
  - Disposition pénale : article L.335-2 du Code pénal.
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée ([cnil.fr](https://www.cnil.fr)).
- Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. (articles 323-1 à 323-7 du Code pénal - Livre III - Titre II - Chapitre III), ([legifrance.gouv.fr](https://www.legifrance.gouv.fr) - Choisir «Les Codes» Puis «Code Pénal - Partie législative»).
- Loi n° 94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels ([legifrance.gouv.fr](https://www.legifrance.gouv.fr) - Choisir «Les Codes» Puis «Code de la propriété intellectuelle - Partie législative»).
- Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.
- Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (« LCEN »).
- Loi du 04/08/1994 relative à l'emploi de la langue française, ([dglf/](https://www.dglf.fr)).

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

## La législation applicable en matière de cryptologie ([cf. ssi.gouv.fr](http://cf.ssi.gouv.fr))

- Règlement européen de protection des données (« RGPD ») du 27 avril 2016 ([eur-lex.europa.eu](http://eur-lex.europa.eu)).
- Règlement (UE) N°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (« eIDAS ») du 23 juillet 2014 ([eur-lex.europa.eu](http://eur-lex.europa.eu)).
- Législation applicable en matière de sécurité de l'information [ssi.gouv.fr](http://ssi.gouv.fr).

## La jurisprudence, notamment

- [Cour de cassation du 17 juin 2009](#) : les moyens de contrôle informatiques ne peuvent être présentés comme moyen de preuve.
- [Cour de cassation du 14 avril 2010](#) : des contenus pornographiques ne peuvent être source de licenciement.
- [L'affaire NIKKON](#) : « le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».
- [Cour de Cassation du 19 mai 2004](#) : il est possible de contrôler l'activité de ses salariés, notamment de leur mail, mais pas d'en lire les contenus.
- [Cour de Cassation du 2 juin 2004](#) : les contenus à caractère diffamatoire, antisémite ou injurieux peuvent être source de licenciement.
- [Cour de cassation arrêt du 6 juin 2007](#) : un employeur peut prendre connaissance des mails de ses salariés considérés comme professionnels, sous certaines conditions.
- [Décision du 15 octobre 2003 sur le principe de laïcité des fonctionnaires appliqué au courrier électronique](#) : il n'est pas possible d'utiliser son adresse professionnelle dans le cadre d'activité remettant en cause certains principes républicains.
- Décision du 28 décembre 2001 sur la recevabilité de réclamation par courrier électronique : un recours est valable quel que soit son support.
- Décision du 7 juin 2017 du Conseil d'État (10ème – 9ème ch.) sur l'accès aux données des personnes décédées par un ayant droit.
- Cour de cassation, arrêt du 3 novembre 2016, concernant la reconnaissance de l'adresse IP comme une donnée à caractère personnel.
- CEDH, arrêt du 5 septembre 2017 : les conditions d'une surveillance des messages personnels des salariés.
- TGI de Marseille, 6ème ch. corr., jugement du 7 juin 2017, traitement de données sans autorisation de la CNIL.

## Zoom sur les textes applicables au devoir de filtrer les connexions internet

- **Lois dites Hadopi**, la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet précise ainsi que la Haute Autorité, dite l'HADOPI « évalue, en outre, les expérimentations conduites dans le domaine des technologies de reconnaissance des contenus et de filtrage par les concepteurs de ces technologies la matière, notamment pour ce qui regarde l'efficacité de telles technologies, dans son rapport annuel prévu à l'article L. 331-14 ».
- **L'arrêté du 27 juin 1989**, dont l'article annexe II définit notamment le filtrage comme « mise en correspondance de formes selon un ensemble, prédéfini de règles ou de critères ».
- **L'article 6 I. – 1° de la loi n° 2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique (« LCEN ») retient la formule suivante « moyens techniques permettant de restreindre l'accès à certains services de communication au public en ligne ou d'opérer une sélection de ces services ».
- Les articles L.331-25 ; L.331-26 ; L.331-27 ; L.335-7-1 et R.331-4 du **Code de la propriété intellectuelle** utilisent les termes « moyens de sécurisation » ;
- **L'article L.336-2 du Code de la propriété intellectuelle** vise : « toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin » ;
- **Le décret n° 2010-1630 du 23 décembre 2010 relatif à la procédure d'évaluation et de labellisation des moyens de sécurisation** destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne.
- **L'article 4 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure** vient modifier l'article 6 I.- 7° : « Lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai. ».
- **L'article 61 de la loi n° 2010-476 du 12 mai 2010 relative à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne** :
  - « l'arrêt de l'accès à ce service aux personnes mentionnées au 2 du I et, le cas échéant, au 1 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. ».
  - « toute mesure destinée à faire cesser le référencement du site d'un opérateur mentionné au deuxième alinéa du présent article par un moteur de recherche ou un annuaire. ».
- L'article L.34-1 du Code des postes et des communications électroniques dispose que : « Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris aux opérateurs de communications électroniques en vertu du présent article. ».

Accusé de réception en préfecture  
071570343-12-2022-03231E  
Date de télétransmission : 28/09/2022  
Date de publication : 29/09/2022

- **L'article L.34-1 du Code des postes et des communications électroniques** dispose que : « Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. ».
- **L'article L. 336-3 alinéa 1, de la loi dite HADOPI**, dispose que : « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. ».
- **L'article L2242-8 du Code du travail modifié par la loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels** dispose que « Les modalités du plein exercice par le salarié de son droit à la déconnexion et la mise en place par l'entreprise de dispositifs de régulation de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos et de congé ainsi que de la vie personnelle et familiale. A défaut d'accord, l'employeur élabore une charte, après avis du comité d'entreprise ou, à défaut, des délégués du personnel. Cette charte définit ces modalités de l'exercice du droit à la déconnexion et prévoit en outre la mise en œuvre, à destination des salariés et du personnel d'encadrement et de direction, d'actions de formation et de sensibilisation à un usage raisonnable des outils numériques. ».

## Zoom sur le secret des correspondances

- **1°- Article 226-15 du code pénal modifié par la loi N°2013-1168 du 18 décembre 2013** dispose : le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions.
- **1°bis- Article 226-18** Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
- **Tribunal de Grande Instance de Paris 17ème chambre, chambre de la presse, 2 novembre 2000** rappelle les dispositions de l'article 433-9 du code pénal « toutes relations par écrit entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis fermés ou ouverts constitue une correspondance couverte par le secret.»
- **Cass. Soc, 5 juillet 2011, pourvoi N° 10-17.284 : L'employeur peut toujours consulter les fichiers qui n'ont pas été identifiés comme personnels par le salarié, il ne peut les utiliser pour le sanctionner s'ils s'avèrent être de sa vie privée.**

Accusé de réception en préfecture  
N° 2022-09222-33-E  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022

# NOM ET PRÉNOM DE L'AGENTF,

.....

Fait à Lieusaint, le ..... / ..... / 2022.

Fait en deux exemplaires

Signature

Accusé de réception en préfecture  
077-287708325-20220923-22-33-DE  
Date de télétransmission : 28/09/2022  
Date de réception préfecture : 28/09/2022