Accusé de réception en préfecture
001-240100883-20260223-D20260223-060-DE
Date de télétransmission : 27/02/2026
Date de réception préfecture : 27/02/2026

DÉLIBÉRATION DU CONSEIL COMMUNAUTAIRE – N° 2026-060
« COMMUNAUTÉ DE COMMUNES DE LA PLAINE DE L'AIN »

L'an 2026, le lundi 23 février, à 18h00, le Conseil de Communauté de Communes de la Plaine de l'Ain, dûment convoqué, s'est réuni en session ordinaire, **à Chazey-sur-Ain, sous la présidence de Jean-Louis GUYADER, Président.**
Date de convocation : mardi 17 février 2026 - Secrétaire de séance : Élisabeth LAROCHE
Nombre de membres en exercice : 84 - Nombre de présents : 66 - Nombre de pouvoirs : 4 - Nombre de votants : 70

Étaient présents et ont pris part au vote : Philippe DEYGOUT, Daniel FABRE, Sylvie SONNERY, Christian de BOISSIEU, Liliane FALCON, Daniel GUEUR, Aurélie PETIT, Jean-Pierre BLANC, Stéphanie PARIS, Thierry DEROUBAIX, Jean-Marc RIGAUD, Joël GUERRY, Mohamed ABBES, Vincent MANCUSO, Gisèle LEVRAT, Hélène BROUSSE, Lionel MANOS, Laurent BOU, Sylvie RIGHETTI-GILOTTE, Marie-Françoise VIGNOLLET, Daniel MARTIN, Bernard PERRET, Jean-Louis GUYADER, Joël BRUNET, Claire ANDRÉ, Jean PEYSSON, Françoise GARIBIAN, Christian LIMOUSIN, Gérard BROCHIER, Serge GARDIEN, Joël MATHY, André MOINGEON, Dominique DALLOZ, Alexandre NANCHI, Walter COSENZA, Lionel KLINGLER, Jean-Pierre GAGNE, Thérèse SIBERT *(à partir de la délibération n°2026-025)*, Franck PLANET, Élisabeth LAROCHE, Régine GIROUD, Marie-José SEMET, Jean ROSET, Patrice MARTIN, Denis JACQUEMIN, Laurent REYMOND-BABOLAT, Nathalie MICOLAS, Pascal PAIN, Pascal COLLIGNON, Valérie CAUWET DELBARRE, Jehan-Benoît CHAMPAULT, Béatrice DALMAZ, Lionel CHAPPELLAZ, Fabrice VENET *(jusqu'à la délibération n°2026-034)*, Sylviane BOUCHARD, Gilbert BOUCHON, Josiane CANARD, Patrick MILLET, Marcel JACQUIN, Agnès OGERET, Daniel BEGUET, Estelle BARBARIN, Françoise VEYSSET-RABILLOUD, Émilie CHARMET, Éric BEAUFORT, Roselyne BURON, Bernard GUERS.
Étaient excusés et ont donné pouvoir : Viviane VAUDRAY (à Agnès OGERET), Jean-Luc RAMEL (à Élisabeth LAROCHE), Jean-Alex PELLETIER (à Régine GIROUD), Frédéric TOSEL (à Marie-José SEMET).
Était excusé et suppléé : Dominique DELOFFRE (par Hélène BROUSSE).
Étaient excusés : Patricia GRIMAL, Serge MERLE, Frédéric BARDOT, Maud CASELLA.
Étaient absents : Ludovic PUIGMAL, Cyril DUQUESNE, Stéphanie JULLIEN, Maël DURAND, Claire RAMONDOT, Mohammed EL MAROUDI, Michel MITANNE, Nazarello ALONSO, Gaël ALLAIN.

Objet : Adoption des chartes informatiques de la collectivité

VU
- le Code général des collectivités territoriales ;
- le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel (RGPD) ;
- le Référentiel Général de Sécurité (RGS) ;
- le Règlement européen relatif à l'intelligence artificielle (AI Act) ;
- l'avis du Comité Social Territorial en date du 9 février 2026 ;
- l'avis favorable du Bureau communautaire du 11 février 2026 ;

Dans le cadre de l'exercice de ses missions de service public, la communauté de communes de la plaine de l'Ain s'appuie sur un système d'information comprenant l'ensemble des données, équipements, applications, utilisateurs et acteurs chargés de son administration.
Le système d'information met à disposition des agents et des élus des outils numériques indispensables à l'accomplissement de leurs missions. Il est donc nécessaire de définir un cadre clair d'utilisation de ces ressources et d'inscrire cette démarche dans une gouvernance numérique structurée.
Une utilisation inappropriée de ces outils, qu'elle résulte d'une imprudence, d'une négligence ou d'un acte malveillant, est susceptible de porter atteinte à la disponibilité, à la confidentialité et à l'intégrité du système d'information, et d'engager la responsabilité civile et/ou pénale des utilisateurs ainsi que celle de la collectivité.

.../...

Accusé de réception en préfecture
001-240100883-20260223-D20260223-060-DE
Date de télétransmission : 27/02/2026
Date de réception préfecture : 27/02/2026

Les chartes informatiques sont des documents destinés à réglementer l'usage des systèmes d'information mis à disposition par la collectivité : elles n'ont pas vocation à décrire de façon exhaustive toutes les règles concrètes, pratiques et opérationnelles mais de fixer les principes généraux structurant les responsabilités de la collectivité et de l'utilisateur.
Face à l'augmentation des menaces cyber susceptibles d'affecter la continuité du service public, la collectivité doit renforcer ses mesures de prévention et de sécurisation. Les chartes informatiques constituent à ce titre un outil essentiel de protection du système d'information.
La communauté de communes de la plaine de l'Ain ne dispose actuellement d'aucune charte informatique formalisée. Leur adoption est rendue nécessaire par les évolutions réglementaires, technologiques et organisationnelles.

Il est proposé d'adopter trois chartes :

- une charte utilisateur (annexe 1) ;

- une charte administrateur (annexe 2) ;

- une charte relative à l'usage de l'intelligence artificielle (annexe 3).

PRÉSENTATION DES CHARTES

La charte utilisateur s'applique à l'ensemble des utilisateurs du système d'information, quel que soit le mode d'accès ou le matériel utilisé. Elle définit les obligations réglementaires, disciplinaires et contractuelles, précise les droits et devoirs des utilisateurs, encadre l'usage des ressources numériques dans le respect des libertés individuelles et du RGPD, et informe sur les dispositifs de contrôle mis en œuvre.

La charte administrateur concerne les personnels disposant de droits d'accès étendus. Elle rappelle les exigences de neutralité, de confidentialité et de loyauté attachées à ces fonctions, et précise le cadre dans lequel ces missions doivent être exercées.
La charte relative à l'intelligence artificielle s'applique à tout utilisateur ayant recours à des outils d'IA. Elle fixe les principes directeurs, le cadre réglementaire et les règles de bonne utilisation de ces technologies au sein de la collectivité.

CONSULTATION DES INSTANCES REPRÉSENTATIVES

Les instances représentatives du personnel ont été informées du contenu des chartes informatiques utilisateur, administrateur et intelligence artificielle lors d'une présentation en Comité Social Territorial (CST) en date du 09/02/2026.

PORTÉE JURIDIQUE

Les chartes informatiques ont un caractère opposable. Tout manquement est susceptible de donner lieu à des sanctions disciplinaires, contractuelles ou pénales. Pour cela, les trois chartes seront annexées au règlement intérieur de la collectivité.

INFORMATION DES AGENTS

Les chartes « utilisateurs » et « intelligence artificielle » seront portées à la connaissance de l'ensemble des agents en tant qu'annexes au règlement intérieur, sans recueil de signature individuelle.

La charte « administrateur » fera l'objet d'une identification des agents concernés par les responsables de service. Les agents désignés devront formaliser leur engagement par la signature d'un acte dédié. Les prestataires externes concernés devront également fournir un engagement écrit.

IMPACT FINANCIER

La présente délibération n'entraîne aucune incidence budgétaire.

.../...

Accusé de réception en préfecture
001-240100883-20260223-D20260223-060-DE
Date de télétransmission : 27/02/2026
Date de réception préfecture : 27/02/2026

Le Conseil communautaire, après avoir délibéré, à l'unanimité :

- APPROUVE la mise en place des trois chartes informatiques.
- APPROUVE les termes de la charte d'utilisation des données et des moyens informatiques et de communications à destination des utilisateurs du système d'information ci-jointe.
- APPROUVE les termes de la charte d'administration des ressources informatiques ci-jointe.
- APPROUVE les termes de la charte d'usage de l'Intelligence Artificielle ci-jointe.

Ainsi fait et délibéré les jour, mois et an ci-dessus, pour extrait conforme,
Le Président certifie, sous sa responsabilité, le caractère exécutoire de la présente délibération,
Transmise en Sous-Préfecture de Belley, le 27 février 2026
Publiée le 04 MARS 2026

Le Président, Jean-Louis GUYADER

COMMUNAUTÉ DE COMMUNES DE LA PLAINE DE L'AIN
Siège CHAZEY SUR AIN

Charte d'utilisation des données et des moyens informatiques et de communications

à destination des utilisateurs

Communauté de communes de la Plaine de l'Ain

Versions du document

Version	Date	Résumé des modifications
V1.0	04/12/2025	Version initiale - Charte des usages informatiques CCPA

Classification	Public	Sensible	Privé	Confidentiel
	X			

Avant-Propos

La Communauté de communes de la Plaine de l'Ain (CCPA) met à la disposition des utilisateurs des informations, des outils informatiques (PC, stations, logiciels, etc.), des moyens de communication (messageries, accès Internet, assistants personnels numériques, etc.), ainsi que des informations et données (bases de données, images, vidéos, etc.). Ces données et ces systèmes d'information sont indispensables au bon fonctionnement et au développement de la collectivité, de ses métiers et de ses fonctions et ils contribuent à la réalisation de ses missions de service public.

Ces données et ces systèmes d'information font partie du patrimoine immatériel et matériel de la Communauté de communes de la plaine de l'Ain. A cet égard, toute information émise, reçue ou stockée sur n'importe quel support (papier, électronique, …) est, et demeure la propriété de la collectivité.

Tout utilisateur de ces données et ces systèmes d'information appartient donc à une vaste communauté, ce qui implique de sa part le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent avoir des conséquences graves pour la communauté et le système d'information de la Communauté de communes de la Plaine de l'Ain.

La Communauté de communes de la Plaine de l'Ain définit et met en œuvre les moyens appropriés, en l'état de la technique, pour protéger les informations, les utilisateurs et les ressources mises à leur disposition contre tout risque matériel et immatériel.

La présente charte définit les droits et les devoirs applicables aux agents de la Collectivité.

Table des matières

1. Préambule

Article 1 - Définitions

Le système d'information

Le système d'information de la Communauté de communes de la Plaine de l'Ain comprend :

- Les informations et les données (quelles que soient leurs supports, numériques, papiers, ou les vecteurs de communication oraux, courrier ou réseaux informatiques, …) qui appartiennent ou qui ont été confiées à la CCPA ;
- L'ensemble des moyens informatiques, de télécommunication, de traitement, de conservation et de stockage ;
- Les utilisateurs, partenaires ou sous-traitants qui accèdent au système d'information de la CCPA ;
- Les acteurs qui mettent en œuvre ou administrent le système d'information.

Les utilisateurs du système d'information

Les utilisateurs du système d'information sont les agents ou agents en position d'encadrement, les élus, les intervenants internes ou externes, tous statuts confondus : permanents, contractuels, stagiaires et intervenants extérieurs temporairement autorisés.

Le Responsable des Systèmes d'Information

Le responsable des systèmes d'information a la charge de la mise en œuvre des dispositifs de traitement de l'information. Ces traitements sont conçus pour répondre aux besoins des métiers de la CCPA dans le respect des règles définies par le RSI. Il possède également le rôle de Responsable Sécurité Système d'Information (RSSI). A ce titre, il a la charge de la définition, de la mise en œuvre de politiques de sécurité du système d'information conformément aux obligations légales, en adéquation avec les besoins de sécurité des directions métiers et ayant pour objectifs la réduction des risques liés à l'usage des outils numériques. Le contrôle de la bonne gestion des risques liés à l'utilisation des données et ressources du système d'information est un point essentiel de sa mission.

Les administrateurs du système d'information

Les administrateurs du système d'information désignent toute personne, (interne, partenaire ou sous-traitante) ayant des droits d'accès privilégiés à des ressources du système d'information (SI) pour réaliser les tâches nécessaires au bon fonctionnement et à la sécurité des systèmes et des données qui lui sont confiées.

Le Délégué à la Protection des Données (DPO)

Le DPO est le Délégué à la Protection des Données à caractère personnel, il a pour mission l'assistance et le conseil auprès de la direction générale et des directions métiers pour la mise en conformité de la CCPA avec la règlementation pour la protection des données personnelles. Le contrôle de conformité à la réglementation est un point essentiel de sa mission.

Les données à caractère personnel

« Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, 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 ».

Les personnes concernées

Les personnes concernées sont toutes les personnes pouvant être identifiées, directement ou indirectement, par des moyens définis, utilisés par la collectivité ou mis en œuvre pour le compte de la collectivité, notamment par référence à un numéro d'identification, à un identifiant en ligne, à des données de localisation ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Traitement de données à caractère personnel

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).

Article 2 - Objectifs de la charte

La présente charte définit les principales règles et bonnes pratiques à adopter par les utilisateurs pour un usage correct, loyal et sécurisé des données et systèmes d'information actuels et futurs mis à sa disposition.

La présente charte ne fait pas obstacle à ce que des dispositions complémentaires soient définies par la collectivité en vue d'une utilisation des données et des systèmes d'information par les représentants du personnel, par les informaticiens, par les fournisseurs, ou par des tiers externes.

Elle définit les conditions générales d'utilisation des services Internet, des réseaux, des services multimédias et plus généralement des moyens de communications au sein de la Communauté de communes de la Plaine de l'Ain conformément au cadre légal et réglementaire en vue de sensibiliser et de responsabiliser l'utilisateur. Elle vise également à informer l'utilisateur des contrôles mis en place.

Article 3 - Champ d'application

La charte concerne la totalité des utilisateurs des données et des systèmes d'information de la collectivité et des structures bénéficiant du SI dans le cadre de mutualisation ; agents ou agents en position d'encadrement, élus et intervenants internes ou externes, tous statuts confondus : permanents, contractuels, stagiaires et intervenants extérieurs temporairement autorisés.

Elle s'applique quel que soit la méthode permettant à l'utilisateur d'accéder au système d'information de la CCPA (accès depuis un autre site, en télétravail, en situation de nomadisme ou tout autre type d'accès distant).

Article 4 - Condition d'application de la charte

L'utilisateur prend connaissance des règles de bonne conduite énoncées dans la charte et est tenu au strict respect de leur application. L'utilisateur est conscient que le non-respect de la charte peut entrainer des sanctions administratives et, le cas échéant sa responsabilité pénale.

Il est rappelé qu'en cas du non-respect du RGPD par l'Entité, celle-ci s'expose à des sanctions pouvant s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial.

Tout manquement à ces règles doit être signalé au responsable hiérarchique et à la direction générale. Ces responsables examinent collégialement les manquements aux dispositions de la charte et prennent les mesures adéquates conformément à la réglementation en vigueur.

Article 5 - Assistance

Le RSI, ainsi que le DPO sont à votre service pour vous assister dans le respect des règles consécutives aux droits et devoirs présentées dans la présente charte.

2. Les principes liés aux obligations réglementaires, disciplinaires et contractuelles

Article 6 - Le devoir de loyauté

Le devoir de loyauté vis à vis de la CCPA interdit aux utilisateurs de faire de leurs fonctions des instruments d'une propagande quelconque vis-à-vis du public, des usagers, des partenaires ou en interne.

La diffusion d'opinions générales pouvant entrainer la responsabilité de la CCPA ou de partenaires, quels que soient les moyens internes (fournis par la collectivité) et externes (non fournis par la collectivité) est interdite (réseaux sociaux, forums, blogs, Internet, intranet, messagerie professionnelle ou privée, …).

Article 7 - L'obligation de discrétion et de secret professionnel

Les utilisateurs s'engagent à faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice de leurs fonctions.

Les utilisateurs manipulant des informations confidentielles (données à caractère personnel, données techniques, données économiques, financières, sociales, médicales, …) sont tenus au secret professionnel. Ce devoir perdure à la fin du contrat ou de la mission.

Article 8 - Le devoir de notification d'incident et de violation de données

L'utilisateur s'engage à signaler dans les plus brefs délais au support, à l'encadrement, au RSI ou au DPO les incidents ou anomalies et les violations de données à caractère personnelle qu'il aurait pu détecter. L'utilisateur s'engage à ne pas exploiter ces incidents ou à en faire une publicité quelconque.

Tout utilisateur qui prendrait connaissance de manière fortuite, (par exemple, à la suite d'une erreur d'une perte ou d'un oubli), d'une information ou d'un document confidentiel sous quelque forme que ce soit (oubli au copieur, erreur de messagerie, …), ne doit en faire aucun usage que ce soit à titre privé ou à titre professionnel mais doit aussi signaler à l'émetteur s'il est identifiable, à l'encadrement, au RSI ou au DPO qu'il a eu connaissance de cette information.

Article 9 - L'utilisation professionnelle

La CCPA s'engage à mettre des moyens professionnels en place pour permettre aux utilisateurs de réaliser leurs missions demandées par la collectivité.

Les ressources du système d'information doivent être utilisées à des fins professionnelles conformément aux principes de la charte.

L'utilisateur s'engage également à ne pas utiliser des ressources personnelles pour ses activités professionnelles sauf sur dérogation validée par la direction générale.

Il en résulte que tout fichier créé par l'utilisateur ou tout message envoyé ou reçu revêt par défaut un caractère professionnel.

Article 10 - Le droit à la déconnexion

Le droit à la déconnexion peut être défini comme le droit d'un 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 (Ce temps comprend les heures normales de travail de l'agent et les éventuelles heures supplémentaires).

La CCPA s'engage à ne pas exiger de ses agents le traitement de courriels, messages ou appels téléphoniques à caractère professionnel envoyés en dehors de leur temps de travail. Seules la gravité, l'urgence ou l'importance exceptionnelle d'une situation peuvent justifier l'usage des outils numériques professionnels en dehors des heures travaillées.

Le responsable hiérarchique doit veiller au respect des modalités d'exercice du droit à la déconnexion. Il s'abstiendra, hors situation d'urgence ou liée à ses responsabilités, de formuler des demandes (par courriels ou autres moyens de communication) auprès de ses agents pendant les périodes de déconnexion.

Chaque utilisateur est acteur de sa propre déconnexion et doit veiller pour soi et ses collègues au respect de ses temps de repos et congés.

L'utilisateur, à l'exception des personnels d'astreinte, est invité à ne pas utiliser les outils numériques professionnels mis à sa disposition durant ses temps de repos. Il n'est pas tenu de prendre connaissance des emails, messages et appels téléphoniques qui lui sont adressés ou d'y répondre en dehors de son temps de travail habituel.

Afin de permettre à 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 à bloquer les accès sur une période donnée.

Par conséquent les accès resteront libres, toutefois chaque utilisateur devra veiller à sa sécurité et à sa santé en respectant les durées de repos quotidiennes et hebdomadaires.

Article 11 - L'usage à titre privé des espaces bureautiques

Conformément à la réglementation, la CCPA tolère l'utilisation à des fins personnelles (privées), du poste de travail, de l'Internet, de la messagerie et de la téléphonie dans la mesure où elle reste modérée, loyale, non lucrative, respectueuse des lois et des règles de la Collectivité.

L'utilisateur s'engage à respecter l'ensemble des principes de la charte dans son utilisation non professionnelle, modérée, loyale, non lucrative, respectueuse des lois et des règles, tolérée par la Collectivité.

Cette utilisation ne doit pas :

- Affecter le travail de l'utilisateur tant d'un point de vue qualitatif que quantitatif ;
- Remettre en cause la disponibilité et plus généralement la sécurité du système d'information ;

Afin que la CCPA puisse respecter cette utilisation privée et ponctuelle, il appartient à l'utilisateur de signaler cet usage privé. Pour cela il doit :

- Stocker les fichiers relatifs à sa vie privée, dans le dossier « Personnel/privé » prévu à cet effet sous le disque local du poste de travail à l'exclusion des espaces partagés ;
- Mentionner « personnel/privé » dans l'objet de ses courriers électroniques relevant de sa vie privée et informer ses correspondants de l'existence de cette règle ;
- Classer les courriers électroniques qu'il reçoit à titre privé dans un dossier de sa messagerie nommé « personnel/privé ».

L'utilisateur doit être conscient que la tolérance de la CCPA vis-à-vis d'une utilisation non professionnelle, modérée, loyale respectueuse des lois et des règles peut aussi entrainer indirectement la responsabilité de la CCPA.

Article 12 - La responsabilité civile

Un dommage causé à un tiers par le biais de l'utilisation des ressources du système d'information de la CCPA est tout à fait possible.

L'utilisateur doit être conscient qu'un dommage causé à un tiers dans le cas d'une utilisation personnelle/privée du système d'information (tolérée si elle est modérée, loyale, non lucrative, conforme aux lois et aux règles de la collectivité), peut entraîner sa responsabilité civile ou pénale individuelle.

Article 13 - Le droit à l'image

L'utilisateur dans le cadre de ses missions s'engage à ne pas prendre de photos ou d'enregistrements permettant d'identifier directement ou indirectement des personnes physiques sans l'autorisation de la personne concernée. Si des éléments d'identification sont présents, ils doivent être floutés.

Tout support d'image pris dans le cadre des activités de la CCPA ou dans ses locaux ne peut être utilisé à des fins personnelles et leur diffusion à l'extérieur est interdite sans l'autorisation écrite de la direction générale.

Article 14 - La lutte contre la fraude informatique

Les dispositions législatives de lutte contre les infractions liées aux technologies de l'information répriment :

- L'accès ou le maintien frauduleux dans un système d'information ;
- L'entrave au fonctionnement du système ;
- La falsification des données.

La CCPA s'engage à mettre en œuvre des dispositifs techniques et organisationnels adaptés afin de limiter les actes de malveillance.

L'utilisateur s'engage par conséquent à :

- Ne pas cacher son ou une identité (ne pas prêter son mot de passe) ;
- Ne pas tenter l'accès au système sans en avoir l'autorisation ;
- Ne pas tenter d'introduire intentionnellement des données ou du code malveillant ;
- Ne pas tenter de saturer le système ;
- Ne jamais télécharger, installer ou utiliser un logiciel sans autorisation, s'il entraine des incompatibilités, des dysfonctionnements dans le système d'information ou une non-conformité juridique. La responsabilité de la personne non autorisée à l'installation sera recherchée.
- Ne pas invalider ou court-circuiter un dispositif de sécurité, par exemple en tentant de désactiver l'antivirus du poste de travail.

Article 15 - La protection de la propriété intellectuelle

Le CCPA s'engage à respecter la propriété intellectuelle de ses fournisseurs et partenaires, à prendre des logiciels et des prestataires respectant les exigences du RGPD.

L'utilisateur n'installe pas de logiciel sans l'autorisation du RSI même s'il a été payé par l'utilisateur, (dans ce cas, la licence a été acquise par une personne physique privée et ne peut donc être utilisé par une personne morale).

Article 16 - La traçabilité

Conformément à la réglementation, la CCPA respecte l'obligation de conservation des données suivantes :

- Les informations permettant d'identifier les utilisateurs ;
- Les données relatives aux équipements utilisés ;
- Les caractéristiques de la consommation (ex : la date, l'horaire, la durée ...) ;
- Les données permettant d'identifier le ou les destinataires de la communication ;
- Les données historiques de navigation de l'utilisation d'internet sont conservées pendant un an.
- Les historiques des appels téléphoniques sont conservés pendant un an.

L'utilisateur est informé que la CCPA peut être amenée à réaliser des analyses statistiques.

L'utilisateur s'engage à ne pas empêcher le fonctionnement normal de ces moyens de traçabilité (usurpation d'identité, masquage d'identité, …).

Article 17 - La gestion des preuves

L'obligation de loyauté impose à l'utilisateur de communiquer à la direction générale tout document nécessaire à la poursuite d'une recherche ou d'une enquête sur incident.

L'utilisateur doit être conscient qu'un message électronique (Courriels, SMS, identifiant Internet, …) peut constituer un élément de preuve pouvant engager sa responsabilité ou celle de la collectivité.

Article 18 - Les contrôles

La confiance envers les utilisateurs passe par la définition de règles claires sur l'utilisation des données et des systèmes d'information mais nécessite également que la CCPA précise les contrôles qu'il effectue pour s'assurer du respect de ces règles.

La CCPA respecte la vie privée des utilisateurs sur le lieu de travail. Il exerce toutefois un contrôle de l'usage des données et des systèmes d'information, dans le respect des dispositions légales applicables, notamment la loi relative à la protection de la vie privée et des données à caractère personnel. Les finalités de ce contrôle sont les suivantes :

- La prévention et la répression de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui, ainsi que la répression de ces faits ;
- La protection des intérêts de la CCPA auxquels est attaché un caractère de confidentialité ;
- La sécurité et/ou le bon fonctionnement technique des systèmes informatiques de la CCPA, y compris le contrôle des coûts y afférents, ainsi que la protection physique des installations ;
- Le respect de la bonne foi des principes et règles d'utilisation des technologies en réseau définis par la présente charte ou autres directives et instructions de la CCPA.

La CCPA respecte le principe de la proportionnalité dans la poursuite de ces finalités. Si les données collectées sont traitées en vue de finalités autres que celles pour lesquelles le contrôle a été installé. La CCPA s'assure que ce traitement est compatible avec les finalités initialement poursuivies et prend toutes les mesures nécessaires pour éviter les erreurs d'interprétation.

La supervision technique

La supervision technique est nécessaire pour assurer le fonctionnement normal du système d'information. La CCPA dispose de moyens informatiques effectuant des contrôles automatiques. Sont notamment surveillées les données relatives à l'utilisation :

- De la messagerie électronique : blocage de pièces jointes aux messages et fichiers infectés ; interdiction à l'envoi ou l'entrée par messagerie de fichiers trop volumineux ;
- Des logiciels applicatifs pour contrôler l'accès, la création, la modification et la suppression de données ;
- Des connexions entrantes et sortantes du réseau ;
- Des communications téléphoniques ;
- Des logiciels de sécurité (antivirus, sondes de détection d'intrusion) ;

Ce contrôle ne s'exerce jamais sur le contenu de l'information.

Le contrôle de la sphère privée

Conformément à la réglementation, la nature « personnelle/privée » ne la soustrait pas à un contrôle de l'employeur, mais définit étroitement les conditions d'un tel contrôle, La CCPA s'engage à respecter ces conditions.

La présente charte informe les utilisateurs que l'espace utilisé par l'utilisateur pour un usage « personnel/privé » peut être sujet à des contrôles. Ces contrôles sont possibles en cas de situation exceptionnelle où les intérêts de la CCPA pourraient être mis en danger, (non-conformité aux obligations légales ou contractuelles, perte d'image, …) ou si des comportements pénalement sanctionnables l'exigeaient.

L'utilisateur en sera toujours informé au préalable notamment en ce qui concerne la finalité de ce contrôle et pourra exiger d'être présent et accompagné d'un représentant du personnel.

Les administrateurs réalisant ces contrôles sont tenus au strict secret professionnel.

Face à des situations d'exceptionnelle gravité, et où l'utilisateur ne pourrait être informé, un contrôle de l'espace réservé « personnel/privé » est possible. L'utilisateur sera toujours informé dès que possible de la situation d'exceptionnelle gravité ayant motivé ce contrôle.

Ce type de contrôle ne peut être réalisé que par les administrateurs et uniquement sur mandat de la direction générale voir des autorités judiciaires.

Le contrôle de l'utilisation d'Internet

Au moyen de logiciels adaptés, la CCPA collecte des données générales concernant les sites internet consultés via le réseau, y compris des données concernant la durée et le moment des visites. Il s'agit d'un contrôle anonyme et non individualisé qui ne vise pas le contenu des informations consultées. Lorsqu'à l'occasion de ce contrôle général ou au départ de données du système d'information, La CCPA constate une anomalie, elle se réserve le droit de procéder à l'identification d'un utilisateur, conformément à la procédure d'individualisation décrite au paragraphe « contrôle individualisé » ci-dessous.

Les informations recueillies dans ce cadre sont les suivantes :

- Date et heure de la consultation ;
- Nom de l'utilisateur ;
- « Adresse réseau » de la station de travail ;
- Site consulté ;

- Catégorie(s) du site ;
- Durée de la connexion ;
- Volume d'informations échangées.

Les données issues du contrôle général et non individualisé de l'utilisation d'Internet sont conservées pour une durée maximale de six mois.

En cas de détection d'une anomalie de sécurité ou d'un usage non conforme nécessitant une investigation, les données strictement nécessaires à cette investigation peuvent être extraites et conservées pour une durée limitée à la clôture des vérifications ou, le cas échéant, de la procédure disciplinaire ou judiciaire associée.

Le déchiffrement des flux sécurisés

La mise en place d'outils de chiffrement est soumise à des dispositions légales relatives à la cryptologie dont la violation peut être sanctionnée sur le plan administratif, civil et pénal.

Dans le cadre de l'usage des services internet, la CCPA ne limite pas l'usage des échanges sécurisés utilisant un chiffrement de données (protocole TLS).

Cependant, l'utilisation de moyens de chiffrement peut être source de responsabilité de la CCPA, notamment, lorsque le chiffrement a permis ou facilité la commission d'infractions ou a conduit au non-respect des obligations de sécurité à sa charge.

En conséquence, dans le cadre des contrôles, la CCPA peut procéder au déchiffrement du contenu de flux chiffrés transitant sur les postes de travail des utilisateurs dans le respect de la législation en vigueur.

Ce déchiffrement vise à lever les cas de doute relatifs à des agissements délictueux qui pourraient être commis par les utilisateurs grâce aux moyens mis à leur disposition (matériels, accès internet, etc.) et dissimulés grâce au chiffrement.

Le contrôle de l'utilisation du courrier électronique

Les messages électroniques peuvent être contrôlés pendant toute la durée de présence dans la boite de messagerie courante. Sur la base d'indices généraux tels que la fréquence, le nombre et le volume des courriers électroniques, les annexes, …, certaines mesures de contrôle pourront être prises par l'administration vis-à-vis de ces messages. Si la CCPA présume un usage anormal ou interdit du système de courrier électronique, il procédera, à l'identification de l'utilisateur concerné, conformément à la procédure d'individualisation décrite ci-dessous.

Le contrôle de la téléphonie

Un relevé mensuel des consommations téléphoniques (téléphones fixes et portables) peut être établi par la CCPA. Il peut mentionner le numéro de téléphone appelé (à l'exception des 4 derniers chiffres), le jour, l'heure et la durée de l'appel ainsi que le montant des communications téléphoniques. Les Informations collectées sont conservées pendant un an.

A la demande de l'autorité territoriale et après information de l'utilisateur concerné, il pourra être établi un relevé spécifique de l'ensemble des appels téléphoniques de l'utilisateur faisant apparaître, pour chacun de ses appels, la date, la durée, le numéro du correspondant appelé et le coût de la communication.

Si elles ne sont pas justifiées par d'évidentes raisons de service, ces communications feront l'objet d'une demande de justification. Le cas échéant, la CCPA se réserve la possibilité de déclencher une procédure disciplinaire en cas d'utilisation non justifiée des moyens téléphoniques mis à disposition de l'utilisateur.

Le contrôle individualisé

La CCPA peut individualiser les contrôles en conformité avec les finalités poursuivies par le contrôle. Par « individualisation », on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un utilisateur identifié ou identifiable.

Lorsque l'objectif du contrôle tient au respect de la bonne foi des règles et principes d'utilisation des technologies fixées dans les normes de sécurité de la CCPA, la CCPA respecte une phase dite « de sonnette d'alarme » qui vise essentiellement à informer l'utilisateur d'une anomalie et à l'avertir d'une individualisation en cas de récurrence.

Si la CCPA suspecte ou constate un manquement aux règles et principes de la présente charte, il avertira l'utilisateur concerné et peut, le cas échéant, enclencher une procédure disciplinaire à son encontre.

L'utilisateur s'engage à ne pas empêcher les contrôles.

3. Le Règlement Général sur la Protection des Données (RGPD)

Article 19 - Les principes fondamentaux de la protection des données

La CCPA s'engage à respecter les principes relatifs à la protection des données à caractère personnel :

Le principe de loyauté, de licéité et de consentement

Les données à caractère personnel doivent être traitées de manière loyale, licite et transparente, avec le consentement de la personne concernée quand le traitement n'est pas consécutif à une obligation légale ou contractuelle, l'exercice d'une mission de service public, l'intérêt légitime de la CCPA ou la sauvegarde des intérêts vitaux de la personne concernée.

Le principe de finalité

La CCPA traite les données à caractère personnel uniquement pour un usage déterminé, explicite et légitime.

Le principe de proportionnalité et pertinence

La CCPA traite uniquement des données à caractère personnel adéquates, pertinentes, limitées, nécessaires, exactes et mises à jour au regard des objectifs poursuivis.

Le principe de durée de conservation

Le CCPA s'engage à ce que les données à caractère personnel ne puissent être conservées de façon indéfinie. La durée de conservation des données à caractère personnel est déterminée en fonction de la finalité de chaque traitement, en concertation avec le délégué à la protection des données.

Le principe de sécurité et de confidentialité des données

La CCPA, en tant que responsable de traitement de données à caractère personnel s'engage à mettre en œuvre des mesures juridiques, organisationnelles et techniques afin de protéger la disponibilité, la confidentialité, l'intégrité et la traçabilité des données.

Le principe du respect des droits des personnes

La CCPA s'assure que le traitement de données à caractère personnel est accompli conformément au principe du respect des droits et des personnes concernées.

La CCPA s'engage à mettre en place et respecter les procédures pour répondre aux demandes des personnes concernées.

A ce titre, elle désigne un DPO afin d'assister les utilisateurs à respecter les principes de la réglementation et s'engage à ce qu'il puisse réaliser ces missions en totale indépendance et sans le mettre dans une situation de potentiel conflit d'intérêt.

Engagement de l'utilisateur

L'utilisateur s'engage à ne pas constituer de fichiers de données à caractère personnel dans le cadre professionnel sans avoir l'autorisation au préalable de son encadrement et du DPO.

Les utilisateurs s'engagent à ne pas faire un usage ultérieur des données qui ne seraient pas compatible avec la finalité des traitements qui ont poussés à la collecte des données sans en avoir l'autorisation au préalable de son encadrement et du DPO.

Les utilisateurs ne collectent pas de données à caractère personnel, excessives ou disproportionnées au regard de la finalité du traitement.

Les utilisateurs engagent leur responsabilité à ne pas utiliser leurs droits de lecture pour des finalités autres que celles définies dans leurs missions.

L'utilisateur s'engage à ne pas mentionner dans les fichiers à caractère personnel des données interdites sans autorisation spécifique (ethnie, religion, croyance, mœurs privées, santé, appartenance syndicale, …).

L'utilisateur s'engage à ne pas mentionner des informations subjectives et/ou non autorisées par la législation dans les zones de commentaires disponibles dans les formulaires et/ou les fichiers sans en informer l'usager et lui avoir demandé son accord, et à ne pas générer des commentaires désobligeants, discriminants, voir injurieux. L'usage des zones de commentaire est strictement réservé aux informations d'ordre général et en aucun cas ne peut porter atteinte aux droits des personnes concernées.

Lorsqu'un service reçoit une demande d'exercice de droit de la part d'une personne, celui-ci est en charge de la réponse à y apporter. En cas de demande complexe ou de besoin, le service peut demander assistance au DPO pour l'appuyer dans la réponse.

En cas de difficulté ou interrogation sur le respect de la réglementation, l'utilisateur s'engage à demander conseil au DPO.

Article 20 - Le respect des droits des personnes

La CCPA s'engage à mettre en place les moyens organisationnels et techniques pour permettre aux utilisateurs de respecter les droits des personnes concernées, notamment en mettant en œuvre une *Procédure RGPD – Exercice des droits* des personnes concernées.

Lors de la réception de l'exercice d'un droit, notamment un droit d'accès, de rectification ou à l'oubli, l'utilisateur s'engage à suivre la *Procédure RGPD – Exercice des droits*. Toute demande doit être notifiée dans les meilleurs délais au DPO et à la hiérarchie qui ont la charge de faire respecter les procédures concernant les demandes des personnes concernées.

Article 21 - Les traitements de données sensibles

La réglementation et les directives de la CNIL imposent un traitement spécifique des données sensibles (opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle, données biométriques ; Infractions, condamnations, mesures de sécurité – autorisation) et des données perçues comme sensibles (numéro de sécurité sociale (NIR), appréciation sur les difficultés sociales, données bancaires).

Chaque utilisateur traitant ce type de données doit veiller à :

- Ne traiter ces données que dans le cadre des obligations légales en vigueur et en respectant les procédures déclaratives auprès du DPO.
- Limiter l'accès aux données (papiers et numériques) aux seuls agents habilités.
- S'assurer que la protection des données est bien assurée (notamment lors de leur stockage et de leur transfert) et d'alerter le DPO en cas de violation sur ces données.

Article 22 - L'archivage ou la suppression des données personnelles

La CCPA s'engage à mettre en place des moyens d'archivage et de suppression des données adaptés à leurs sensibilités.

La conservation de données des usagers ou des agents est soumise à des obligations légales qui imposent une suppression ou un archivage de celles-ci dans les délais prévus par la loi ou par les règles d'archivages.

L'utilisateur doit s'informer des durées légales de conservation des données des administrés qu'il est amené à traiter et à respecter les procédures relatives à l'archivage ou à la purge des données.

Lorsque les données ne sont pas soumises à une obligation d'archivage, l'utilisateur s'engage à les supprimer dès lors qu'elles ne sont plus utiles dans le cadre du traitement qu'elles soient sous une forme numérique ou papier en respectant strictement les procédures en vigueur à la collectivité.

4. Les principes liés à l'utilisation du système d'information

Article 23 - Les équipements numériques

La CCPA met à disposition des utilisateurs les équipements numériques (postes de travail sédentaires ou mobiles, tablettes, smartphones, …) pour une utilisation professionnelle et met en œuvre des mécanismes de journalisation des actions réalisées avec ces équipements notamment lors des connexions à distance.

Les utilisateurs des postes de travail, smartphones et tablettes veilleront à n'en faire usage que dans un cadre professionnel.

Toutefois, la CCPA tolère une utilisation « raisonnable » à des fins personnelles, c'est-à-dire modérée, mais aussi loyale respectueuse des intérêts de la collectivité, conforme aux règles citées et respectueuse des lois. Cette utilisation « raisonnable » est définie comme ne nuisant en aucune façon à l'exécution normale des missions de l'utilisateur ou au bon fonctionnement des systèmes d'information de la collectivité.

L'utilisateur s'engage à être vigilant à l'utilisation d'internet ainsi qu'aux communications passées lors de déplacements à l'extérieur notamment l'étranger.

L'usage et le branchement d'équipements (Smartphone, PC Portable, disque dur/clé USB, …) personnels de l'utilisateur sur le système d'information de la CCPA est strictement interdit sauf sur dérogation écrite et approuvée par la direction.

Tout usage abusif des systèmes d'information mis à disposition par la CCPA est strictement interdit. En cas de manquement à cette disposition, l'utilisateur s'expose à des sanctions disciplinaires proportionnées à la gravité des faits concernés. Il faut entendre par « usage abusif » :

- L'usage répété et prolongé durant et/ou en dehors des heures normales de travail des données et des systèmes d'information mis à disposition par la CCPA pour des fins non professionnelles.

- L'usage des systèmes d'information durant et/ou en dehors des heures normales de travail pour des finalités contraires à toute législation, à l'ordre public et aux bonnes mœurs ou pour des finalités qui sont susceptibles d'être sanctionnées, par voie pénale ou autre, par une autorité compétente ou une quelconque autorité étrangère.

De manière plus générale, il est interdit de faire usage des données et des systèmes d'information mis à disposition par la CCPA dans un sens contraire aux principes repris dans la présente charte ou contraire aux instructions ou directives données par les responsables hiérarchiques.

L'utilisateur en cas de départ définitif de la CCPA s'engage à restituer les équipements numériques qui lui ont été confiés.

Article 24 - L'installation et la maintenance

Seule les équipes en charge de la gestion du système d'information (RSI, infogérance) sont habilitées à acheter, installer et dépanner des matériels informatiques et télécoms. Les logiciels sont inclus dans cette disposition afin de respecter les exigences sur les licences d'utilisation. La direction générale est sollicitée en cas d'arbitrage entre les différentes demandes des services.

L'utilisateur est responsable du bon usage de son équipement. Il s'engage à :

- Ne pas déplacer du matériel sans autorisation, ni de déplacer les connexions réseau ou téléphonique vers d'autres prises.
- Faciliter les conditions d'intervention du support informatique.
- Respecter la législation en vigueur sur la reproduction et le copyright des logiciels

L'utilisateur n'est en aucun cas habilité à installer des logiciels sur les systèmes d'information mis à sa disposition. L'installation de logiciels est de la compétence exclusive des équipes en charge de la gestion du système d'information. Seule la direction générale est habilitée à valider l'achat de logiciels.

Lorsque l'utilisateur quitte son poste de travail, il s'engage à le verrouiller.

Article 25 - L'identification, l'authentification et l'habilitation

La CCPA met à disposition des utilisateurs des codes d'identification et d'authentification (nom d'utilisateur, mot de passe, …). La CCPA ne connait pas les mots de passe individuels des utilisateurs du système d'information.

Chaque utilisateur utilisant le système d'information doit être identifié et authentifié par un compte nominatif. La CCPA s'engage à limiter l'utilisation de comptes génériques ne permettant pas d'identifier une personne physique.

L'utilisateur n'a accès qu'aux seules informations et ressources dont il a besoin dans le cadre de ses missions.

En cas de changement de fonction, les habilitations sont modifiées pour répondre aux nouvelles missions de l'agent selon les informations transmises par le service ressources humaines ou par la direction métier. Pour information, cette autorisation est suspendue dès que les missions de l'utilisateur prennent fin même temporairement.

La CCPA se réserve la possibilité de modifier les habilitations décernées à l'utilisateur en cas de modification significative de ses conditions de travail, (exemples : exécution de préavis, suspension du contrat de travail, etc.), de changement de poste ou d'utilisation non conforme à la présente charte.

Les utilisateurs doivent être conscients que ces codes d'authentification ne formalisent pas des autorisations d'accès mais garantissent la véracité de l'identité d'un utilisateur. Les codes d'authentification sont strictement personnels, incessibles, confidentiels et temporaires. Ces dispositifs d'authentification de leurs identifications engagent donc leurs responsabilités.

De plus concernant les mots de passe :

- L'utilisateur s'engage à utiliser un mot de passe différent entre la sphère privée et la sphère professionnelle ;
- L'utilisateur est responsable de son code utilisateur et de son mot de passe d'accès, et ce, pour toutes les ressources auxquelles il a accès ; Dans l'hypothèse d'un oubli par l'utilisateur de son mot de passe, un nouveau mot de passe utilisateur pourra être créé conformément à une procédure sécurisée ;
- L'utilisateur veille à ce qu'une personne non autorisée ne puisse pas travailler sous son code utilisateur ; Dès qu'un utilisateur soupçonne que son mot de passe est connu d'autres utilisateurs ou d'un tiers, il est tenu de le changer immédiatement ; Les tentatives d'accès non autorisé, d'intrusion ou de contournement des sécurités d'accès sont interdites ;
- L'utilisateur ne doit pas communiquer son mot de passe à un tiers sauf nécessité et autorisation préalable et écrite de l'autorité territoriale ;
- L'utilisateur ne doit pas utiliser ou essayer d'utiliser des codes utilisateurs autres que les siens ou de masquer sa véritable identité ; La transmission du mot de passe ou le fait de travailler avec le code utilisateur d'un autre utilisateur sont interdits ;
- L'utilisateur s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès au système d'Information de la collectivité. Toutes les opérations effectuées sous un code utilisateur sont considérées comme ayant été initiées par l'utilisateur à qui a été attribué ce code. Ainsi, l'Utilisateur est responsable des fautes, erreurs, détournements, fraudes, malversations réalisées par le biais de son code utilisateur, sauf à prouver l'utilisation frauduleuse de ce code par un tiers ;
- L'utilisateur doit choisir des mots de passe robustes conformes à la politique de sécurité des mots de passe de la CCPA. Ces mots de passe ne doivent jamais être repris par écrit et stockés près d'un ordinateur ou d'un poste de travail ou ailleurs.

Article 26 - Le stockage et les sauvegardes

La CCPA met à disposition sur des serveurs (stockage partagé) des dossiers informatiques et en assure la sauvegarde régulière, tels que :

- Un dossier « service » accessible uniquement par les utilisateurs du service. Certaines restrictions d'accès sont possibles sur certains sous-dossiers.
- Des dossiers accessibles par une communauté de travail (par exemple un répertoire partagé entre plusieurs services) ou par l'ensemble des utilisateurs.
- Un dossier personnel (privé) et nominatif dont la taille est limitée. Les données stockées doivent être conformes aux principes de la présente charte et aux lois.

La CCPA met à disposition des postes de travail (stockage individuel) et des disques amovibles (stockage amovible) qui ne sont pas sauvegardés.

Chaque utilisateur s'engage à :

- Observer la plus grande vigilance dans l'utilisation de périphériques USB sur le poste de travail.
- Stocker ses données professionnelles sur les serveurs de la CCPA. L'utilisateur est seul responsable des données présentes sur son poste.
- Ne pas stocker de fichiers privés (photos privées, films, etc…) sur les serveurs.
- Ne pas enregistrer des données professionnelles sur des environnements Cloud (Google drive, One drive, Drop box, iCloud, etc…) non validés par la CCPA.

- Archiver ou éliminer les fichiers dont il n'a plus une utilité immédiate.

Dans le cas où l'utilisateur enregistre sur un poste de travail des données privées, il doit clairement nommer son répertoire « Privé » ou « Personnel ».

La CCPA est susceptible d'accéder à ces dossiers pour des motifs légitimes (sécurité informatique, respect des lois …), sur mandat de la direction générale et après une information préalable obligatoire de l'utilisateur qui peut exiger d'être présent, accompagné ou représenté.

Article 27 - Les impressions

La CCPA fait en sorte de mutualiser au maximum les moyens d'impression existants afin de limiter le nombre des imprimantes personnelles sans porter atteinte aux conditions et à la qualité du travail des utilisateurs. Un rapport peut être adressé périodiquement à chaque utilisateur faisant apparaître le nom des utilisateurs et le nombre d'impressions.

Les utilisateurs des systèmes d'impression, dont les photocopieurs et matériels multifonctions, veilleront à n'en faire usage que dans un cadre professionnel.

Article 28 - La messagerie

La CCPA met à la disposition des utilisateurs une messagerie électronique pour un usage professionnel.

Un usage privé et raisonnable respectueux des règles de la CCPA et des obligations légales, dans le cadre des nécessités de la vie courante et familiale est toléré, sous réserve que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels, la sécurité du système d'information, les missions de l'utilisateur.

Dans ce cas, l'utilisateur fera apparaître dans le champ objet du message le caractère privatif du message : « PRIVE ».

De plus, il devra supprimer dans le corps du message, toute mention relative à la CCPA (telle que la signature automatique) et toute autre indication qui pourrait laisser suggérer que le message est rédigé par l'utilisateur dans le cadre de ses fonctions.

En l'absence de toute indication, le message électronique sera considéré comme un message professionnel et non comme un message à caractère privé.

La messagerie électronique est soumise aux règles qui régissent les droits et obligations des utilisateurs, notamment la discrétion, la réserve et la neutralité. Les messages ne doivent pas porter atteinte à l'image de la collectivité, notamment par des mentions injurieuses, insultantes ou diffamatoires.

Il est interdit de :

- Créer et utiliser, à titre professionnel, des adresses électroniques autres que celles attribuées par la CCPA.
- Utiliser l'adresse de la messagerie professionnelle pour s'inscrire sur un site internet à usage non professionnel.
- Envoyer des courriers électroniques contraires à l'ordre public ou des messages diffusant des informations fausses, erronées, tendancieuses, dangereuses ou couvertes par le secret et divulguées sans l'autorisation de leur légitime propriétaire ou dépositaire.
- Diffuser des œuvres protégées par le droit d'auteur comme les livres, les brochures, les écrits littéraires, artistiques ou scientifiques, les illustrations, les dessins, les photographies, les compositions musicales, etc.

- Diffuser à l'ensemble des adresses électroniques des messages à caractère personnel, politique, syndical, religieux ou philosophique.
- Diffuser des canulars informatiques qui sont des informations fausses, périmées ou invérifiables.
- Transférer ou rediriger des messages vers une boîte électronique privée est strictement interdit sans autorisation de la CCPA.
- Utiliser la signature professionnelle automatique, l'en-tête/logo ou toute autre indication de la CCPA lors des courriers électroniques et d'échanges électroniques à des fins personnelles ou syndicales.
- Participer à des chaînes de lettres/messages

L'utilisateur ne doit jamais diffuser un message électronique qu'il s'interdirait d'exprimer oralement ou par tout autre moyen (courrier, télécopie, etc.).

Par ailleurs il doit également :

- Utiliser avec discernement les listes de diffusion individuelles ou collectives ;
- Eviter l'envoi de copies à un nombre injustifié de destinataires ;
- S'appliquer à rédiger des messages courts et clairs pour éviter toute surcharge informationnelle nuisant à l'efficacité de la communication.
- S'assurer qu'il s'agit du bon destinataire pour tout envoi de données personnelles ou d'informations sensibles.
- En cas d'envoi à plusieurs personnes dont au moins 1 destinataire est externe à la CCPA, il est recommandé d'utiliser le champ CCI (copie cachée).

Article 29 - L'Internet

Une solution de filtrage permet d'empêcher la connexion à un certain nombre de sites interdits par la loi (pédophilie, révisionnisme …) ou par la charte, ou pour des raisons de sécurité informatique (virus …).

Ce filtrage ne peut être efficace à 100%, aussi l'accessibilité à un site ne signifie pas qu'il est légal et/ou autorisé.

L'utilisateur doit être conscient que la navigation sur Internet est avant tout professionnelle.

Un usage personnel est toutefois toléré pour autant qu'il ne porte pas atteinte à autrui, au bon fonctionnement du réseau ou à la productivité de l'utilisateur. La CCPA se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès aux sites dont il juge le contenu illégal, offensant ou inapproprié. La CCPA ne saurait être tenue pour responsable de toute infraction commise par un utilisateur ne se conformant pas à ces règles.

Il est formellement interdit de :

- Consulter ou télécharger des données (textes, images, sons) ayant un caractère, contraire à la loi, portant atteinte à la dignité ou à la vie privée, à caractère injurieux, raciste, pornographique, diffamatoire, en rapport avec une secte ou incitant à la violence ;
- Consulter des sites où il n'est pas possible d'identifier la personne juridiquement responsable du service Internet ;
- Consulter des sites de jeux d'argents, de partage peer to peer, de pornographie ou de contournement de proxy (site de redirection masquant le trafic réel) ;
- Télécharger et installer des logiciels sans autorisation de la CCPA ;

- Accéder ou tenter d'accéder à un serveur ou à un poste de travail sans avoir été préalablement habilité ;
- Se livrer à des actions portant atteinte à la sécurité ou au bon fonctionnement des systèmes d'information ;
- Créer des sites web personnels en utilisant les ressources informatiques de la CCPA ;
- S'exprimer sur les blogs, forums ou les réseaux sociaux au nom de la CCPA sans en avoir l'habilitation ;

La CCPA ne saurait être tenu pour responsable de toute infraction commise par un utilisateur ne se conformant pas à ces règles.

Article 30 - La téléphonie

La CCPA met à disposition des téléphones fixes et mobiles pour une utilisation professionnelle. Elle définit le niveau de service proposé aux utilisateurs (SMS, messagerie, forfait, etc.) en accord le chef de service concerné.

La CCPA s'engage à respecter les exigences réglementaires sur l'enregistrement des conversations téléphoniques sur le lieu de travail, consultation des instances représentatives du personnel, information au préalable des agents et des interlocuteurs, possibilité de neutraliser l'enregistrement pour les appels privés.

Les utilisateurs des téléphones fixes et mobiles veilleront à n'en faire usage que dans un cadre professionnel.

Toutefois, les communications téléphoniques à caractère personnel de courte ou de longue distance (appels sortants) limitées uniquement aux cas d'urgence sont tolérées. On entend par cas d'urgence les situations qui ne peuvent attendre le retour de l'agent dans la sphère privée.

Les appels entrants de courte durée peuvent être autorisés pour peu qu'ils ne perturbent pas le fonctionnement des services.

Dans un souci d'économie, il convient de ne pas renvoyer les appels des téléphones fixes vers les mobiles de manière systématique et permanente.

Article 31 - L'utilisation de l'informatique en « nuage » (Cloud)

L'utilisateur s'engage à ne pas stocker ou déposer des données professionnelles sur des services « cloud computing » grand public (exemple : Drop box, WeTransfer, Google Drive, iCloud, …) sans en avoir reçu préalablement l'autorisation de la CCPA.

Article 32 - L'utilisation des systèmes d'intelligence artificielle

L'usage de tout système d'intelligence artificielle est régi par une charte spécifique à ces technologies. Cette charte d'usage de l'IA est annexée au règlement intérieur de la collectivité.

Article 33 - L'utilisation des certificats électroniques

La CCPA met à la disposition de son personnel des certificats électroniques pour s'authentifier ou signer des documents administratifs dans le cadre de la mise en œuvre des démarches d'administration électronique. Ces certificats électroniques sont attribués personnellement aux agents désignés.

Il appartient aux agents concernés d'assurer la sécurisation des supports des certificats qui ne doivent en aucun cas être partagés.

En cas de perte du support de certificat, l'utilisateur doit informer sans délai son supérieur hiérarchique.

Article 34 – La continuité de service : gestion des absences et procédures en cas de départ

En cas d'absence temporaire (planifiée ou imprévue) et afin d'assurer la continuité de service, la CCPA peut être amenée à accéder aux données professionnelles (fichiers, messages électroniques, …) stockées par l'utilisateur. A la demande du responsable hiérarchique et pour des motifs professionnels légitimes, la CCPA, après consultation et accord de l'autorité territoriale, pourra mettre à sa disposition :

- L'ensemble des fichiers informatiques de l'utilisateur, sauf ceux contenus dans son dossier personnel-privé.
- Le contenu de la messagerie de l'utilisateur dans le respect de la protection de sa vie privée (notamment l'interdiction d'accès aux courriels « Privé/Personnel »)

Le service RH informera l'utilisateur dès que possible des accès qui ont été donnés au supérieur hiérarchique.

En cas d'absence temporaire ou définitive, si l'utilisateur ne rédige pas de message de « réponse automatique » dans sa messagerie, le supérieur hiérarchique peut également demander de mettre en place un message de « réponse automatique » orientant vers un autre interlocuteur.

L'utilisateur est informé que, à la suite de son départ définitif (planifié ou non planifié) :

- Des procédures spécifiques relatives à l'accès aux données professionnelles après son départ sont prévues par la direction générale afin de permettre la continuité du service public dans le respect du secret de correspondance et de la vie privée.
- La boîte de messagerie professionnelle de l'utilisateur sera supprimée dans un délai défini par la direction générale.

Afin d'assurer la continuité de service en son absence ou en cas de départ, l'utilisateur doit définir dans sa messagerie professionnelle un message de « réponse automatique » informant de son absence ou départ et permettant également d'orienter les correspondants vers un autre interlocuteur susceptible de répondre à la sollicitation.

En cas de départ de la collectivité, l'utilisateur s'engage à restituer l'ensemble des matériels et données professionnelles qui lui a été confié. Il est responsable de la suppression de ses données personnelles/privées (fichiers, messages électroniques, …). En aucun cas lors d'un départ, l'utilisateur est habilité à détruire des données professionnelles.

Article 35 - La fin de vie des matériels et informations et le développement durable

La CCPA s'engage à collecter et mettre au rebut d'éventuels équipements informatiques, téléphoniques ou en fin de vie.

Par ailleurs, les documents considérés comme confidentiels doivent faire l'objet d'une destruction avant recyclage.

La CCPA met en place des mesures pour limiter les consommations énergétiques des matériels informatiques tels que la mise en veille automatique et prolongée des ordinateurs et l'extinction des écrans. Les impressions en noir et/ou en recto-verso permettent d'économiser du papier et/ou du toner.

L'utilisateur s'engage à éteindre ses équipements de travail en fin de journée quand il quitte la collectivité.

Article 36 - La sécurité des documents papiers

L'utilisateur s'engage :

- A n'utiliser les documents papiers contenant des données personnelles que dans le cadre de ses missions et sur site, et à ne pas les ramener à son domicile.
- A ne pas laisser de manière apparente des documents contenant des données à caractère personnel lorsqu'il quitte son bureau.
- A ne pas jeter des documents contenant des données sensibles à la poubelle si ce n'est après l'utilisation d'une broyeuse
- A ne pas dupliquer ou récupérer des documents dont il n'a pas la charge.

Article 37 – La sécurité physique

Accès aux locaux

La CCPA détermine la politique de sécurité relative au travail des utilisateurs dans les zones de sécurité. Elle détermine, notamment, les habilitations d'accès du personnel et des tiers aux différentes zones de sécurité en respectant la règle du « moindre privilège ».

Il incombe aux utilisateurs de respecter les directives et les procédures d'accès aux locaux.

Les utilisateurs sont tenus d'accompagner leurs visiteurs tout au long de leur présence dans les locaux de la CCPA, de leur arrivée jusqu'à leur départ.

Sécurité dans les bureaux

Il incombe aux utilisateurs de respecter les principes suivants :

- Les documents et/ou les supports électroniques (clés USB, CD…) contenant des informations sensibles doivent être systématiquement rangés dans les armoires fermées à clé lorsqu'ils ne sont plus utilisés.
- L'utilisateur est tenu, dans la mesure du possible, de fermer à clé son bureau à chaque fois qu'il le quitte. Pour les bureaux partagés, il incombe au dernier utilisateur occupant le bureau de le fermer à clé.

5. Entrée en vigueur de la charte

Article 38 - Publicité

La présente charte, adoptée en date du 23/02/2026, est annexée au règlement intérieur de la Communauté de communes de la plaine de l'Ain et s'impose à tous. Elle pourra être révisée selon les besoins et évolutions réglementaires.

Tout manquement aux règles établies dans cette charte pourra entraîner des sanctions disciplinaires conformément au règlement intérieur et au statut de la fonction publique territoriale.

FIN DU DOCUMENT

Charte d'administration des ressources informatiques

Communauté de communes de la Plaine de l'Ain

Versions du document

Version	Date	Résumé des modifications
V1.0	04/12/2025	Version initiale - Charte des usages numérique « Administrateurs »

Classification	Public	Sensible	Privé	Confidentiel
	X			

Avant-Propos

L'information et les systèmes d'information associés constituent des éléments indispensables au bon fonctionnement et au développement de la Communauté de communes de la Plaine de l'Ain (CCPA), de ses métiers et de ses fonctions et ils contribuent à la réalisation de ses missions de service public.

Dans ce contexte, la bonne administration des données et des ressources les supportant, les transportant ou les traitant, participe directement à la performance et à la bonne réalisation de ces missions.

Les personnels en charge de cette administration, appelés « administrateurs informatiques », disposent de droits d'accès étendus.

Dans l'exercice de leur fonction, ils peuvent être amenés à accéder à des informations ou des données d'autres utilisateurs présentant par ailleurs un caractère confidentiel.

Ils effectuent également régulièrement des actions potentiellement sensibles : changement de mécanismes de protection, création ou modification de comptes utilisateurs et des droits associés, suppression de fichiers, transfert de données, etc.

Toute action de ce type, mal exécutée, peut entraîner de graves conséquences telles que l'indisponibilité de certaines applications et la destruction voire l'altération ou la compromission d'informations essentielles.

En raison de leurs prérogatives, ces personnels jouent un rôle essentiel, requérant discrétion et diplomatie : leur démarche se doit d'être impartiale.

Leurs interventions ne doivent pas outrepasser leurs attributions ni relever d'actions effectuées pour leur propre compte ou par intérêt personnel. Il convient donc de fixer les règles, en particulier de déontologie, à respecter.

La présente charte est destinée à préciser les principes structurant leurs obligations et leurs droits dans le cadre d'actions qu'ils sont amenés à effectuer.

Elle s'inscrit en cohérence et en complément des règles définissant l'utilisation des ressources informatiques de la Communauté de communes de la plaine de l'Ain (CCPA).

Table des matières

Article 1 - Définitions

Le système d'information

Le système d'information de la Communauté de communes de la Plaine de l'Ain comprend :

- Les informations et les données (quelles que soient leurs supports, numériques, papiers, ou les vecteurs de communication oraux, courrier ou réseaux informatiques, …) qui appartiennent ou qui ont été confiées à la CCPA ;
- L'ensemble des moyens informatiques, de télécommunication, de traitement, de conservation et de stockage ;
- Les utilisateurs, partenaires ou sous-traitants qui accèdent au système d'information de la CCPA ;
- Les acteurs qui mettent en œuvre ou administrent le système d'information.

Les utilisateurs du système d'information

Les utilisateurs du système d'information sont les agents ou agents en position d'encadrement, intervenants internes ou externes, tous statuts confondus : permanents, contractuels, stagiaires et intervenants extérieurs temporairement autorisés.

Le Responsable des Systèmes d'Information

Le responsable des systèmes d'information a la charge de la mise en œuvre des dispositifs de traitement de l'information. Ces traitements sont conçus pour répondre aux besoins des métiers de la CCPA dans le respect des règles définies par le RSI. Il possède également le rôle de Responsable Sécurité Système d'Information (RSSI). A ce titre, il a la charge de la définition, de la mise en œuvre de politiques de sécurité du système d'information conformément aux obligations légales, en adéquation avec les besoins de sécurité des directions métiers et ayant pour objectifs la réduction des risques liés à l'usage des outils numériques. Le contrôle de la bonne gestion des risques liés à l'utilisation des données et ressources du système d'information est un point essentiel de sa mission.

Les administrateurs du système d'information

Les administrateurs du système d'information désignent toute personne, (interne, partenaire ou sous-traitante) ayant des droits d'accès privilégiés à des ressources du système d'information (SI) pour réaliser les tâches nécessaires au bon fonctionnement et à la sécurité des systèmes et des données qui lui sont confiées.

Les personnels habilités à administrer le système d'information

Sont concernés :

- Les agents titulaires, apprentis ou personnels contractuels, affectés à des taches d'administration informatique formés et désignés par la direction générale
- Les agents titulaires, apprentis ou personnels contractuels, affectés à des taches d'administration fonctionnelles de logiciels métiers, formés et désignés par leurs responsables hiérarchiques ;
- Les prestataires formés et sous contrats validés et/ou signés par la direction générale.

Ne sont pas concernés :

- Les étudiants en stage dans un cadre scolaire ou universitaire ;
- Les agents titulaires, apprentis ou personnels contractuels ne disposant pas des formations et compétences suffisantes pour occuper une fonction d'administrateur sur les ressources informatiques concernées.

Le Délégué à la Protection des Données (DPO)

Le DPO est le Délégué à la Protection des Données à caractère personnel, il a pour mission l'assistance et le conseil auprès de la direction générale et des directions métiers pour la mise en conformité de la CCPA avec la règlementation pour la protection des données personnelles. Le contrôle de conformité à la réglementation est un point essentiel de sa mission.

Article 2 - Objet de la charte

La présente charte a pour objet de préciser les droits et obligations des administrateurs informatiques dans l'exercice de leur fonction.

Elle s'applique à tout personnel habilité (cf Article 1) par la CCPA à intervenir sur les systèmes d'information de la collectivité.

Elle concerne également toute personne appelée à valider les demandes d'ouverture de droits et d'autorisations appropriés des administrateurs informatiques.

En outre les supérieurs hiérarchiques de ces administrateurs doivent avoir connaissance des exigences de cette charte et doivent aussi les prendre en considération avant d'affecter les autorisations à ces personnes.

Elle se doit, par ailleurs, d'être connue de toute personne impliquée dans :

- Le recrutement de ressources humaines de type administrateurs informatiques
- La passation de contrats avec des sociétés extérieures amenées à intervenir sur le système d'information de la collectivité.

Article 3 - Identification des administrateurs informatiques

Au sein de chaque service concerné, les responsables doivent être informés de l'identité des personnes auxquelles sont attribuées des fonctions d'administrateur informatique.

La fiche de poste ou tout autre document spécifiera le périmètre d'action et les ressources impliquées.

S'agissant des personnels de prestataires extérieurs privés, ces éléments seront précisés dans le contrat.

A sa demande, le Responsable des Systèmes d'Information (RSI) de la CCPA doit être informé de l'identité des administrateurs informatiques, il peut être amené à consulter leur lettre de mission, fiche de poste, fiche descriptive ou éléments significatifs du contrat afin de vérifier la pertinence et le bon usage des accès privilégiés attribués.

Chaque responsable concerné se doit de tenir à jour la liste des administrateurs informatiques placés sous sa responsabilité ainsi que le périmètre de leur champ d'intervention.

Article 4 - Les droits de l'administrateur informatique

En application des consignes qui lui ont été transmises, l'administrateur informatique peut prendre toute disposition nécessaire afin d'assurer le bon fonctionnement et la sécurité des composants des systèmes d'Information dans son périmètre de responsabilité tels que désignés dans sa fiche de poste ou tout autre document qui définit ses missions.

En particulier, il peut :

- Isoler, suspendre ou reconfigurer des comptes utilisateurs, équipements ou applications informatiques pouvant compromettre la sécurité du système d'information ; lorsque la situation l'exige (par exemple, dans le cas où il s'agit de couper l'accès à un site attaqué pour préserver

l'accès aux autres ressources) il demande l'autorisation de son supérieur hiérarchique et du Responsable des Systèmes d'Information ;

- Procéder à des vérifications techniques sur les fichiers et bases de données, la messagerie, les connexions à Internet, les fichiers de journalisation, etc., afin de déceler toute anomalie ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement et à la sécurité des systèmes d'information dans les activités d'administration et d'assistance ;
- Traiter (détection, analyse, éradication, filtrage, etc.) ou s'assurer du traitement de tout flux informatique présentant des risques de sécurité (par exemple : virus, intrusion, utilisation d'un logiciel interdit ou potentiellement dangereux, etc). Si nécessaire, il sera demandé à l'administrateur de faire remonter à son responsable et au RSI, des informations relatives à la sécurité, sous forme de statistiques régulières ou de signalisation ponctuelle. Sur la base de ces données statistiques, l'administrateur peut les alerter relativement à toute utilisation de ressources informatiques qui apparaîtrait comme non conforme à la charte d'utilisation des ressources.

Les limites de l'intervention de l'administrateur informatique sont fixées par la réglementation et les normes en vigueur, par la présente charte et par la fiche de poste ou tout autre document qui définit ses missions. Il ne peut être contraint à enfreindre la loi : ainsi, il doit refuser de faire un contrôle ou une action qui ne respectent pas les obligations légales ou les droits élémentaires des utilisateurs.

Article 5 - Les obligations de l'administrateur informatique

5.1 - Obligation de confidentialité

L'administrateur informatique est soumis à une obligation de confidentialité (secret professionnel) et de non-divulgation liée à ses activités. C'est pourquoi :

- Les permissions d'administration attribuées à un administrateur ne sont utilisées que pour mener à bien les tâches qui lui sont confiées. Il veille à ce que les tiers non-autorisés n'aient pas connaissance de telles informations ;
- L'administrateur prend connaissance des informations contenues dans les systèmes d'information ou donne accès à celles-ci seulement dans le cadre de ses fonctions et/ou sur demande explicite de son responsable ou en son absence du RSI (un résumé succinct de l'action sera consigné) ;
- Le devoir de réserve et le principe de neutralité lui imposent l'interdiction absolue de faire de sa fonction l'instrument d'une propagande quelconque ;
- Les outils mis à sa disposition ne sont utilisés que dans un but professionnel d'administration, supervision, exploitation, maintenance ou assistance ;
- Les seuls cas dans lesquels il autorise un accès aux données personnelles des utilisateurs sont les cas particuliers prévus par la loi, sur demande explicite de l'utilisateur à des fins d'assistance ou lorsque des personnes ont été dûment habilitées et préalablement désignées ;
- Il s'engage à ne pas faire état ni utiliser les informations qu'il peut être amené à connaître dans le cadre de ses fonctions ;
- En cas d'assistance, il ne prend en main, à distance, le poste de travail d'un utilisateur qu'avec l'autorisation explicite de ce dernier et ne se connecte qu'aux seules ressources nécessaires à l'accomplissement de sa mission d'assistance ;
- Il a le devoir de ne pas abuser de ses prérogatives ; les contrôles réalisés doivent être faits non seulement en toute transparence mais aussi de manière proportionnée et adaptée à la finalité présentée à l'utilisateur lors de l'information préalable à ces contrôles ;

- Il s'efforce d'éviter tout conflit pouvant exister entre ses intérêts personnels et ceux du service, il informe sa hiérarchie de tout conflit d'intérêt dans lequel il pourrait être impliqué pouvant altérer l'efficacité de sa mission ;
- Il veille à ce que les logiciels soient utilisés dans les conditions de licences souscrites.
- Il veille au respect des politiques et des directives relatives à la protection des données à caractère personnel et de la loi dite « informatique et libertés ».

5.2 - Continuité des activités d'administration des ressources

En toutes circonstances, la continuité du service et de la mission de l'administrateur doit être assurée.

Il est donc tenu d'assurer le suivi de son poste :

- Il formalise les procédures d'administration des systèmes qu'il gère pour que soit assurée cette continuité de service ;
- Il documente ses actions et interventions de telle sorte que ses collaborateurs ne soient pas dans un état de dépendance en cas d'absence ou lorsqu'il quitte sa fonction ;
- Il collabore et coopère avec le RSI, il est tenu de suivre les procédures préalablement définies.

5.3 - Respect des bonnes pratiques d'administration des ressources

L'administrateur informatique observe strictement les règles de sécurité et les limites fixées à ses interventions :

- Il limite ses actions aux ressources informatiques dont il a la charge et dans le respect de la finalité de sa mission ; par ailleurs, il ne modifie les configurations et les droits d'accès que dans les cas préalablement définis ;
- Il a le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques. De même il s'engage à informer l'utilisateur de toute opération inhabituelle tendant à accéder à ses données personnelles, directes ou indirectes, sur son poste informatique, et des motifs l'y autorisant conformément à l'exercice de ses missions (sauf au cas où la discrétion des opérations est imposée par les autorités judiciaires) ;
- Il ne prend pas ses consignes d'une personne non habilitée et fait remonter auprès de son supérieur direct tel que mentionné dans sa fiche de poste et au RSI toute requête lui paraissant inappropriée ou contraire à la réglementation ; en cas de requête qui lui semblerait non appropriée présentée par sa hiérarchie, il a le devoir d'expliquer à celle-ci les raisons de son opposition ; si cette requête était maintenue, il prévient le RSI ;
- Il observe les procédures de sécurité établies et il veille, selon les possibilités du système administré, à ce que les mécanismes de traçabilité soient actifs et à ce qu'il n'y ait aucune atteinte à l'intégrité des fichiers de journalisation ;
- Dans le cadre de la conduite de sa mission et vis-à-vis des ressources à sa charge (serveurs, bases de données, postes de travail utilisateurs, etc.), il utilise les logiciels faisant partie des standards approuvés par la collectivité. Toute installation de logiciel ne faisant pas partie de ces standards doit faire l'objet d'une autorisation préalable et explicite du RSI.

5.4 - Notification d'incident de sécurité

L'administrateur doit tenir informé le RSI des incidents de sécurité et vulnérabilités du système d'information rencontrés dans l'exercice de sa mission : tentatives d'intrusion, fuite de données, mauvaises habilitations, virus détectés, matériels obsolètes, saturation de ressources informatiques, plan de reprise/continuité d'activité non opérationnel, etc…

D'une manière générale, il doit signaler tout événement, règle de sécurité violée, charte de bon usage non respectée, et toutes autres activités pouvant avoir un impact légal ou réglementaire ou bien induisant un risque (technique, juridique, financier, image de marque…) non négligeable pour la CCPA.

En cas d'incident de sécurité :

- Il informe son supérieur direct et le RSI de toute faille ou incident de sécurité qu'il pourrait découvrir ou dont il pourrait avoir connaissance ; il utilise la chaîne d'alerte quand elle existe ;
- Il coopère avec le RSI en cas d'attaque impliquant un composant du système qu'il administre ;
- Il préserve, conserve et sauvegarde les « traces » nécessaires à la résolution d'un incident et à toute investigation ultérieure.

5.5 - Identification et authentification de l'administrateur

L'administrateur informatique s'assure de la protection des droits d'accès liés à sa fonction.

Il observe les règles de sécurité en vigueur visant à protéger l'utilisation des comptes et des droits privilégiés qui lui ont été attribués.

Il veille notamment à la protection des postes de travail à partir desquels il exerce ses fonctions et à la gestion des identifiants et mots de passe des comptes privilégiés :

- Les mots de passe utilisés pour les opérations d'administration doivent être robustes et changés régulièrement conformément à la politique de sécurité des mots de passe ;
- Il est rappelé que les droits confiés à un administrateur (et par conséquent les couples identifiant/mot de passe associés) sont confidentiels et donc incessibles ;
- Il n'utilise ses comptes privilégiés que pour les activités et besoins directement liés aux tâches d'administration, d'exploitation ou d'assistance dont il a la charge, étant donné que toute action sur les systèmes d'information peut faire l'objet d'une journalisation permettant leur imputabilité.

Des contrôles des traces de connexion ou des sessions des administrateurs informatiques peuvent être effectués par le RSI ou une personne désignée par lui en cas d'incident ou à titre préventif.

5.6 - Sensibilisation et formations des administrateurs informatiques

La Communauté de communes de la Plaine de l'Ain s'engage à sensibiliser et former ses administrateurs informatiques.

Les administrateurs informatiques doivent participer aux formations et sensibilisations qui les concerne.

Les administrateurs informatiques en contact avec les utilisateurs, tels les personnels en charge de l'assistance, doivent participer à la sensibilisation de ces derniers, en rappelant les principes des chartes en vigueur à tout utilisateur semblant les méconnaître, avec l'appui du RSI : En prévenant les utilisateurs des consignes techniques de sécurité à mettre en œuvre afin de préserver les systèmes d'information et les données professionnelles et privées.

5.7 - Respect de l'utilisation privée dite résiduelle

Avant toute intervention sur son poste de travail, chaque fois que cela est possible, les administrateurs invitent l'utilisateur à séparer ses documents personnels/privés de ses documents professionnels et à les mettre dans le répertoire portant la mention « Personnel » afin de respecter l'intimité de sa vie privée.

Article 6 - Respect de la législation et de la présente charte

L'administrateur informatique s'engage à respecter en toute circonstance la législation et les normes en vigueur, ainsi que les règles de la présente charte et celles définissant l'usage des systèmes d'information de la Communauté de communes de la Plaine de l'Ain.

Article 7 - Date d'entrée en vigueur

La présente charte, adoptée en date du 23/02/2026, est annexée au règlement intérieur de la Communauté de communes de la Plaine de l'Ain et s'impose à tous Elle pourra être révisée selon les besoins et évolutions réglementaires.

Tout manquement aux règles établies dans cette charte pourra entraîner des sanctions disciplinaires conformément au règlement intérieur et au statut de la fonction publique territoriale.

FIN DU DOCUMENT

Acte d'engagement de l'administrateur

Merci de retourner le coupon suivant, rempli et signé au RSI de la Communauté de communes de la Plaine de l'Ain dans les 15 jours suivant la réception :

Nom et Prénom : ……..…….

Service : ……..

Fonction : …….

☐ Je déclare avoir lu l'intégralité de la présente charte d'administration des ressources informatiques.

A ……..…….. le ……..…….

(Signature)

Charte d’usage de l’Intelligence Artificielle

Communauté de communes de la plaine de l’Ain

Versions du document

Version	Date	Résumé des modifications
V1.0	17/11/2025	Version initiale - Charte d'usage de l'Intelligence Artificielle

Classification	Public	Sensible	Privé	Confidentiel
	X			

Avant-Propos

L'Intelligence Artificielle (IA) constitue l'une des évolutions technologiques majeures de notre époque. Elle ouvre de nouvelles perspectives pour améliorer l'efficacité, la réactivité et la qualité du service public. Dans le cadre des missions de la communauté de communes de la plaine de l'Ain, elle peut contribuer à mieux informer les usagers, à simplifier certaines tâches répétitives, à accompagner la prise de décision et à soutenir l'innovation locale.

Ces opportunités s'accompagnent cependant de responsabilités. L'IA n'est pas infaillible : elle peut générer des erreurs, reproduire des biais ou être utilisée de manière inappropriée. Son usage doit donc être encadré afin de protéger les usagers, les agents et les élus, tout en respectant les valeurs fondamentales du service public : neutralité, transparence, équité, respect de la vie privée et responsabilité environnementale.

La présente charte a pour objectif de définir les règles claires d'usage de l'intelligence artificielle, applicables à l'ensemble des services de la Communauté de communes de la plaine de l'Ain.

Table des matières

Article 1 - Définitions

Les utilisateurs du système d'information

Les utilisateurs du système d'information (SI) sont les agents ou agents en position d'encadrement, intervenants internes ou externes, tous statuts confondus : permanents, contractuels, stagiaires et intervenants extérieurs temporairement autorisés.

Intelligence Artificielle (IA)

L'Intelligence Artificielle désigne un ensemble de technologies capables d'exécuter des tâches qui nécessitent habituellement des capacités cognitives humaines, telles que l'analyse d'information, la reconnaissance de modèles, l'élaboration de recommandations ou la génération de contenu. L'IA n'agit pas sur la base d'une intention ou d'une compréhension réelle : elle repose sur des calculs, des bases de données et des modèles statistiques.

Modèle d'apprentissage automatique (Machine Learning)

Un modèle d'apprentissage automatique est un système informatique capable d'identifier des tendances, des corrélations ou des comportements à partir de données existantes afin de réaliser des tâches spécifiques telles que le classement de documents, la détection d'anomalies, la prédiction de valeurs. Son fonctionnement repose principalement sur l'analyse de données, sans produire de nouveaux contenus. Ces modèles s'améliorent progressivement et sont entraînés à partir de grandes quantités de données. La qualité, la fiabilité et de la représentativité des données utilisées pour l'entraînement sont des éléments essentiels.

IA générative

L'IA générative est une catégorie particulière de machine learning capable de produire du contenu original, comme du texte, des images, des vidéos, des schémas, du code informatique ou des sons, à partir d'instructions fournies par un utilisateur. Le contenu généré résulte de calculs probabilistes : il peut être cohérent, mais également imprécis, erroné ou biaisé.

Le prompt (Instruction)

Le prompt est la consigne écrite ou orale formulée par un utilisateur pour interagir avec un outil d'IA. Il peut s'agir d'une simple question, d'une demande structurée ou d'un scénario complet. La précision, la neutralité et la clarté du prompt influencent directement la qualité des réponses produites.

Les biais algorithmiques

Les biais algorithmiques correspondent à des erreurs systématiques dans les résultats ou les comportements d'un système d'intelligence artificielle. Ils apparaissent lorsque les données d'entraînement sont incomplètes, incorrectes, non représentatives ou influencées par des stéréotypes culturels, sociaux ou historiques. Ces biais peuvent conduire l'IA à produire des réponses discriminatoires, injustes, inégales ou trompeuses, notamment dans l'évaluation d'informations, l'analyse de profils ou la génération de contenu.

Les hallucinations de l'IA

Une hallucination correspond à la génération d'un contenu inventé, incorrect ou non fondé, présenté comme vrai. Ces réponses erronées peuvent sembler structurées et crédibles, mais ne reposent sur aucune référence factuelle ou vérifiable ; c'est une réponse erronée créée lorsque l'IA manque d'informations fiables ou cherche à combler un manque de données. Les hallucinations rendent indispensable la vérification systématique des informations produites par l'IA avant leur utilisation ou diffusion.

Les données à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, 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.

Le Référent Intelligence Artificielle

Le Référent Intelligence Artificielle est l'agent désigné pour assurer le suivi, la conformité et le bon usage des outils IA au sein de la CCPA. Il accompagne les directions métiers dans la mise en œuvre des outils d'intelligence artificielle et veille au respect des règles établies dans la présente charte.

Le Délégué à la Protection des Données (DPO)

Le délégué à la protection des données est la personne désignée par la Communauté de communes de la Plaine de l'Ain pour veiller au respect de la réglementation relative à la protection des données à caractère personnel.

Il est associé aux projets et usages impliquant des données à caractère personnel, y compris lorsqu'ils recourent à des outils d'intelligence artificielle, et constitue le point de contact en matière de conformité RGPD

Article 2 - Champ d'application

La charte concerne la totalité des utilisateurs du système d'information de la collectivité et des structures bénéficiant du SI dans le cadre de mutualisation ; agents ou agents en position d'encadrement, élus et intervenants internes ou externes, tous statuts confondus : permanents, contractuels, stagiaires et intervenants extérieurs temporairement autorisés.

Elle s'applique quel que soit les outils d'intelligence artificielles utilisés.

Article 3 – Les principes directeurs

Les principes suivants régissent l'utilisation de l'IA au sein de la collectivité :

- **La primauté de l'humain et la fiabilité des résultats**

L'IA est un outil d'assistance, non une autorité décisionnelle. Les agents et élus demeurent seuls responsables des choix engageant la collectivité. Toute production issue de l'IA doit être relue et validée par un humain.

- **La transparence**

Tout contenu ou service ayant bénéficié d'une contribution de l'IA doit le mentionner explicitement. Les citoyens doivent toujours savoir si une information provient d'un système automatisé.

- **La protection des données**

Les agents ne doivent jamais transmettre à un outil d'IA externe des données personnelles, sensibles ou stratégiques. L'usage doit rester limité à des informations non confidentielles.

- **L'équité et la non-discrimination**

L'IA peut reproduire ou amplifier des biais. La collectivité s'engage à utiliser des outils respectueux du principe d'égalité.

- **La sobriété numérique et l'impact environnemental**

Les technologies d'IA reposent sur des infrastructures énergivores. Leur utilisation doit rester mesurée et justifiée. Cet engagement participe à la transition écologique.

Article 4 – L'encadrement des usages

4.1 Le cadre règlementaire

Tout usage de l'IA doit être conforme aux réglementations en vigueur, notamment :

- La loi Informatique et Libertés : Loi n°78-17 du 6 janvier 1978 modifiée.
- Le Règlement Général sur la Protection des Données (RGPD) : Règlement (UE) 2016/679 du 27 avril 2016.
- La Directive ePrivacy : Directive 2002/58/CE modifiée.
- L'AI Act (Règlement sur l'intelligence artificielle) : Règlement (UE) 2024/1689 du 13 mars 2024.
- Le code de la commande publique et décrets d'application pertinents pour l'acquisition d'outils numériques.

4.2 Les domaines d'application potentiels

L'IA peut, sous réserve de validation par le comité de pilotage IA, être mobilisée dans différents domaines pour renforcer l'efficacité de l'action publique et améliorer la qualité du service rendu aux citoyens. Il est rappelé que tout usage qui n'a pas été expressément validé par le comité de pilotage IA est présumé interdit.

A titre d'exemple, les domaines d'application potentiels suivants sont identifiés :

- Reformulation de textes, résumés de documents, élaboration de plans et productions linguistiques.
- Analyse et statistiques : appui dans la production de synthèses de données chiffrées facilitant la compréhension et la prise de décision.
- Traduction et accessibilité : simplification du langage administratif ou traduction de documents afin d'améliorer l'accessibilité pour tous les usagers.
- Relation aux usagers : assistance automatisée pour répondre aux questions courantes, en complément d'un accueil humain.
- Innovation territoriale : soutien à des exercices de prospective ou de simulation (démographie, économie, aménagement).

4.3 Usages et interdictions

L'usage de l'IA est strictement encadré. Les usages à risque, ci-dessous listés, sont formellement interdits :

- Décider automatiquement d'une mesure affectant un usager sans validation humaine.
- Traiter ou divulguer des données à caractères personnelles (ex : données nominatives, médicales, dossier RH…), ainsi que des données jugées sensibles ou stratégiques pour la collectivité.
- Produire un contenu trompeur, discriminatoire ou contraire aux valeurs du service public.
- Utiliser l'IA à des fins personnelles, politiques ou commerciales étrangères aux missions de la collectivité.
- Employer l'IA pour manipuler l'opinion publique ou influencer illégitimement un scrutin.
- Générer des contenus attentatoires à la dignité humaine ou à la neutralité administrative.

Tout usage compromettant la sécurité, l'éthique, la confidentialité ou la neutralité du service public est interdit, même s'il n'apparaît pas explicitement dans cette liste.

4.4 Protection des données à caractère personnel

Tout usage d'un outil d'intelligence artificielle impliquant, directement ou indirectement, des données à caractère personnel doit respecter la réglementation applicable en matière de protection des données ;

Tout projet, expérimentation ou usage d'IA susceptible d'impliquer des données à caractère personnel est examiné en lien avec le délégué à la protection des données (DPO) ;

Le cas échéant, cet usage peut nécessiter la réalisation d'une analyse d'impact relative à la protection des données (AIPD), conformément au règlement (UE) 2016/679 (RGPD).

4.5 Les outils

Seuls les outils d'intelligence artificielle expressément validés par la collectivité peuvent être utilisés dans un cadre professionnel. L'utilisation d'outils d'intelligence artificielle via des comptes personnels ou d'outils non validés par la collectivité est interdite, y compris lorsque ces outils sont accessibles gratuitement ou en ligne. La liste des outils d'intelligence artificielle autorisés est définie et actualisée périodiquement par la collectivité. Elle est tenue à jour par le référent IA.

Article 5 – Les bonnes pratiques d'utilisation de l'IA

5.1 Réflexes à adopter

L'utilisation responsable de l'IA suppose des réflexes quotidiens. La liste ci-dessous, présentant quelques bonnes pratiques d'utilisation et écueils à éviter, est indicative et pourra évoluer :

- Formuler des demandes claires et neutres ;
- Ne pas entrer des données personnelles dans un outil non validé ;
- Limiter les informations partagées au strict nécessaire ;
- Relire attentivement les productions (Ne pas copier un texte généré par IA sans vérification) ;
- Croiser les résultats avec des sources fiables ;
- Utiliser uniquement les outils validés par la collectivité.
- Ne pas considérer l'IA comme infaillible ;
- Ne pas déléguer systématiquement des tâches nécessitant un discernement humain ;
- Ne pas utiliser l'IA comme substitut à la réflexion collective ;
- Mentionner l'usage de l'IA dans un document officiel ;
- Ne pas multiplier les requêtes sans nécessité, générant une consommation énergétique inutile.
- Consulter le référent IA en cas de doute ;

5.2 Discernement et responsabilité

Avant toute diffusion de contenu généré par l'IA, chaque agent doit se demander :

- La collectivité peut-elle assumer la responsabilité de ce contenu ?
- Le contenu généré par IA est-il conforme aux valeurs de la collectivité ?
- L'usage est-il proportionné au besoin réel ?

Article 6 - Gouvernance de l'IA

6.1 Instances de pilotage

Afin d'assurer un pilotage clair, transparent et sécurisé de l'usage de l'IA au sein de la collectivité, un Comité de pilotage IA (COPIL-IA) est créé. Ce comité, placé sous l'autorité du Directeur Général des Services (DGS), se réunit périodiquement ; il est chargé de :

- Rendre les arbitrages stratégiques liés à l'utilisation de l'IA au sein de la collectivité
- Définir les usages tolérés (Tout cas d'usage non validé par le comité de pilotage IA est présumé interdit)
- Gérer les risques associés à l'IA

Pour l'accompagner dans cette démarche, un référent IA est nommé. Il constitue l'interlocuteur de référence en matière d'usages de l'IA au sein de la collectivité.

Ainsi, le référent IA organise les réunions du comité de pilotage, assure le suivi des décisions, accompagne les agents dans leurs usages et le choix des outils d'IA, diffuse les bonnes pratiques et signale les risques juridiques ou techniques.

Le délégué à la protection des données (DPO) est associé aux travaux du COPIL-IA pour les sujets impliquant des données à caractère personnel.

Il intervient à titre consultatif.

Son avis est sollicité en amont de la validation de tout usage d'intelligence artificielle susceptible d'impliquer des données à caractère personnel, notamment dans le cadre de l'analyse des risques et, le cas échéant, de la réalisation d'analyses d'impact

6.2 Gestion des incidents liés à l'intelligence artificielle

Tout incident lié à l'utilisation d'un outil d'intelligence artificielle (notamment erreur grave, production de contenu inapproprié, biais manifeste, dysfonctionnement technique, fuite ou exposition de données, impact négatif sur un usager ou un agent) doit être signalé sans délai au référent Intelligence Artificielle.

Lorsqu'un incident est susceptible d'impliquer des données à caractère personnel, il doit également être signalé sans délai au délégué à la protection des données, joignable à l'adresse suivante : dpo@cc-plainedelain.fr.

Lorsqu'un incident est susceptible de constituer une violation de données à caractère personnel, il est traité conformément à la procédure interne de gestion des violations de données personnelles et à la réglementation applicable, notamment en ce qui concerne les obligations de notification auprès de la CNIL et, le cas échéant, d'information des personnes concernées.

Les incidents font l'objet d'une analyse afin d'identifier leurs causes, d'évaluer leurs impacts et de définir les mesures correctives ou préventives appropriées.

Le comité de pilotage IA est informé des incidents significatifs et des actions mises en œuvre, afin d'adapter, le cas échéant, les règles d'usage, les outils autorisés ou les mesures de prévention.

Article 7 - Engagements de la collectivité

La Communauté de communes de la plaine de l'Ain s'engage à :

- Former régulièrement les agents aux usages responsables de l'IA.
- Sélectionner et valider des outils conformes à la réglementation en vigueur.
- Mettre à disposition un référent Intelligence Artificielle pour accompagner les usages.

- Évaluer périodiquement les bénéfices, risques et impacts environnementaux liés à l'IA.
- Adapter la présente charte en fonction des évolutions technologiques et réglementaires.

Article 8 - Date d'entrée en vigueur

La présente charte, adoptée en date du 23/02/2026, est annexée au règlement intérieur de la Communauté de communes de la plaine de l'Ain et s'impose à l'ensemble des agents. Elle pourra être révisée selon les besoins et évolutions réglementaires.

Tout manquement aux règles qu'elle définit est susceptible d'entraîner l'application de mesures disciplinaires, dans les conditions prévues par le règlement intérieur et par le statut de la fonction publique territoriale.