

L'ESSENTIEL

Tous les agents en activité ont droit à des congés annuels. Ces congés sont calculés sur la base du nombre de jours de travail par semaine. La pose des congés annuels peut générer ou non l'acquisition de jours de congés supplémentaires, appelés jours de fractionnement.

Selon le nombre d'heures travaillées par semaine, l'agent a droit, ou non, à des ARTT.

■ LE PRINCIPE

Les congés :

Les congés annuels :

Tout agent en activité a droit, pour une période de référence du 1^{er} janvier au 31 décembre, à un congé annuel d'une durée égale à **cinq fois ses obligations hebdomadaires de service**. Cette durée est appréciée en jours ouvrés.

Exemples :

Un agent travaillant 5 jours par semaine dispose de 5×5 : 25 jours de congés annuels

Un agent travaillant 4.5 jours par semaine dispose de 4.5×5 : 22.5 jours de congés annuels

Les jours de fractionnement :

Lorsque les agents utilisent leur droit à congés annuels dans la période comprise entre le 1^{er} janvier et le 30 avril et le 1^{er} novembre et le 31 décembre, ils bénéficient de congés supplémentaires :

- Pour 5, 6, ou 7 jours pris en dehors de la période, ils bénéficient d'1 jour supplémentaire ;
- Pour 8 jours ou plus pris en dehors de la période, ils bénéficient de 2 jours supplémentaires.

Les ARTT :

Le nombre de jours supplémentaires de repos prévus au titre de la réduction du temps de travail est calculé en proportion du travail effectif accompli au-delà de la durée légale du travail, 35 heures par semaine.

LES DROITS & ENJEUX

Les congés :

Durée hebdomadaire de temps de travail	Nombre de jours travaillés par semaine (Rythme de travail)	Nombre de congés annuels
36h30	5	25
	4.5	22.5
	4	20
36h00	5	25
	4.5	22.5
	4	20
35h00	5	25
	4.5	21.5*
	4	18.5*

*Nombre de jours de congés légaux minorés des jours complémentaires à travailler pour respecter la durée annuelle légale de temps de travail.

Les ARTT :

Durée hebdomadaire de travail	Rythme de travail (nombre de jour travaillés)	Nombre jour de ARTT temps plein	Nombre de jours de ARTT à temps partiel				
			90%	80%	70%	60%	50%
36h30	5	9	8,00	7,00	6,50	5,50	4,50
	4,5	7,5	7,00	6,00	5,50	4,50	4,00
	4	6	5,50	5,00	4,00	3,50	3,00
36h00	5	6	5,50	5,00	4,00	3,50	3,00
	4,5	4,5	4,00	3,50	3,00	2,50	2,50
	4	3,5	3,00	3,00	2,50	2,00	2,00
35h00	PAS DE ARTT						

Lorsque les agents sont à temps partiel, pour faciliter la gestion des jours d'absence, le nombre déterminé peut être arrondi à la demi-journée supérieure.

A temps partiel thérapeutique, les agents ne génèrent pas de ARTT.

En cas de maladie, les jours de ARTT sont réduits comme suit, par nombre de jours d'absences sur une année :

Durée hebdomadaire de travail	Rythme de travail (nombre de jour travaillés)	Nombre jour de ARTT temps plein	Nombre de jours de ARTT déduit par nombres de jours d'absence				
			1	2	3	4	5
36h30	5	9	26	52	78	104	130
	4,5	7,5	31	62	93	124	155
	4	6	38	76	114	152	190
36h00	5	6	38	76	114	152	190
	4,5	4,5	51	102	153	204	255
	4	3,5	66	132	198	264	330

Jours d'absence

LA PROCÉDURE INTERNE

Les congés :

Le rythme de travail doit être signalé au responsable hiérarchique et au gestionnaire en charge des congés à la DRH.

Les jours de congés annuels et les jours de fractionnement acquis au titre de l'année A peuvent être posés jusqu'au 31 janvier de l'année A+1.

Les membres du personnel chargés de famille bénéficient d'une priorité pour le choix des périodes de congés annuels.

L'absence de service ne peut excéder 31 jours consécutifs sauf cas particulier du personnel autorisé à bénéficier d'un congé bonifié (personnel originaire d'outre-mer).

Les ARTT :

Les jours d'ARTT non pris au titre d'une année ne peuvent être reportés sur l'année suivante. Ils peuvent, le cas échéant, être déposés sur le compte épargne temps.

▪ QUELQUES CONSEILS

Pour les agents à Temps Partiel Thérapeutique, le calcul des droits à congés est réalisé sur la base du rythme de travail habituel. Les congés doivent donc être posés comme à temps plein.

Vous devez signaler tout changement de votre rythme hebdomadaire ou passage à temps partiel (sur autorisation, de droit ou thérapeutique) à votre responsable hiérarchique et au gestionnaire en charge des congés à la DRH.

Un agent en maladie génère des droits à congés annuels.

Un agent en arrêt maladie pendant sa période de congés annuels voit ses congés reportés.

Cadre juridique

- Article L621-1 du Code général de la fonction publique
- Loi n°2019-828 du 6 août 2019 de transformation de la fonction publique
- Décret n°85-1250 du 26 novembre 1985
- Circulaire ministérielle NOR COTB1117639C

Pour toutes questions, vous pouvez envoyer un mail à l'adresse mail :

absences@gaillac-graulhet.fr

CIBLE

Agents fonctionnaires ou stagiaires relevant du régime spécial (CNRACL) et agents contractuels

L'ESSENTIEL

Tous les agents en activité, qu'ils soient fonctionnaires ou contractuels, qu'ils exercent à temps complet, temps non complet ou temps partiel, ont droit à un congé pour l'arrivée d'un enfant placé en vue de son adoption et à un congé d'adoption.

▪ **LE PRINCIPE**

Dans le cadre d'une adoption d'un enfant en France ou à l'étranger, les agents peuvent bénéficier de congés spécifiques.

▪ **LES DROITS ET ENJEUX**

Les bénéficiaires :

En cas d'adoption, le congé pour l'arrivée d'un enfant placé en vue de son adoption est accordé de droit à l'agent qui en fait la demande.

De plus, le congé d'adoption est accordé à l'un ou l'autre des parents adoptifs. Si les deux parents sont fonctionnaires en poste, le congé pourra être réparti entre les deux agents.

La durée des congés :

Congé pour l'arrivée d'un enfant placé en vue de son adoption

Le congé de **3 jours** est obligatoirement pris de manière continue ou fractionnée à l'occasion de chaque arrivée d'un enfant. Il doit être pris dans une période de 15 jours entourant l'arrivée de l'enfant adopté au foyer.

Congé d'adoption

Pour l'adoption d'un seul enfant :

- Portant le nombre d'enfants du ménage à **un** ou **deux** enfants : **16 semaines**
- Portant le nombre d'enfants du ménage à **trois** ou **plus** enfants : **18 semaines**

Nota : lorsque les deux conjoints sont fonctionnaires en activité, cette période de 16 ou 18 semaines est augmentée de 25 jours en cas de répartition du congé d'adoption entre les deux parents adoptifs.

Pour l'adoption de plusieurs enfants :

- Le congé est de **22 semaines**.

Nota : lorsque les deux conjoints sont fonctionnaires en activité, cette période de 16 ou 18 semaines est augmentée de 32 jours en cas de répartition du congé d'adoption entre les deux parents adoptifs.

Néanmoins, la durée du congé réparti entre les deux parents ne peut excéder pour chaque parent les durées mentionnées ci-dessus : 16, 18 ou 22 semaines selon le cas.

Le congé d'adoption débute à la date d'arrivée de l'enfant au domicile. Néanmoins, il est possible de le débiter au maximum 7 jours avant son arrivée. Il est également possible de le faire débiter juste après le congé de trois pour l'arrivée d'un enfant placé en vue de son adoption.

La situation de l'agent pendant les congés pour l'arrivée d'un enfant placé en vue de son adoption et le congé d'adoption :

Les agents conservent l'intégralité de leur rémunération. Les congés pour l'arrivée d'un enfant placé en vue de son adoption étant considérés comme une période de service effectif, les agents bénéficient de l'intégralité de leurs congés annuels. En revanche, durant cette période ils ne génèrent pas de ARTT.

▪ LA PROCEDURE INTERNE

Congé pour l'arrivée d'un enfant placé en vue de son adoption	Congé d'adoption
Transmission de la demande* au service santé et protection sociale par courrier ou par mail : absences@gaillac-graulhet.fr La demande indique : • La date de l'arrivée de l'enfant, • Les dates prévisionnelles du congé <i>*Accompagnée de tout document attestant l'adoption de l'enfant</i>	Transmission de la demande* au service santé et protection sociale par courrier ou par mail : absences@gaillac-graulhet.fr La demande indique : • La date de l'arrivée de l'enfant, • Les dates prévisionnelles du congé <i>*Accompagnée de tout document attestant l'adoption de l'enfant et précisant la date d'arrivée de l'enfant au foyer et d'une déclaration du conjoint adoptant attestant qu'il ne bénéficie pas d'un congé d'adoption ou que le congé est réparti entre les deux fonctionnaires adoptants.</i>

▪ QUELQUES CONSEILS

Cadre juridique :

- Article L. 631-8 du Code Général de la Fonction Publique
- Articles L 331-3 à L331-6 et R331-5 à R331-6 du Code de la sécurité sociale
- Articles 10 et 11 du décret n° 88-145 du 15 février 1988 modifié relatif aux agents contractuels de la fonction publique territoriale
- Circulaire DGCL n° NOR : FPPA9610038C du 21 mars 1996 relative au congé de maternité ou d'adoption et aux autorisations d'absence liées à la naissance pour les fonctionnaires et agents de la fonction publique territoriale
- Circulaire DGCL n° 78-153 du 29 mars 1978 relative à l'application de la loi n°76-617 portant diverses mesures de protection sociale de la famille : congé d'adoption, congé postnatal et recul de la limite d'âge applicable au recrutement par concours des agents de catégorie A en faveur des femmes élevant ou ayant élevé un enfant
- Article 8 du décret n° 92-1194 du 4 novembre 1992 modifié fixant les dispositions communes applicables aux fonctionnaires stagiaires de la fonction publique territoriale

Pour toutes questions vous pouvez envoyer un mail à l'adresse mail : absences@gaillac-graulhet.fr

Envoyé en préfecture le 17/02/2026

Reçu en préfecture le 17/02/2026

Publié le 17/02/2026

ID : 081-200066124-20260209-31_2026-DE



CHARTRE DES USAGES NUMÉRIQUES

Sommaire

1.	Champ d’application de la charte	2
1.1	Les utilisateur·rices concerné·es	2
1.2	Les outils et services numériques	2
2.	Les raisons, l’intérêt et la portée d’une charte des usages numériques.....	2
3.	L’utilisateur au sein de la Communauté d’Agglomération Gaillac-Graulhet.....	3
3.1	Responsabilité et obligation de vigilance	3
3.2	Conditions d’accès au système d’information	4
3.3	Confidentialité des données	5
3.4	Mail pour Tou·tes	6
3.5	Le nommage des fichiers	6
3.5.1	La procédure interne de nommage.....	6
3.5.2	Le cadre juridique	7
3.6	Matériel confié.....	7
3.7	Les logiciels à disposition des utilisateur·rices	8
3.8	Données et fichiers	9
3.9	Utilisation de l’Intelligence Artificielle.....	9
3.10	Communication écrite	10
3.10.1	Messagerie électronique	10
3.10.2	Présence sur les réseaux sociaux	11
3.10.3	Messagerie instantanée.....	12
3.11	Utilisation d’Internet	12
3.12	Utilisation des téléphones fixe et mobile.....	13
3.13	Utilisation des dispositifs d’impression	14
3.14	Droit à la déconnexion	14
3.15	Gestion des absences.....	15
3.15.1	Cas de l’absence planifiée	15
3.15.2	Cas de l’absence soudaine et imposée (force majeure)	16
3.16	Le droit syndical	16
3.17	Départ de la collectivité	16
4.	L’administrateur·rice du système d’information et de communication	17
4.1	L’analyse et contrôle de l’utilisation des ressources	17
4.2	Le respect de la vie privée	18
4.3	Le respect de la légalité des usages des TIC.....	18

1. Champ d'application de la charte

1.1 Les utilisateur·rices concerné·es

La présente charte s'applique à tout·e agent·e, élu·e ou personne qui, ayant un lien de droit statutaire ou contractuel avec la collectivité, est amené·e à utiliser les outils numériques mis à disposition par cette dernière, pour satisfaire à ses missions.

1.2 Les outils et services numériques

Les outils et services numériques englobent les équipements informatiques, électroniques et téléphoniques de la collectivité, interconnectés ou non entre eux. Il s'agit notamment :

- Des ordinateurs (fixes ou portables) ;
- Des périphériques y compris clés USB, assistants personnels, réseaux informatiques (serveurs, routeurs et connectiques) ;
- Des photocopieurs, imprimantes et scanners ;
- Des téléphones, smartphones, tablettes et clés Télécom ;
- Des logiciels, fichiers, données et bases de données ;
- Des systèmes de messagerie ;
- Des connexions internet, intranet, extranet et abonnements à des services interactifs.

2. Les raisons, l'intérêt et la portée d'une charte des usages numériques

- Parce qu'elle entend respecter et faire respecter les lois et règlements qui encadrent les activités numériques ;
- Parce qu'elle se doit de sauvegarder l'intégrité de son système informatique, son bon fonctionnement et le respect de la confidentialité des données détenues dans ses services ;
- Parce qu'elle veut organiser la sécurité juridique, eu égard aux éventuels recours liés à des dommages causés par les agents dans l'accomplissement de leurs missions ;
- Parce qu'elle souhaite promouvoir largement l'usage d'outils informatiques modernes et efficaces sur une base de confiance et de responsabilité partagées ;

La Communauté d'Agglomération Gaillac-Graulhet :

- Décide que la présente charte s'impose à tous les utilisateur·rices ;
- Rappelle à tous les utilisateur·rices de ses outils et services numériques que certains usages sont pénalement répréhensibles, que d'autres peuvent nuire au bon fonctionnement

du réseau ou sont susceptibles d'engager la responsabilité personnelle de l'utilisateur·rice ou celle de la collectivité ;

- Fixe par la présente charte les conditions générales et particulières d'utilisation des moyens et ressources informatiques et de télécommunication mis à disposition par la collectivité ;
- Porte en parfaite transparence à la connaissance des utilisateur·rices les dispositifs mis en place pour garantir la sécurité des systèmes et des données.

Cette charte régit l'utilisation des outils et services numériques. Elle comprend les obligations tant des utilisateurs internes ou externes de la Communauté d'Agglomération Gaillac-Graulhet que des administrateur·rices des systèmes d'information.

Les marchés ou contrats conclus entre la collectivité et tout tiers ayant pour but ou pour conséquence de donner accès aux ressources de la collectivité, devront stipuler que ces tiers utilisateurs s'engagent à prendre connaissance de la présente charte et à la respecter scrupuleusement.

Le Comité de Gouvernance Numérique veille à la mise en œuvre, au suivi et à l'évolution de la charte . Il est composé à minima du·de la Vice-Président·e en charge du numérique, des membres du Comité de Direction Générale et du·de la responsable des systèmes d'information, auxquels sont associés pour ce sujet le·la responsable des ressources humaines, le·la responsable juridiques, le·la·les délégué·es à la protection des données Personnelles.

3. L'utilisateur au sein de la Communauté d'Agglomération Gaillac-Graulhet

3.1 Responsabilité et obligation de vigilance

Les utilisateur·rices des outils numériques sont responsables de l'usage rationnel et loyal des ressources informatiques et du réseau auxquels ils ont accès et contribuent à leur sécurité.

L'utilisation des outils informatiques et des moyens d'information et de communication mis à la disposition des agent·es doit être exclusivement professionnelle, sauf autorisation préalable de la Direction. Si une telle autorisation devait être accordée, l'usage personnel qui en résulterait devrait être occasionnel et raisonnable, tant dans la fréquence que dans la durée, conformément à la législation en vigueur et ne pas porter atteinte à la sécurité et à l'intégrité du système d'information, des données professionnelles ou à caractère personnel traitées au sein de la collectivité ou encore à l'image de la collectivité, et plus largement à celle de la fonction publique.

À ce titre, chaque utilisateur·rice s'engage à prendre soin des matériels et des installations informatiques mis à leur disposition. Il signale tout dysfonctionnement ou anomalie qu'il constate, toute erreur d'utilisation pouvant entraîner des conséquences dommageables : il contacte pour cela sans délai le Service des Systèmes d'Information (SSI) au 05 63 83 61 72 ou par mail : support@gaillac-graulhet.fr

L'accès à certains éléments du système d'information est protégé par **des paramètres de connexion requérant un identifiant et un mot de passe. Ces paramètres sont personnels à l'utilisateur-riche et doivent être gardés confidentiels.**

Ces éléments doivent être mémorisés par l'utilisateur-riche et ne pas être conservés, sous quelque forme que ce soit. Ils ne doivent pas être transmis à des tiers ou être aisément accessibles. Il est fortement déconseillé d'enregistrer vos mots de passe dans le navigateur internet. Le service informatique se réserve le droit de retirer les droits d'accès et/ou de mettre en place une solution de remplacement. Il est préférable de les saisir à chaque accès et ne pas les conserver en mémoire dans le système d'information.

Lorsqu'ils sont choisis par l'utilisateur-riche, les paramètres doivent respecter un certain degré de complexité, conformément aux recommandations de l'[ANSSI](#), et être modifiés régulièrement.

Les utilisateur-rices ne doivent jamais utiliser (ou communiquer) leurs identifiant et mot de passe professionnels pour accéder à un réseau, un service ou une application qui serait étranger à la Communauté d'Agglomération Gaillac-Graulhet.

3.2 Conditions d'accès au système d'information

Le droit d'accès aux ressources informatiques et de télécommunication de la collectivité est conditionné au respect des termes de cette charte.

Les accès informatiques sont personnels, uniques, incessibles et temporaires. Ils cessent avec la disparition des raisons qui ont motivé leur attribution.

Par ailleurs, l'étendue des ressources informatiques auxquelles les utilisateur-rices ont accès peut être limitée en fonction des besoins réels et des contraintes imposées par le partage de ces ressources avec d'autres utilisateur-rices.

Le droit d'accès peut être suspendu, par mesure conservatoire de l'autorité hiérarchique ou par le service SI si le comportement d'un-e utilisateur-riche n'est plus compatible avec les règles énoncées dans la présente charte.

Les accès sont strictement personnels et confidentiels, ainsi :

- Quand l'utilisation d'un système informatique implique l'ouverture d'un compte nominatif, l'utilisateur-riche ne doit pas se servir, pour y accéder, d'un autre compte que celui qui lui a été attribué par l'administrateur habilité. Il ne doit pas chercher à masquer sa véritable identité ;
- Tout besoin d'autorisation nouvelle doit faire l'objet d'une demande à la hiérarchie habilitée et ne peut justifier l'usurpation de l'identité informatique d'autrui, avec ou sans son consentement ;
- L'utilisateur-riche s'engage à ne pas mettre à la disposition d'utilisateur-rices non autorisé-es un accès aux applications ou au réseau, à travers un poste de travail professionnel dont il a l'usage.
- Les utilisateur-rices équipées de certificats de signatures électronique sur clé USB s'engagent à ne pas laisser accessible ces certificats, ne pas les copier sur un autre support

et à ne les confier à aucune autre personne (même de confiance), à ne pas divulguer ou noter le code PIN associé à ces certificats.

3.3 Confidentialité des données

Chaque utilisateur·rice accède au réseau par un nom de compte unique (identifiant) auquel est associé un mot de passe confidentiel, dont il-elle est propriétaire.

Toutes les connexions réalisées à l'aide du compte de l'utilisateur·rice engagent sa responsabilité. Il lui appartient donc de ne communiquer son mot de passe à aucune tierce personne, ni même à un agent du service SI, il-elle n'en a pas besoin.

Cette pratique est d'autant plus nécessaire que des outils de synchronisation des identifiants ont été mis en place. Ces outils permettent de donner des accès à la messagerie, à Internet, à des applications (intranet, messagerie, etc...) ou des fichiers avec une identification unique. Dès lors, l'utilisateur·rice confie son mot de passe à une personne, celle-ci pourra accéder à l'ensemble de son dossier personnel et utiliser potentiellement son identité numérique.

Chaque utilisateur·rice s'engage expressément à :

- Ne pas masquer sa véritable identité ;
- Ne pas usurper l'identité d'autrui ;
- Ne pas quitter son poste en laissant une session en cours non verrouillée ;
- Ne jamais « prêter » son mot de passe ;
- Changer immédiatement de mot de passe en cas de doute sur son intégrité ;
- Signaler au SSI toute anomalie constatée.

Des mises en veille automatiques ont été paramétrées sur les postes de travail, protégées par un mot de passe. Pour des raisons de sécurité ces mises en veille automatiques ne doivent pas être supprimées.

Au cours de son activité professionnelle, chaque utilisateur·rice est amené·e à accéder à des données à caractère personnel et à respecter la confidentialité desdites données.

Il-elle doit par conséquent, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du Règlement général sur la protection des données, à prendre toutes précautions conformes aux usages et à l'état de l'article dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Chaque utilisateur·rice s'engage pendant toute la durée de ses fonctions et après la cessation de celles-ci, quelle qu'en soit la cause à :

- Ne pas utiliser les données auxquelles il-elle peut accéder à des fins autres que celles prévues par ses attributions ;

- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- Ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de ses fonctions ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- Prendre toutes précautions conformes aux usages pour préserver la sécurité physique et logique de ces données ;
- S'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- En cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

3.4 Mail pour Tou·tes

La communauté d'Agglomération a mis en place le « Mail pour tou·tes », il s'agit d'une adresse électronique professionnelle mise à disposition des agent·es non-équipé·es d'outil informatique.

Cette adresse e-mail professionnelle vous permettra de recevoir des informations importantes de la part de l'Agglomération et de vous connecter à un ensemble de services, progiciel RH pour la pose de vos congés, le coffre-fort électronique individuel l'extranet et autres outils collaboratifs, etc.

Pour l'obtenir, deux critères :

- Être non informatisé ;
- Avoir un contrat de plus de six mois.

Cette adresse étant professionnelle, lors du départ d'un·e agent·e de la collectivité, celle-ci est automatiquement supprimée immédiatement après son départ.

3.5 Le nommage des fichiers

Le traitement des archives numériques vise à conserver l'information validée et pertinente pour préserver les intérêts des citoyen·nes et de la collectivité.

3.5.1 La procédure interne de nommage

Le nom d'un fichier est approprié lorsque la lecture seule de ce nom est suffisante pour en identifier son contenu sans devoir l'ouvrir

La longueur du nom d'un fichier ne doit pas excéder les 30 caractères, extension incluse.

- **Sujet** - Il s'agit du sujet principal traité au sein du document ; - Il découle d'une analyse du document. - Il peut être qualifié par des mots-clés
- **Typologie documentaire** Le type de document est précisé dans le nom du fichier lorsque nécessaire. PV : procès-verbaux CR : compte-rendu etc.
- Exprimer **les dates** selon le format AAAA-MM-JJ (années, mois, jour).

Commencer par l'année permet de maintenir les fichiers dans un ordre chronologique (Norme ISO 8601)

Indiquer les **versions** des fichiers : Convention_V01... Convention_V58 (***pensez à supprimer les versions intermédiaires lorsqu'elles ne sont plus nécessaires***)

Ex : ODJ_CA_20240917_V1 (ordre du jour du conseil d'agglomération du 17 septembre 2024_V1)

3.5.2 Le cadre juridique

La norme Z42-013 décrit « les mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'en assurer la conservation et l'intégrité ».

3.6 Matériel confié

Chaque utilisateur·rice est responsable du matériel qui lui est confié pour accomplir ses missions. Ce matériel ne constitue en aucun cas un équipement ou un espace privé.

Il·elle doit donc veiller à ne pas effectuer les opérations suivantes qui pourraient entraîner des conséquences directes sur le matériel mis à ma disposition :

- Modifier le fonctionnement, le paramétrage et les caractéristiques de son poste de travail informatique (installation de nouveaux matériels, de logiciels même gratuits, modification de fichiers systèmes, systèmes de cryptage autres que ceux fournis par le SSI) ;
- Transporter son ordinateur portable sans la sacoche qui a été fournie ;
- Retirer les équipements de protections du matériel qui lui est confié ;
- Laisser le matériel informatique confié à la vue de tous (dans sa voiture par exemple) ;
- Laisser les mallettes de visioconférence contenant tout le matériel nécessaire, sans surveillance, dans les salles après utilisation ou encore à dissocier les équipements qu'elles contiennent ;
- Modifier des éléments de configuration tels que veilles animées, curseurs animés, fonds d'écrans dans des limites portant atteinte aux performances de mon poste de travail. Seul les fonds d'écran standard fournis par Microsoft, le constructeur du matériel (s'ils ne contiennent pas de publicité) et la Communauté d'Agglomération Gaillac-Graulhet sont autorisés ;
- Accéder ou essayer d'accéder à des informations privées d'autres utilisateur·rices du réseau. Il est expressément rappelé que l'accès à des informations privées d'autres utilisateur·rices, leur éventuelle destruction ou modification sont des agissements pénalement sanctionnés.

Lors d'une absence prolongée (nuit, week-end), il est demandé, pour terminer proprement ses sessions, d'éteindre son poste de travail. Ce geste procède également d'une démarche écocitoyenne (réduction de la consommation électrique).

Les postes non affectés spécifiquement à un·e agent·e sont dits en libre-service. Ils sont destinés à permettre à plusieurs personnes (sur un même équipement et pour un créneau horaire réservé) de disposer d'un accès partagé au système d'information. Sur ces postes, les utilisateurs adaptent leur

temps de consultation à la nécessité de mutualiser ces équipements. Les mêmes droits et devoirs sont applicables aux utilisateur·rices de ces postes.

Les utilisateur·s qui ont recours à des matériels de mobilité tels que téléphones (mobiles ou smartphones), tablettes ou ordinateurs portables s'engagent à sécuriser d'une part l'accès physique à leurs matériels (par exemple en utilisant le câble antivol) et l'accès aux données qu'ils contiennent par le respect des consignes de sécurité en matière de mot de passe et de mise en veille notamment.

Il·elles sont responsables de la sauvegarde des données présentes sur leur terminal.

Les cybercafés, les hôtels, les lieux publics n'offrent pas de garantie de confidentialité, il convient donc de rester prudent dans les échanges de données réalisés en ces lieux. Lors d'un voyage à l'étranger, il est demandé de ne pas partir avec des données sensibles ou bien alors de chiffrer ces données ou les protéger par un mot de passe.

En cas de perte, de vol ou de détérioration d'équipement informatique ou de télécommunication appartenant à la collectivité, les utilisateur·rices s'engagent à :

- En cas de vol : établir une déclaration auprès du commissariat de police ou de gendarmerie le plus proche et la transmettre au service SI (par mail support@gaillac-graulhet.fr) ;
- En cas de perte : établir une déclaration sur l'honneur de perte validée par le·la responsable hiérarchique et la transmettre au service SI (par mail support@gaillac-graulhet.fr) ;
- En cas de détérioration : établir un rapport circonstancié relatant les faits, validé par le·la responsable hiérarchique et le transmettre au service SI ;
- Avertir sans délai le service SI et le·la responsable hiérarchique ;
- Demander au service SI de modifier immédiatement le mot de passe ;
- Alerter le·la supérieur hiérarchique si l'équipement contenait des données sensibles, confidentielles ou pouvant porter atteinte aux intérêts de la Communauté d'Agglomération Gaillac-Graulhet en cas de diffusion : le service SSI préviendra le·la Délégué·e à la protection des données et pourra, selon l'équipement concerné, effacer les données à distance sur le terminal volé ou perdu.

L'utilisateur·rice s'engage, lorsqu'il·elle quitte la collectivité de façon permanente ou temporaire, à restituer le matériel qui lui a été confié.

La collectivité se réserve le droit de facturer à l'utilisateur·rice :

- Tout matériel non restitué ;
- Tout matériel portant des marques d'usures non liées à un usage normal ;
- Tout matériel dans un état de propreté incompatible avec les missions de l'utilisateur·rice ;
- Tout matériel modifié, que ce soit au niveau matériel ou esthétique.

3.7 Les logiciels à disposition des utilisateur·rices

L'utilisateur·rice n'est pas habilité·e à installer un logiciel ou jeu sur ses équipements (poste de travail, tablette, smartphone...), qu'il soit payant ou gratuit, de quelque origine qu'il soit. Cette installation est réalisée par le SSI sous réserve d'une validation préalable d'opportunité formalisée par le·la responsable hiérarchique auquel·le l'agent·e est rattaché·e.

L'utilisateur·rice n'est pas davantage autorisé·e à utiliser à titre professionnel des services applicatifs gratuits ou des réseaux sociaux qui n'auraient préalablement pas été évalués et validés par la collectivité.

Cette validation technique et sécuritaire revient au service SI qui apprécie :

- Leur conformité à la Réglementation générale européenne sur la protection des données ; (RGPD) et à la Loi « Informatique et Libertés » de 1978 modifiée en vigueur ainsi que les recommandations liées à la protection des données personnelles ;
- La robustesse technique de ces solutions alternatives ;
- Leur capacité à garantir et préserver la confidentialité, l'intégrité et la disponibilité de données transmises ;
- La redondance avec des outils déjà déployés et mis à disposition des agent·es ;
- Leur présence ou non sur [le socle interministériel des logiciels libres](#).

Aucune copie de logiciels n'est autorisée en dehors des copies de sauvegarde. L'utilisateur·rice est informé·e que l'usage et la diffusion de logiciels piratés constituent un délit passible d'amende et d'emprisonnement. Leur diffusion correspond à du recel. Le service SI se réserve la possibilité d'interdire techniquement l'installation de logiciels directement par les utilisateur·rices, voire de les désinstaller.

L'utilisateur·rice ne doit pas chercher à contourner, désactiver ou désinstaller les logiciels de protection et de filtrage.

3.8 Données et fichiers

L'ensemble des données saisies et mises en forme par l'utilisateur·rice dans le cadre de ses missions appartient à la collectivité (hors répertoire désigné ou incluant le mot « Privé », « Personnel » ou « Droit syndical »).

Tous les fichiers de l'utilisateur·rice (hors ceux dans les dossiers décrits comme « Privé », « Personnel » ou « Droit syndical ») doivent être partagés dans le cadre de l'organisation de la collectivité afin d'assurer la continuité du service public. Les fichiers électroniques doivent faire l'objet d'un archivage électronique suivant les mêmes règles de conservation que les documents « papier » de même nature. Les fichiers sur serveurs partagés doivent être triés et organisés.

L'utilisateur·rice est responsable de la sauvegarde des données présentes sur son poste de travail en les déposant sur les ressources gérées par le SSI (arborescence de fichiers, gestion électronique de documents SharePoint) qui bénéficient d'une sauvegarde automatisée.

3.9 Utilisation de l'Intelligence Artificielle

Les utilisateur·rices doivent faire un usage raisonné de l'intelligence artificielle (IA)

Il est essentiel de privilégier une utilisation raisonnée de l'IA en veillant à respecter la confidentialité des données personnelles, à éviter toute diffusion de contenus biaisés ou discriminatoires, et à vérifier la fiabilité des informations générées.

Une charte de l'IA doit préciser le cadre d'utilisation au sein de l'agglomération.

3.10 Communication écrite

3.10.1 Messagerie électronique

3.10.1.1 Comportements interdits

Il est interdit aux utilisateur·rices de stocker, transférer ou diffuser des courriels professionnels ou privés comprenant :

- Des éléments de nature offensante, diffamatoire, injurieuse, à connotation pornographique, sexiste ou raciste, ou toute autre discrimination au sens de la loi ;
- Des incitations à des diffusions en chaîne ou pyramidale.

3.10.1.2 Conservation des messages

Comme l'ensemble des documents produits dans le cadre des activités des agents de la Collectivité (papiers et électroniques), les messages envoyés ou reçus doivent faire l'objet d'opérations d'archivage. Les documents engageants pour la collectivité font l'objet d'une attention toute particulière et doivent être enregistrés dans les dossiers correspondants sur le réseau.

Pour des raisons de fonctionnement (restauration de messages supprimés accidentellement), il existe une sauvegarde des messages échangés. Cette sauvegarde permet de récupérer des messages jusqu'à trois mois maximum.

3.10.1.3 Sécurité

La messagerie est devenue le premier vecteur de propagation des virus. Des outils ont été mis en place pour se prémunir contre ce type d'attaque. Tout message infecté détecté par le système de protection est éradiqué par nettoyage ou traité par le système antispam.

Toutefois, il est impossible de garantir un niveau de sécurité total. Il est donc nécessaire de respecter les précautions simples décrites ci-après :

- Les messages suspects (ayant un objet douteux, un émetteur inconnu, une pièce jointe étrange ou de type « .exe », ...) ne doivent pas être ouverts mais supprimés ou directement transférés au service SI pour analyse ;
- Afin d'assurer un niveau de sécurité maximum, il est strictement interdit de désactiver les systèmes de protection du poste de travail installés par le service SI.

Par ailleurs, les exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau conduisent le service SI à mettre en place des outils de mesure de la fréquence et de la taille des fichiers transmis en pièce jointe aux messages électroniques.

3.10.1.4 Utilisation de la messagerie électronique à des fins personnelles

Il est considéré que tout message reçu ou envoyé à partir du poste de travail mis à disposition de l'utilisateur·rice revêt par principe un caractère professionnel.

L'utilisation de la messagerie à des fins personnelles, lorsqu'elle est rendue nécessaire par les impératifs de la vie courante et familiale, est tolérée si elle est mesurée. Dans ce cas, doit être supprimée toute mention relative à la Collectivité (telle que la signature automatique) ou tout autre indication laissant à penser que le message est rédigé dans le cadre de l'exercice de ses fonctions.

Le message qui comporte en objet la mention « Privé », « Personnel » ou « Droit syndical » bénéficie du droit au respect de la vie privée et du secret des correspondances.

Tout message qui n'est pas identifié comme tel est réputé être professionnel. Cependant, des messages professionnels ne peuvent pas être transformés en correspondance privée permettant ainsi de les communiquer à des personnes extérieures non autorisées.

L'utilisateur·rice est informé·e que, pour des raisons de sécurité, d'organisation ou de gestion de l'encombrement du réseau, le service SI peut mettre en place des dispositifs d'analyse de messages ou des dispositifs visant à limiter la taille des messages échangés. La mise en place de ces dispositifs n'ayant pas pour objet le contrôle individuel des utilisateur·rices, la confidentialité des messages est respectée.

3.10.2 Présence sur les réseaux sociaux

Chaque utilisateur·rice doit être vigilant·e dans son usage des réseaux sociaux qu'ils soient professionnels ou privés.

Il en est ainsi notamment :

- Des outils comme les réseaux sociaux de la collectivité ou les forums,
- Pour des échanges en direct : des outils de visioconférence ou de messagerie instantanée avec vidéo,
- D'autres modalités de recueil d'expression comme les baromètres sociaux.

Les réseaux sociaux internes et externes sont devenus de nouveaux outils de partage et de communication. Ils entrent dans le cadre de la présente charte et sont astreints aux mêmes règles, bonnes pratiques et obligations que les autres systèmes informatiques.

Pour les réseaux sociaux internes (blogs, forums, fils de discussion, tchats, ...) :

- **Valeur ajoutée** : ne contribuer que si l'intervention apporte une valeur ajoutée au thème concerné,
- **Responsabilité** : être responsable de ses contributions, respecter la discrétion et la confidentialité professionnelles associées aux sujets abordés,
- **Tonalité** : être professionnel sur le fond et rester courtois dans les échanges,
- **Contribution** : adapter sa réactivité et ses contributions à son rôle dans les thèmes concernés, ne pas négliger ses autres obligations professionnelles,
- **Respect** : ne pas publier des jugements et considérations sur d'autres personnes.

Pour les réseaux sociaux externes (blogs, Facebook, LinkedIn, Twitter, tchats ...) :

- Ne pas utiliser ses login et mot de passe professionnels,
- Ne pas porter atteinte aux intérêts de la collectivité,

L'attention des agents est attirée sur le caractère public des propos tenus sur les blogs, et sur les risques de porter ainsi atteinte à leurs obligations.

3.10.3 Messagerie instantanée

Comme pour la messagerie électronique, il est interdit aux utilisateurs de stocker, transférer ou diffuser des messages professionnels ou privés comprenant :

- Des éléments de nature offensante, diffamatoire, injurieuse, à connotation pornographique, sexiste ou raciste, ou toute autre discrimination au sens de la loi.
- Des incitations à des diffusions en chaîne ou pyramidale.

Une mauvaise utilisation de la messagerie instantanée peut entraîner des problèmes de sécurité et de confidentialité, il est nécessaire d'être vigilant sur ce qui est partagé.

Séparer les conversations privées et professionnelles en créant un canal de discussion distinct.

Utiliser la messagerie instantanée à bon escient. Les messages instantanés doivent être brefs et concis, dans le cas contraire, la messagerie électronique est à privilégier.

L'utilisation des messages instantanés à des fins professionnelles doit se faire dans le respect des heures de travail et ne doit pas entraîner de notifications en dehors des heures de bureau. Avant d'envoyer un message instantané, il est recommandé de s'assurer de la nécessité d'obtenir une réponse en dehors des heures de travail.

3.11 Utilisation d'Internet

Seuls ont vocation à être consultés les sites Internet ayant un lien direct et nécessaire à l'activité professionnelle et présentant une utilité au regard des missions et fonctions à exercer.

Une consultation ponctuelle et mesurée des sites Internet est admise dès lors que leur contenu :

- N'est pas contraire à l'ordre public ;
- Ne met pas en cause les intérêts et les règles éthiques et déontologiques de la collectivité ;
- Ne constitue pas une incitation à transmettre des données personnelles. Par exemple : données personnelles de type professionnel (adresse électronique de l'agent-e) ou confidentielles (données qui seraient la production et la propriété de la Communauté d'Agglomération Gaillac-Graulhet).

La collectivité sanctionnera toute utilisation abusive, notamment pour le téléchargement de fichiers audio ou vidéo, etc.

Les utilisateur·rices doivent en conséquence respecter expressément les lois et règlements en vigueur sur le territoire français, et notamment de manière non limitative ceux régissant le fonctionnement des services en ligne, le commerce, la vente à distance, la protection des mineur·es, le respect de la personne humaine et de la vie privée, la protection intellectuelle.

Les utilisateur·rices s'interdisent de consulter, télécharger, stocker, diffuser ou rendre accessible, de quelque façon que ce soit, tout site ou message dont le contenu serait de caractère diffamatoire, injurieux, obscène, xénophobe, pornographique ou contraire notamment à la dignité humaine, à

l'ordre public ou constituant une incitation à toute forme d'intolérance ou de malveillance, à la haine raciale, au meurtre, au terrorisme, au proxénétisme, au trafic de stupéfiants, à la contrefaçon, au piratage informatique ou susceptible de constituer une atteinte à la sécurité nationale.

Dans la mesure où des utilisations contrevenant aux règles ci-avant énoncées sont susceptibles d'engager la responsabilité civile et/ou pénale de la collectivité, outre bien évidemment la sienne, l'administrateur·rice du SSI, de par la loi, est tenu à exercer un droit de regard sur l'usage de l'Internet par le personnel et une traçabilité de tous les accès Internet.

3.12 Utilisation des téléphones fixe et mobile

L'utilisation de la téléphonie fixe de la collectivité (au travers d'un poste téléphonique ou d'un « softphone », logiciel de téléphonie installé sur un ordinateur) et mobile est également réservée à des fins professionnelles. Néanmoins, un usage ponctuel de la téléphonie fixe et mobile pour des communications personnelles, hors numéros à tarifs spéciaux et appels vers l'étranger, est toléré à condition que cela n'entrave pas l'activité professionnelle.

Les agent·es sont invité·es à protéger leur messagerie téléphonique par un mot de passe, dont ils assureront la confidentialité. En cas d'absence de l'agent, la ligne téléphonique doit être renvoyée soit vers la ligne d'un·e collègue, soit sur la messagerie téléphonique.

Il faut noter que, pour tout appel téléphonique émis depuis les lignes fixes de la collectivité, les six premiers chiffres sont conservés avec le numéro du poste appelant et la durée de communication pendant douze mois courant à la date de l'exigibilité des sommes dues en paiement des prestations des services de téléphonie (délai prévu à l'article L. 34-2 du code des postes et des communications électroniques).

Les utilisateur·rices doté·es d'un terminal de téléphonie mobile (ou « smartphone ») sont responsables du matériel (son maintien en bon état de fonctionnement, sa protection contre toute détérioration, sa surveillance en situation de déplacement) et de l'usage qui en est fait (nombre, nature, durée des appels, volume des téléchargements ou échanges de données).

L'utilisateur·rice doté·e d'un téléphone mobile doit avoir pris connaissance des limites d'utilisation associées au contrat opérateur, qu'il se trouve au bureau, chez lui, en déplacement ou bien à l'étranger. L'agent·e est tenu·e de vérifier régulièrement son suivi de consommation et d'en tenir compte dans l'utilisation quotidienne de son smartphone.

Les responsables hiérarchiques sont destinataires de l'état des consommations individuelles de téléphonie fixe et mobile (relevés individuels des numéros de téléphone des appels sortants et entrants ou des services de téléphonie utilisés) uniquement en cas d'utilisation manifestement anormale de ces services.

- L'utilisateur·rice doit protéger le téléphone mobile mis à sa disposition par un code d'accès qui lui est personnel ;
- Il·elle vérifie sa consommation téléphonique régulièrement ;
- Il·elle se connecte dès que possible au Wifi qui l'entoure pour préserver sa consommation Data

- Il-elle doit enregistrer une annonce personnalisée professionnelle conviant son-sa interlocuteur-ric(e) à laisser un message ;
- Il-elle privilégiera le mode vibreur plutôt qu'une sonnerie qui pourrait gêner ses collègues quand il-elle travaille dans un espace partagé ;
- Il-elle ne parle pas trop fort s'il-elle n'est pas seul-e ;
- Les dispositifs de type téléphone mobile ou smartphone obéissent aux mêmes règles que tous les autres équipements qui me sont confiés ;

3.13 Utilisation des dispositifs d'impression

L'utilisation des dispositifs d'impression est réservée à des fins professionnelles. Néanmoins, un usage personnel ponctuel et très modéré est toléré à condition que cela n'entrave pas l'activité professionnelle.

Il est à noter que, dans le cadre de l'utilisation d'un dispositif d'impression équipé d'un moyen d'identification de l'agent, des informations sont enregistrées par le système d'information dans un journal électronique. En fonction du dispositif les traces du document imprimé ne sont généralement pas conservées, seules les informations suivantes sont enregistrées : le jour, l'heure, le lieu, l'identité de l'agent, le nom et le type de document imprimé, le nombre de pages et le mode d'impression (noir et blanc, couleur, recto verso). Quelques dispositifs conservent la totalité du fichier d'impression avec tout son contenu (traceur, certaines imprimantes ...).

Les responsables hiérarchiques peuvent être destinataires du journal d'utilisation des dispositifs d'impression de leurs collaborateur-rices. Ces informations ont principalement pour vocation à optimiser et rationaliser le recours aux impressions dans un objectif d'écoresponsabilité mais peuvent aussi être utilisées pour corriger une utilisation inappropriée ou abusive.

- Les utilisateur-ric(e)s doivent privilégier les impressions en Noir & Blanc et en Recto / Verso ;
- La très grande majorité des documents générés électroniquement n'ont pas vocation à être imprimés mais à être partagés par voie numérique (courriel, serveur de fichiers, chat pro, vidéoprojection ...) et les documents telles que les courriels, présentations ne doivent pas être imprimés, sauf cas exceptionnel.
- Les utilisateur-ric(e)s doivent faire appel au service de reprographie pour imprimer de manière écoresponsable tout travail d'impression de plus de 100 exemplaires (plaquettes, brochures, livrets ...);

3.14 Droit à la déconnexion

L'accord cadre sur le télétravail du 13 juillet 2021 donne un cadre clair à toutes les administrations et précise notamment le droit à la déconnexion.

Le droit à la déconnexion peut donc être entendu comme le droit de chaque agent-e de ne pas répondre aux courriels et autres messages en dehors des heures de travail, afin de garantir l'équilibre entre vie professionnelle et vie privée, les temps de repos et de récupération, de réguler la charge mentale et réduire les risques d'épuisement professionnel.

Concernant les courriels et les messages par messagerie instantanée, l'envoi est à éviter en semaine entre 20 h et 7h30, le week-end et les jours fériés, sauf nécessité de service, astreintes et horaires de

travail particuliers (travail le week-end par exemple). Il n'est pas attendu de réponse aux messages sur ces mêmes créneaux. Ce principe est modulé en fonction des cycles de travail pour les agent-es en horaires décalés ou d'astreinte et ne s'applique pas, en cas de gestion de crise.

- Les utilisateur-rices évitent de lire ou d'envoyer des messages entre 20h et 7h30 ;
- Lors de leurs congés les utilisateur-rices doivent paramétrer un message d'absence annonçant leur date de retour et ils ont précisé qui suivait leurs dossiers ;
- Les utilisateur-rices sont en droit de configurer les outils mis à disposition favorisant le droit à la déconnexion (Viva Insight).

3.15 Gestion des absences

3.15.1 Cas de l'absence planifiée

Dans le souci d'assurer la continuité de l'activité, l'utilisateur-riche doit en cas d'absence :

- Renvoyer ses lignes téléphoniques (fixe et mobile) vers un-e collègue et/ou enregistrer un message d'absence ;
- Paramétrer dans sa messagerie électronique un message automatique de réponse, dans lequel il informe l'expéditeur-riche de sa date de retour et lui propose d'adresser sa demande à l'un-e de ses collaborateur-rices ou collègues.

À défaut, le-la directeur-ice ou directeur-ice général-e peut demander au Service SI d'habiliter un-e mandataire provisoire pour accéder aux ressources individuelles informatiques ou téléphoniques de l'agent-e.

La personne désignée provisoirement mandataire de ces accès est tenue à une obligation de réserve et n'est autorisée à ne prendre connaissance que des contenus strictement professionnels de l'agent-e absent-e.

Pareille procédure exclut tout accès aux répertoires et/ou boîtes aux lettres expressément signalés par les agent-es comme lieu de stockage de données personnelles ou syndicales (identifiés par « Privé », « Personnel » ou « Droit syndical »).

Ces démarches permettent d'avoir accès aux données et documents nécessaires à l'activité du service, contenus par exemple sur la messagerie, le répondeur vocal, les fichiers sur le réseau ou les outils collaboratifs.

Les messages identifiés comme personnels ou privés, émis ou reçus par le collaborateur-riche depuis son poste de travail professionnel, ainsi que les fichiers identifiés comme tels et contenus sur le disque dur du collaborateur ne peuvent être ouverts par l'employeur.

En revanche, les messages professionnels émis ou reçus par les utilisateur- s ainsi que les fichiers professionnels contenus sur le disque dur de celui-ci peuvent être librement consultés par l'employeur.

Par conséquent, si le fichier ou le dossier n'est pas notifié comme étant personnel ou relevant du droit syndical, il doit être présumé, par défaut, comme étant professionnel.

3.15.2 Cas de l'absence soudaine et imposée (force majeure)

Dans le cas d'un arrêt non planifié où l'agent ne serait pas en mesure de paramétrer ses lignes téléphoniques ou sa messagerie électronique, la Collectivité désigne un collaborateur·rice ou collègue mandataire et l'habilite à accéder à la messagerie électronique afin de créer le message automatique de réponse susmentionné ou d'accéder aux messages professionnels utiles à la continuité du service et à renvoyer les lignes de l'agent·e absent·e sur celles d'un·e collègue.

3.16 Le droit syndical

L'utilisation de la messagerie, de l'intranet et d'Internet est autorisée aux organisations syndicales représentatives des personnels sous réserve du respect des règles de la présente charte.

En outre, l'utilisation raisonnée de la messagerie leur est autorisée à condition de ne diffuser que des informations et des données d'intérêt général et à caractère syndical.

Les organisations syndicales représentatives des personnels peuvent en revanche transmettre par ce canal des messages personnels à leurs adhérent·es ou à des groupes de contacts pourvu qu'il soit offert aux destinataires la possibilité de se désabonner et ne plus recevoir aucun message. Les destinataires doivent être clairement et préalablement informé·es de cette pratique afin de pouvoir manifester leur accord ou leur opposition à l'envoi de tout message syndical sur leur messagerie professionnelle.

Enfin, la mise en place de ces outils de communication sera effective, sous réserve de l'engagement formel des organisations syndicales représentatives des personnels auprès du Président de la Communauté d'Agglomération Gaillac-Graulhet, de respecter les dispositions précitées.

En cas de manquement à ces règles, le·la Président·e, garant du respect de l'application de la présente charte, se réserve le droit de suspendre l'accès à la messagerie, à l'intranet et l'Internet aux organisations syndicales représentatives.

Tous les fichiers présents dans un dossier « Droit syndical » bénéficient de la protection liée au droit syndical. Il en est de même de tout message qui comportera la mention « Droit syndical » en objet.

3.17 Départ de la collectivité

Lorsqu'un utilisateur quitte la collectivité, les données de celui-ci doivent faire l'objet d'un traitement :

À faire	Délai
Compte de messagerie	Désactivation de la messagerie dans les plus brefs délais sauf autorisation d'accès donnée par écrit par l'agent sortant en précisant qui

	peut accéder aux données et pour quelle durée. Seules les données à vocation professionnelles peuvent être ainsi exploitées.
Comptes et données des appareils numériques	Désactivation de la messagerie dans les plus brefs délais sauf autorisation d'accès donnée par écrit par l'agent sortant en précisant qui peut accéder aux données et pour quelle durée. Seules les données à vocation professionnelles peuvent être ainsi exploitées.
Accès distant	Dans les plus brefs délais suivants le départ
Accès logiciels métiers, fournisseurs	Dans les plus brefs délais suivants le départ
Accès locaux	Dans les plus brefs délais suivants le départ
Accès intranet	Dans les plus brefs délais suivants le départ

Toutes les données de l'agent·e, n'ayant aucune obligation légale d'archivage sont supprimées après le départ de celui-ci. L'agent·e sera supprimé·e de l'annuaire et de l'organigramme après son départ.

4. L'administrateur·rice du système d'information et de communication

Le·la responsable des systèmes d'information, dénommé·e « administrateur·rice », assure la direction de toutes les activités liées à la production, au transport et au stockage des données informatiques. Il·elle peut déléguer tout ou partie de cette fonction à un·e ou des agent·es du service SI.

Il·elle a accès à toutes les données qui s'échangent tant sur le réseau interne qu'avec l'extérieur. Il·elle est tenu·e à un strict respect du secret professionnel et du droit de réserve.

4.1 L'analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau informatique sont analysés et contrôlés dans le respect de la législation applicable et notamment du RGPD.

L'administrateur·rice vérifie que les matériels et logiciels des utilisateur·rices sont conformes aux besoins définis par leur hiérarchie ainsi qu'aux politiques de sécurité définies par le SSI.

Concernant leur usage, il·elle comptabilise les temps de connexion, les sites visités, les volumes téléchargés ainsi que toutes activités relatives à l'usage des ordinateurs et serveurs, de la messagerie

électronique, d'intranet et d'Internet. Le Service des Systèmes d'Information se réserve le droit de réaliser des rapports périodiques non personnalisés, transmissibles par voie hiérarchique.

En cas de détection de comportements non conformes à la charte, l'administrateur·rice peut, après validation par sa hiérarchie, réaliser une surveillance personnelle dont les résultats sont communiqués à l'autorité territoriale.

Dans tous les cas l'administrateur·rice se garde le droit :

- D'effacer, de compresser ou d'isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques ;
- De suspendre à tout moment, et sans avertissement, l'accès aux systèmes d'information (sites Internet notamment), en cas d'inobservation des présentes règles par l'utilisateur, sauf en cas de risque majeur pour la collectivité ;
- De bloquer à tout moment, sans avertissement préalable, l'accès aux sites dont le contenu est jugé illégal ou offensant, sauf en cas de risque majeur pour la collectivité.

4.2 Le respect de la vie privée

Toute personne a droit au respect de sa vie privée et intime. Ce principe a une valeur constitutionnelle et est affirmé par l'article 9 du Code civil. La vie privée relève notamment de l'identité, de la vie familiale, sexuelle et sentimentale, de l'image, du domicile, de la santé, de la situation financière, de la religion ou encore, des convictions politiques.

L'administrateur·rice est donc tenu·e à un strict respect du secret professionnel. La surveillance de l'administrateur·rice ne s'exerce pas sur les dossiers informatiques nommés « Privé », « Personnel » ou « Droit syndical ».

Néanmoins, si dans le cadre de son activité professionnelle, l'administrateur·rice est amené·e à constater des faits graves préjudiciables à la collectivité, il-elle pourra en informer sa hiérarchie sans divulguer le contenu des faits suspects, sauf après une demande écrite de cette dernière.

4.3 Le respect de la légalité des usages des TIC

Sans préjudice de la confidentialité des correspondances, l'administrateur·rice est tenu·e de dénoncer au 250 à la procureur·e de la république les usages illégaux (tels que pédophilie, incitation à la haine raciale, terrorisme) qu'il constaterait dans l'usage des outils TIC.