

CHARTRE INFORMATIQUE

La présente charte définit les conditions d'accès et les règles d'utilisation des ressources et des systèmes d'information et de communication, pour un usage loyal et responsable, qui ne mette pas en cause la sécurité de ces ressources et systèmes.

L'utilisation de ces ressources doit être exclusivement professionnelle, sauf exceptions prévues par la présente charte.

Ces ressources font partie de l'entreprise. A cet égard, toute information émise, reçue ou stockée sur le poste de travail ainsi que les moyens de communication mis à disposition du personnel sont et demeurent la propriété de CG2J.

Chaque utilisateur doit être conscient que, d'une part, l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi ainsi que dans le respect de la sécurité de l'entreprise et du bon usage des ressources, gage d'efficacité opérationnelle, et que, d'autre part, sa négligence ou la mauvaise utilisation des ressources fait courir des risques à l'ensemble de la société, et donc à lui-même.

Nous vous informons que le DPO est Mme DI PASQUALE Aurélie, vous pouvez le contacter à l'adresse mail : a.dipasquale@adp-qualite.com

Article 1 : Champ d'application

Les règles et obligations définies par la présente charte s'appliquent à l'ensemble des utilisateurs des ressources et systèmes d'information et de communication du cabinet ainsi que des ressources extérieures accessibles via les réseaux informatiques, notamment Internet.

Est considéré « utilisateurs » toute personne ayant accès aux données, ressources et système d'information et de communication de la Collectivité quel que soit son statut, le lieu et les moyens utilisés : agents, stagiaires, intérimaires, personnels extérieurs, consultants, partenaires, prestataires etc.

Les ressources et systèmes d'information et de communication de la société regroupent :

- ✓ Les équipements informatiques : ensemble des ordinateurs, fixes ou portable, matériel informatique, connectique ou bureautique, serveurs, hubs, switches, câbles du réseau, photocopieurs, fax etc.
- ✓ Les logiciels
- ✓ Les moyens de communication : messageries, téléphones, réseaux sociaux, accès internet, accès intranet, Smartphones, tablettes, etc.

➤ **Le non-respect des règles et mesures de sécurité figurant dans la présente charte engage la responsabilité personnelle de l'utilisateur dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables et l'expose éventuellement et de manière appropriée et proportionnée au manquement commis, aux sanctions disciplinaires définies par le Règlement intérieur.**

Article 2 : Règles générales d'utilisation, de sécurité et de bon usage

L'agent est responsable de l'usage qu'il fait des ressources de la Collectivité dans l'exercice de ses fonctions au sein de celui-ci.

L'usage de ces ressources doit être limité au cadre de l'activité professionnelle

L'agent ne doit se livrer, en aucune circonstance, à l'une des activités suivantes : charger, stocker, publier, diffuser ou distribuer, au moyen des ressources de la Collectivité, des documents, informations, images ou vidéos à des fins personnels, politiques, syndicales ou religieuses ou qui pourraient porter atteinte à l'image ou aux ressources de la Collectivité et de ses clients et plus particulièrement à l'intégrité et à la conservation des données de celle-ci

L'utilisateur s'interdit par ailleurs :

- ✓ D'utiliser les ressources de la Collectivité à des fins de harcèlement, menace ou injure et de manière générale de violer les droits en vigueur ;
- ✓ De charger ou transmettre, sciemment, des fichiers contenant des virus ou des données altérées ;
- ✓ De falsifier la source d'éléments contenus dans un fichier ;
- ✓ D'utiliser les ressources de la Collectivité de manière à gêner l'accès des autres utilisateurs.

Il est interdit d'accéder à des serveurs Web traitant de ces sujets avec le risque de voir l'adresse e-mail de l'utilisateur reprise par courrier de masse comportant des pièces jointes illicites.

Si l'utilisateur est amené à recevoir, à son insu, de tels éléments, il est tenu de les détruire aussitôt.

D'une façon générale, l'agent doit :

- ✓ assurer la protection de ses informations et sauvegarder ses données en utilisant les différents moyens préconisés par la direction et suivant les recommandations données par ce dernier ;
- ✓ signaler à la direction et au DPO toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
- ✓ pour toute installation de logiciel, veiller à demander l'autorisation à la direction
- ✓ mettre en œuvre les mesures de sauvegardes définies par CG2J ;
- ✓ s'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux, que ce soit par des manipulations anormales du matériel, la suppression de logiciels, le changement de paramètres ou par l'introduction de logiciels ou de fichiers personnels non autorisés par la direction ;
- ✓ ne pas installer, copier, modifier, détruire des logiciels sans autorisation ; renseigner le mot de passe lorsqu'il lui est demandé ;
- ✓ veiller à la confidentialité des codes, mots de passe et clés qui lui sont confiés et notamment à ne jamais prêter son identifiant ou mot de passe.

Accusé de réception en préfecture
58301555-20260202-2026_003-DE
Date de réception préfecture : 10/02/2026

- ✓ veiller à la confidentialité des informations et données auxquels il a accès en utilisant les outils mis sa disposition par la direction et protéger spécifiquement ses fichiers confidentiels ;
- ✓ verrouiller son ordinateur dès qu'il quitte son poste de travail ;
- ✓ utiliser un antivirus sur tout document de provenance externe au service ;
- ✓ ne jamais désactiver l'antivirus installé sur les postes, ni introduire de fichiers provenant de l'extérieurs sans contrôle préalable à l'aide de l'antivirus.

Règles de bon usage des mots de passe

Selon les recommandations de la CNIL, il est recommandé un mot de passe de douze caractères ou plus qui doit contenir au moins :

- ✓ Un nombre
- ✓ Une majuscule
- ✓ Un signe de ponctuation ou un caractère spécial (dollar, dièse, ...)

Le mot de passe doit être renouvelé tous les 6 mois

Rappels :

- Ne pas préenregistrer leurs mots de passe dans les navigateurs, notamment lors de l'utilisation ou la connexion à un ordinateur public ou partagé (salons, déplacements)
- Ne pas conserver les mots de passe dans des fichiers ou sur des post-it ;

Ressources informatiques personnelles

Les ressources informatiques personnelles (ordinateurs, smartphones, tablettes, etc. achetés sur des crédits personnels), lorsqu'elles sont utilisées pour accéder aux serveurs du cabinet, ne doivent pas remettre en cause ou affaiblir, les politiques de sécurité en vigueur par une protection insuffisante ou une utilisation inappropriée.

Lorsque ces ressources informatiques personnelles sont utilisées pour accéder, à distance ou à partir du réseau local aux serveurs informatiques ou stocker des données professionnelles, ces ressources sont autorisées et sécurisées suivant les directives issues de l'entreprise et à la direction.

Les agents qui souhaiteraient faire l'acquisition de tels matériels prennent préalablement conseil auprès de la direction

Départ de l'agent

L'utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ. En cas de circonstances exceptionnelles (départ impromptu ou décès) CG2J ne conserve les espaces de données à caractère privé présents sur les ressources informatiques que pour une période de 3 mois maximum (délai permettant à l'utilisateur ou ses ayants droits de récupérer les informations qui s'y trouvent).

Les données professionnelles restent à la disposition de l'employeur

Accusé de réception en préfecture
083-258301555-20260202-2026_003-DE
Date de réception préfecture : 10/02/2026

Article 3 : Respect de la législation concernant la propriété intellectuelle

L'utilisation de moyens informatiques et de communication électronique de la société implique le respect des droits de propriété intellectuelle.

L'utilisation de logiciels informatiques au sein de l'entreprise est ainsi soumise à l'obtention de licences d'utilisation accordées par des entreprises extérieures. CG2J n'est pas propriétaire des droits de ces logiciels ou de la documentation et, sauf autorisation expresse de l'éditeur, ne dispose pas du droit de les reproduire. Seule une copie de sauvegarde effectuée par le responsable informatique est autorisée.

Sans que cette liste soit exhaustive, l'utilisateur s'engage à :

- Utiliser les logiciels, applications, dans les conditions de la licence d'utilisation souscrite par CG2J et sous contrôle de la direction ;
- Ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels CG2J ne posséderait pas un droit d'usage ;
- Ne pas reproduire et utiliser les bases de données, pages web ou autres créations de l'entreprise ou de tiers protégés par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- Ne pas diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur le réseau internet ;
- Ne pas copier et remettre à des tiers des créations appartenant à des tiers ou à CG2J sans s'assurer de l'autorisation du titulaire des droits qui s'y rapporte.

➤ **Rappel : Les personnes impliquées dans la reproduction et/ou l'utilisation illicite de logiciels s'exposent à des poursuites judiciaires pouvant entraîner des amendes voire des peines d'emprisonnement. www.hadopi.fr**

Article 4 : Respect de législation sur la protection des données personnelles

Si, dans l'accomplissement de ses missions, l'Utilisateur constitue des fichiers contenant des données à caractère personnel soumis aux dispositions de la loi informatique et libertés, il en informe le dirigeant afin qu'un suivi puisse être réalisé en conformité avec la législation applicable.

Article 5 : Règles d'utilisation des services internet, de messagerie (web, messageries, forum ...)

L'agent doit se conformer aux principes issus de la législation en vigueur.

Utilisation d'Internet

Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle et une utilité au regard des fonctions exercées ou des missions à mener.

Une consultation pour un motif personnel est tolérée, à condition qu'elle reste ponctuelle, ne concerne que des sites Internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et ne mette pas en cause l'intérêt et l'organisation du conseil. L'utilisateur s'engage à respecter les règles suivantes dans les activités de navigation sur internet :

Accusé de réception en préfecture
083-258301555-20260202-2026_003-DE
Date de réception préfecture : 10/02/2026

- ✓ Ne pas consulter de sites à caractère raciste, pornographique, contraires aux bonnes mœurs, portant atteinte à la protection des mineurs, au respect de la personne humaine et de sa dignité, etc. ;
- ✓ Ne pas se connecter à des sites d'enchères ou de jeux en ligne par exemple...
- ✓ Prendre toutes les précautions permettant d'éviter que ses données (formulaires, adresses, coordonnées) soient utilisées des fins commerciales ou autres ;
- ✓ Ne pas consulter de sites contrevenant aux lois et règlements du droit français et/ou de la législation en vigueur dans le pays correspondant au site visité ;
- ✓ Ne pas télécharger de fichier sans l'accord de la société ;
- ✓ D'une façon générale, veiller à adopter un comportement prudent et avisé.

L'agent s'interdit de réaliser des pages ou sites personnels avec le matériel informatique appartenant à CG2J.

L'utilisation des réseaux sociaux répond aux mêmes règles de bon usage. En outre, l'utilisateur s'engage, dès que son appartenance à CG2J apparaît, à ne pas porter atteinte à l'image de marque interne et externe de l'entreprise, de ses clients et de ses partenaires.

L'utilisateur s'engage ainsi à :

- Veiller au respect de son obligation de réserve (ne pas dénigrer, ne pas divulguer...) ;
- Ne pas créer un profil au nom de CG2J sans autorisation préalable et expresse du directeur.

Utilisation de services de messagerie à partir du matériel appartenant à l'entreprise

L'agent doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques. Il lui est interdit d'émettre une quelconque opinion personnelle, étrangère à son activité professionnelle et susceptible, par son caractère illicite, de porter préjudice à CG2J.

L'agent ne doit jamais écrire un courriel qu'il s'interdirait d'exprimer oralement ou par un autre moyen, car le courriel peut constituer une preuve ou un commencement de preuve par écrit. à condition que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels.

Rappel :

- L'usage de messageries privées est interdit
- Il est demandé aux utilisateurs de procéder à un nettoyage régulier de leurs messageries afin de ne pas surcharger le serveur
- Chaque utilisateur doit être extrêmement vigilant lorsqu'il reçoit un mail avec pièce jointe ou un lien hypertexte. Si la provenance est inconnue ou douteuse (langue étrangère, faute d'orthographe ...) il convient de jeter le mail sans ouvrir la pièce jointe.
- si le mail vous demande de cliquer sur un lien, passez la souris sur le lien afin de vérifier sur quel site exactement cela vous amène : Ne cliquez pas si vous avez le moindre doute

Article 6 : Contrôle de l'utilisation des ressources informatiques

Pour des nécessités de maintenance, de gestion et de sécurité technique, l'utilisation des ressources matérielles ou logicielles, ainsi que les échanges via le réseau, peuvent être analysés et contrôlés, dans le respect de la législation applicable.

Contrôle des fichiers enregistrés sur le disque dur

Sauf preuve contraire, tout fichier stocké sur le disque dur d'un ordinateur ou d'un outil informatique propriété de CG2J et mis à la disposition du salarié est présumé professionnel.

Des vérifications et des audits réguliers pourront être effectués, dans les limites prévues par la loi et la jurisprudence.

➤ A titre informatif, l'employeur pourra ouvrir des fichiers identifiés par le salarié comme personnels, dès lors qu'il a connaissance de faits qui permettent de soupçonner un usage personnel abusif de l'ordinateur professionnel et qu'il a contacté le salarié afin qu'il puisse être témoin de la vérification, ou lorsqu'un risque ou évènement particulier nécessite l'ouverture de ce fichier en urgence.

Contrôle des connexions internet

La direction peut mettre en place un système de filtrage des sites internet consultables.

Un contrôle a posteriori des données de connexion à internet, par utilisateur, peut être effectué par celle-ci.

Contrôle de l'utilisation des messageries

Un ordinateur, mis à la disposition de l'agent dans le cadre de la relation de travail, est la propriété de la Collectivité et ne peut comporter que subsidiairement des informations relevant de l'intimité de la vie privée. Il doit être considéré qu'un message envoyé ou reçu depuis le poste de travail revêt *a priori* un caractère professionnel.

Néanmoins, tout message où figure le mot « privé » ou « personnel » bénéficiera d'une protection particulière : il sera couvert par le secret des correspondances.

Dans un souci de sécurité ou de contrôle de l'encombrement du réseau, CG2J peut mettre en place un dispositif de limitation du volume ou de la taille des messages échangés ou du format des pièces jointes.

Des vérifications et des audits réguliers pourront être effectués, dans les limites prévues par la loi et la jurisprudence.

Les agents ont été informés de ces contrôles et de leurs modalités par la présente Charte.

Une conservation de ces données pour une période de 6 mois est prévue.

Article 7 : Responsabilité / Sanction en cas de non-respect

Tout contrevenant aux principes mentionnés ci-dessus s'exposerait à une sanction déterminée par l'employeur, voire à des poursuites judiciaires, en fonction de la gravité des faits.

Les personnels de l'établissement sont soumis au secret professionnel : de ce fait, ils doivent faire preuve d'une discrétion absolue dans l'exercice de leur mission et notamment dans toute communication orale écrite téléphonique ou électronique.

Chaque utilisateur doit assurer la confidentialité des informations qu'il détient. Il ne doit pas divulguer par quelques moyens que ce soit (fichier numérique, fax internet ...) Des données nominatives et/ou confidentielles.

Article 8 : Entrée en vigueur

La présente charte entre en vigueur à compter de sa date de diffusion.

Chaque utilisateur reconnaît en avoir pris connaissance et s'engage à la respecter.

Engagement personnel :

Je soussigné (Nom, Prénom, Fonction)

Utilisateur des moyens informatiques de la Collectivité, déclare avoir pris connaissance de la Charte SI et m'engage à la respecter.

Fait à

Signature précédée de la mention lue et approuvée