COMITE TECHNIQUE

Mercredi 4 mars 2020 à 9h30 Espace Coëvrons

COMPTE RENDU PROVISOIRE

Etaient présents :

Représentants du personnel :
Pour la CFDT : Stéphanie DOYE, Guillaume FOURMONT-HAMELIN, Philippe DUTREIX, titulaires, Sophie DUCROCQ, Christine DROGUET, suppléantes.
Pour FO : Elisabeth DUPLEIX remplaçant Jacky REAUTE titulaire.

Représentants de l'administration : Joël BALANDRAUD, Président du CT, Robert GESLOT, François DELATOUCHE, Maurice SUHARD, titulaires, Isabelle DUTERTRE, suppléante.

Assistaient également : Pierre BOUTELOUP, DGS, Marie-Noëlle NEVEUX, responsable RH.

Approbation du compte-rendu de la réunion du 27 nov. 2019

Le compte-rendu de la réunion précédente est approuvé par l'ensemble des membres.

1) Examen du tableau de suivi des avis du comité

Voir document joint (annexe 1).

Il est demandé d'ajouter le restaurant du foyer de jeunes travailleurs le Nymphéa à la liste des établissements conventionnant avec la CC pour la prise en charge directe des repas des personnels en mission « voirie ».

2) Avis sur le projet de charte informatique

Voir document joint (annexe 2).

Ce document, élaboré par le Directeur des systèmes d'information, a pour objet de poser les règles en matière d'utilisation des différents matériels et logiciels informatiques utilisés au sein de la Communauté de communes des Coëvrons et de la Commune d'EVRON (puisque le service Informatique est mutualisé entre les deux entités). Les droits d'accès donnés dépassent cependant le cadre de ces deux entités (par exemple les élus et secrétaires des 31 communes du territoire ont accès à l'Intranet depuis des ordinateurs n'appartenant ni à la CC, ni à EVRON).

Aussi, il semble utile de répertorier dans un document de référence les principales obligations liées à l'utilisation des outils numériques mis à disposition.

Ce document, une fois approuvé par le Conseil communautaire, aura vocation à être annexé au règlement intérieur du personnel et, dès lors, à figurer dans le livret d'accueil des agents. En cas d'extension du périmètre mutualisé, il aura également vocation à s'appliquer aux agents des nouvelles communes intégrant le dispositif.

La représentante FO apporte des compléments par rapport à l'archivage des données à intégrer dans le document. Le projet joint en annexe est la version corrigée après passage en comité technique.

Monsieur DELATOUCHE attire l'attention sur l'importance de la rigueur dans la gestion des mots de passe et dans la diffusion d'une culture de sécurité informatique. Concernant l'archivage, il fait part de son expérience professionnelle au cours de laquelle étaient pratiqués des « cleaning days » : deux fois par an, tous les collaborateurs pendant une même journée avaient obligation de se consacrer à l'archivage physique et électronique de leurs documents. C'était astreignant, mais efficace, car prévu et fixé dans le calendrier annuel.

Monsieur BALANDRAUD estime qu'il y a une interaction à trouver entre archives et informatique.

Avis des représentants du personnel : favorable à l'unanimité

Avis des représentants de l'administration : **favorable à l'unanimité**

3) Avis sur la proposition de valorisation du travail des jours fériés

Régulièrement, la remarque de la différence importante de traitement du travail les dimanches et jours fériés selon que les heures accomplies viennent en plus de l'objectif annuel (heures supplémentaires : IHTS) ou contribuent à atteindre l'objectif annuel (indemnité horaire) est soulignée.

Repères : le montant d'une IHTS de dimanche et jour férié = (salaire horaire de base + 25%) + 66% ; en € cela donne pour un agent dont l'indice de rémunération est IM351, un salaire horaire de base de 10,84 € et un coût majoré avec IHTS de 22,50 €/h.

L'agent dont le jour de dimanche ou férié entre dans son emploi du temps normal pour atteindre son objectif annuel de temps de travail voit son salaire horaire de base majoré de 74 centimes d'euro par heure. Dans le cas précédent, 11,58 €/h contre 10,84 habituellement

Des propositions relatives à la valorisation de certaines heures de dimanches et de certains jours fériés dans le service Tourisme et de certains jours fériés dans le service Patrimoine ont été présentées au Président, lequel souhaite plutôt un traitement identique dans tous les services concernés (Jardin aquatique également).

Aussi, il est proposé de considérer tout jour férié comme un jour de travail supplémentaire, non inclus dans l'objectif annuel des agents (1607 heures). Ainsi, il serait donné le choix aux agents pour le travail **des jours fériés** entre rémunération en IHTS de jours fériés ou récupération heure pour heure ou intégration dans l'objectif annuel avec dans ce cas, une indemnité horaire de 0.74 €/h.

Pour les agents à temps non complet cependant, en l'état actuel de la loi, les heures complémentaires ne sont pas majorées (cela concerne les hôtes de caisse du JA et un agent Tourisme) ; ce point fait l'objet cependant de discussions au niveau national.

Pour les dimanches, des agents n'ont pas le choix, c'est un jour comme un autre sinon ils n'atteignent pas leur objectif annuel ou introduction d'une différence de traitement selon les services.

Les représentants CFDT se déclarent favorables à la mise en place d'une réponse globale, et pas par service.

Monsieur BALANDRAUD précise qu'il y a toujours des particularités selon les services (exemple : le débat national sur la notion de pénibilité).

Sur la proposition que tout jour férié soit considéré comme un jour de travail supplémentaire et donne lieu, soit à récupération heure pour heure ou à versement d'indemnité horaire pour travail supplémentaire de jour férié lorsque les cadres d'emploi et temps de travail le permettent :

Avis des représentants du personnel : favorable à l'unanimité

Avis des représentants de l'administration : **favorable à l'unanimité**

4) Présentation de la proposition de la démarche pour un RIFSEEP plus équitable

Repères : le RIFSEEP n'est pas obligatoire, il est composé de 2 parties : l'IFSE et le CIA

Actuellement (délibération de décembre 2016, complétée en 2018 et 2019) :

L'IFSE est versée mensuellement + 1300 € brut en novembre

Le CIA est versé en avril + entre 0 et 140 € brut en novembre

avec un maximum ne devant pas dépasser le montant annuel de la catégorie du poste (C2 ou C1, B2 ou B1, A3, A2 ou A1)

Afin de rationaliser le régime indemnitaire et dépasser le mode empirique d'attribution actuel sans réel fondement équitable, il est proposé d'amorcer un travail de structuration en amorçant **la réflexion autour de quatre questions** :

1- **Quoi ?** Objectif : clarifier. Travailler sur une proposition « socle » avec un plancher et un plafond pour la part IFSE et une proposition « socle » pour la part CIA

2- **Comment ?** Objectif : prendre en compte l'équité et la reconnaissance professionnelle (*cf.* Projet d'administration). Trouver un espace commun pour apprécier la part indemnitaire liée au poste en lui-même dans chaque catégorie, et la part indemnitaire liée à l'appropriation du poste.

3- **Quand ?** Objectif : impliquer les managers dans le processus d'attribution du régime indemnitaire. Bâtir une procédure d'appréciation du potentiel des agents : périodicité, support, mode de saisine…

4- **Avec qui et pourquoi** ? Objectif : récompenser la performance collective. L'idée est de répartir une enveloppe sur la durée du mandat du Président (6 ans) afin que chaque programme (défini dans la segmentation stratégique jointe en annexe pour information) puisse en bénéficier une fois. Fixer des modalités d'attribution et tester en 2021 avant généralisation ensuite.

Deux autres vigilances sont essentielles :

5- **Pilotage financier et contrôle** : intégration du paramétrage d'ensemble dans la logique du futur pilotage pluriannuel par programme, masse salariale comprise et lien avec d'autres dispositifs.

6- **Cohérence budgétaire et politique RH** : étude de l'impact des propositions tant sur les aspects budgétaires que RH (adéquation avec la politique d'avancement, de mobilité, d'interventions sociales).

La mise en place de groupes de travail regroupant directeurs de service, représentants du personnel et agents volontaires est proposée pour traiter de ces différentes questions

D'un point de vue calendaire, l'appel à candidatures des agents volontaires pourrait être lancé au cours de la réunion des agents de juin, permettant ainsi au Comité technique, d'ici cette date, de produire leurs propres propositions ou contributions quant aux items précités pour les intégrer au travail collectif. Un rendu des propositions est attendu avant la fin du mois d'octobre 2020 avant l'intégration éventuelle des premiers éléments au BP 2021.

Monsieur BALANDRAUD estime que l'objectivité est compliquée dans le sens où elle se heurte aux réalités de chacun et au prisme d'observation choisi.

A propos de la prise en compte de la Performance :

Madame DUTERTRE relate une discussion assez longue tenue lors du conseil d'administration du CDG53 quant à la mise en place d'une prime de performance collective. C'est bien l'idée de se motiver tous qui est recherchée, tout le monde a la prime ou personne. La somme initialement proposée au sein du CDG53 a été au final divisée par deux par le conseil d'administration.

Monsieur DELATOUCHE partage son expérience professionnelle d'un monde différent visant à récompenser chacun à la performance collective :

1- On partageait objectifs quantitatifs, qualitatifs, individuels et collectifs lors d'un entretien individuel ;
2- Un consultant externe avait formé à la revue d'équipe les encadrants afin qu'ils apprécient rationnellement les réalisations et contributions de leurs collaborateurs ; c'était aussi l'occasion de construire des plans de formation. L'appréciation était plus objective et décorrélée de la rémunération ;
3- Les managers étaient impliqués dans la rétribution de leurs collaborateurs.
Les promotions étaient partagées en comité de direction de l'entreprise.

Monsieur DELATOUCHE estime que les élus (vice-présidents a minima) devraient également donner leur avis sur la contribution apportée par les agents.

Monsieur BALANDRAUD soulève la problématique de l'objectivité dès lors qu'une incidence financière est sous-jacente. Il constate que chacun est peu formé à cela. Cependant, depuis un moment, on avance. Le statut des fonctionnaires créé une culture égalitariste complète. Il faut donc faire bien attention que la rétribution de la performance soit comprise et traiter en parallèle les règles d'avancement. Selon lui, les vice-présidents expriment déjà leur position de façon plus ou moins informelle suivant les postes, mais il faut se méfier de la responsabilité finale et ne pas créer d'écarts entre les DG. Le processus de mise en œuvre et d'attribution est aussi important que le résultat final. Il faut de la transparence : savoir où ça va, comment ça vient.

Pour M. BALANDRAUD, il reste important que lors de l'entretien d'évaluation professionnelle annuel, on ne parle pas d'argent ce jour-là.

Les représentants CFDT souhaiteraient avoir une garantie que tout ne soit pas trop mis sur le manager car il peut y avoir antérieurement de l'animosité, un manque de recul et pensent qu'il serait bien qu'il y ait un élu dans la concertation.

Monsieur DELATOUCHE invite à former les managers là-dessus. Selon lui, la puissance de la revue d'équipe est extraordinaire. Dire la contribution de chacun (sans les agents encadrés) est vertueux. Le manager découvre des choses. Il relate l'exemple d'une entreprise de nettoyage où cet exercice était pratiqué une fois par mois. Cela amène à être dans le rationnel et dans le vrai, cela éloigne la crainte du délit de faciès, cela porte sur des arguments étayés qui sont le socle d'un axe de progrès lequel met en lumière les formations nécessaires à l'agent pour s'améliorer.

Madame DUTERTRE rappelle que le rôle du manager n'est pas confortable, toujours au milieu entre les exigences de la hiérarchie et les demandes de la base.

Pour participer aux groupes de travail RIFSEEP : 1 membre du CODIR, 1 membre du CT, 1 élu du CT en préparation + 1 agent ensuite.

5) Information sur modifications du Tableau des emplois permanents au 1er avril 2020.

Des modifications sont apportées au tableau des emplois permanents, à la demande des communes mais aussi pour prendre en compte les mutations internes au sein de la CC qui ont donné lieu à une modification du temps de travail de certains postes.

ENFANCE-JEUNESSE

Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Animateur/trice ALSH référent/e	15 h 30	1		Adjoint d'animation

Modification :

Animateur/trice ALSH référent/e	24 h 00	1	C	Adjoint d'animation

ADMINISTRATION GENERALE

Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Directeur/trice du service	35 h 00	1	A et B	Attachés, rédacteurs : poste pourvu
Archiviste, chargé/e de veille documentaire et communication, animateur/trice du centre de ressources	35 h 00	1	A	Attachés, attachés de conservation du patrimoine : poste pourvu
Assistant/e administratif/ve et financier/e	35 h 00	2	C	Adjoints administratifs

Modification :

ADMINISTRATION GENERALE

Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Directeur/trice du service	35 h 00	1	A et B	Attachés, rédacteurs : poste pourvu
Archiviste : changement d'appellation du poste à la demande de l'agent titulaire	35 h 00	1	A	Attachés, attachés de conservation du patrimoine : poste pourvu
Gestionnaire administratif/ve et financier/e	35 h 00	2	B et C	Rédacteurs, adjoints administratifs

ETAT CIVIL/ACCUEIL EVRON

Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Responsable du service	35 h 00	1	B et C	Rédacteurs, adjoints administratifs : poste pourvu
Secrétaire de mairie / agent d'accueil	35 h 00	1	C	Adjoints administratifs : poste pourvu
Secrétaire de mairie / agent d'accueil (17h30) Gestionnaire des autorisations d'urbanisme (17h30)	35 h 00	1	C	Adjoints administratifs : poste pourvu –
Assistant/e de secrétariat / agent/e d'accueil et d'état civil	35 h 00	3	C	Adjoints administratifs : postes pourvus
Agent/e d'accueil	35 h 00	1	C	Adjoints administratifs : poste pourvu

URBANISME

Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Directeur/trice du service	35 h 00	1	B et C	Rédacteurs, adjoints administratifs : poste pourvu

Gestionnaire des autorisations d'urbanisme	35 h 00	1	B et C	Rédacteurs, adjoints administratifs : poste pourvu
Gestionnaire des autorisations d'urbanisme	17 h 30	1	B et C	Rédacteurs, adjoints administratifs : poste pourvu par secrétaire de mairie
Chargé/e de mission Foncier	35 h 00	1	B et C	Rédacteurs, adjoints administratifs : poste pourvu

Modifications :

ETAT CIVIL/ACCUEIL EVRON

Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Responsable du service	35 h 00	1	B et C	Rédacteurs, adjoints administratifs
Secrétaire de mairie / agent d'accueil	35 h 00	1	C	Adjoints administratifs
Secrétaire de mairie / agent d'accueil	17 h 30	3	C	Adjoints administratifs
Assistant/e de secrétariat / agent/e d'accueil et d'état civil	35 h 00	2	C	Adjoints administratifs
Agent/e d'accueil	35 h 00	1	C	Adjoints administratifs

URBANISME

Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Directeur/trice du service	35 h 00	1	B et C	Rédacteurs, adjoints administratifs
Gestionnaire des autorisations d'urbanisme	35 h 00	1	B et C	Rédacteurs, adjoints administratifs
Gestionnaire des autorisations d'urbanisme	35 h 00	1	B et C	Rédacteurs, adjoints administratifs : Christine
Chargé/e de mission Foncier	35 h 00	1	B et C	Rédacteurs, adjoints administratifs

COMMUNE D'HAMBERS

Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Secrétaire de mairie	35 h 00	1	A, B et C	Attachés, rédacteurs, adjoints administratifs : poste pourvu –

Modification :

COMMUNE D'HAMBERS				
Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Secrétaire de mairie	20 h 00	1	B et C	Rédacteurs, adjoints administratifs à recruter

COMMUNE D'IZE				
Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Agent/e de restauration, d'entretien, de surveillance périscolaire, d'accompagnement en école maternelle	14 h 45	1	C	Adjoints techniques : poste pourvu
Agent/e de restauration, d'entretien, de surveillance périscolaire	10 h 00	1	C	Adjoints techniques : poste pourvu mais départ en retraite : recrutement à lancer sur moins d'heures

Modifications :

COMMUNE D'IZE				
Poste	Nb h. hebdo	Nb postes	catg	Cadres d'emplois
Agent/e de restauration, d'entretien, de surveillance périscolaire, d'accompagnement en école maternelle	20 h 00	1	C	Adjoints techniques : poste pourvu – partie des heures de l'agent partant en retraite à ajouter
Agent/e de restauration, d'entretien, de surveillance périscolaire	5 h 30	1	C	Adjoints techniques : poste pourvu mais départ en retraite : recrutement à lancer sur moins d'heures

6) Information campagne « mobilité choisie »

Pour information, 8 agents se sont manifestés en renvoyant l'imprimé, 5 ont été invités à le faire suite à la prise de connaissance de leur entretien d'évaluation 2019 : 1 à décliner (trop tôt), 1 est en cours et 3 n'ont pas répondu. Sur l'ensemble, 2 demandes ont trait à un motif de santé.

Pour Monsieur BALANDRAUD, l'action « Comprends mon job » pourrait être lancée avec les agents qui se sont déclarés dans cette perspective de mobilité choisie. Il constate à la fois une force et une fragilité à bouger : il y a des équilibres à trouver à plus ou moins long terme.

7) Questions diverses

- Groupe de travail sur le « service minimum » dans certains services lors de grève (point reporté de la dernière séance).

Monsieur BALANDRAUD précise qu'il ne met pas sur ce dossier une pression forte, l'enjeu étant de mener une réflexion et de trouver un équilibre sur la notion de « service minimum » quand une crise survient, que ce soit une grève ou autre chose. La notion centrale est « quel est le besoin minimal de l'usager ? Comment y répond-on ? »

Les représentants CFDT indiquent que cette discussion doit être menée au niveau des organisations syndicales. Monsieur BALANDRAUD propose qu'avant d'organiser cette rencontre, les propositions des services puissent être examinées au sein d'un groupe de travail en sa présence, et avec des représentants du personnel de la CC.

Madame NEVEUX fait un a-parte sur le décompte appliqué sur les fiches de paie des agents grévistes. Elle rappelle que dans la fonction publique d'Etat, 1 jour de salaire est enlevé quel que soit le nombre d'heures de grève effectif dans la journée alors que dans la fonction publique territoriale, le décompte se fait soit par jour, par demi-journée ou par heure. Elle attire l'attention sur le fait que déclarer 4h de grève et non ½ journée n'aboutit pas à la même chose et est souvent désavantageux pour l'agent. Il revient à l'agent d'en avoir conscience lorsqu'il remplit sa déclaration.

- Les représentants de la CFDT informent d'un courrier adressé au Président par les agents du multi-accueil d'EVRON sollicitant la possibilité de déroger au cadre réglementant l'aménagement horaire journalier des femmes enceintes, la possibilité d'octroyer des temps partiels sur autorisation, la possibilité de déroger à la réglementation sur le temps de travail visant à prendre en compte la pénibilité du travail d'auxiliaire de puériculture.

- Lors du prochain CT, les éléments du rapport d'orientations budgétaires 2020 seront présentés par Pierre BOUTELOUP.

L'ordre du jour étant clos, Monsieur BALANDRAUD lève la séance à 11h35.

Le Président,	Le secrétaire de séance,	La secrétaire adjointe,
Joël BALANDRAUD	François DELATOUCHE	Stéphanie DOYE

ANNEXE POINT 1 – CT DU 4 MARS 2020

CHARTE INFORMATIQUE

COMMUNAUTÉ DE COMMUNES
COEVRONS

Mars 2020

Table des matières

1. PREAMBULE 13
2. CHAMP D'APPLICATION 13
2.1. Utilisateurs concernés 13
2.2. Système d'information et de communication 14
3. CONDITIONS D'UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATION ELECTRONIQUE 14
3.1. Le matériel 15
3.2. La navigation sur Internet 15
3.3. Les données informatiques 16
3.4. La messagerie électronique 16
3.5. Les systèmes d'impression 18
4. GESTIONS DES ARRIVEES, DES ABSENCES ET DES DEPARTS DES UTILISATEURS 19
4.1. Arrivées 19
4.2. Absences 19
4.3. Départs 20
5. CONFIDENTIALITE 20
5.1. Mot de passe 20
5.2. Accès à distance 21
6. PROTECTION DES DONNEES A CARACTERE PERSONNEL 21
7. TELEPHONIE 22
8. PROTECTION DE LA PROPRIETE INTELLECTUELLE 23
9. MOBILITE 23
10. SECURITE 24
11. MESURES D'URGENCE ET PLAN DE CONTINUITE D'ACTIVITE 25
12. MAINTENANCE 25
13. CONTROLE ET AUDIT 26
14. REGLES DE CONSERVATION ET DE SAUVEGARDE 27
15. SANCTIONS 28
16. EVOLUTION DE LA CHARTE 28

1. PREAMBULE

La présente charte d'utilisation du système d'information de la Communauté de communes des Coëvrons et de la ville d'Evron (désignées ci-après « la collectivité ») a pour objet de fixer les règles d'utilisation des moyens informatiques et de communication électroniques mis à la disposition des utilisateurs dans le cadre de leurs activités.

Tout utilisateur est responsable de l'usage qu'il fait des moyens informatiques mis à sa disposition. En effet, l'utilisation de ces moyens suppose le respect de règles dont les rôles sont d'assurer la sécurité, la performance, la confidentialité des données et le respect des dispositions légales et réglementaires applicables.

La présente charte tient compte notamment des recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL) www.cnil.fr et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) www.ssi.gouv.fr.

La présente charte n'a pas pour objet et objectif de couvrir de façon exhaustive tous les cas de figure susceptibles de se présenter dans le cadre de l'utilisation des moyens informatiques et de communication électronique mis à la disposition des utilisateurs. C'est l'esprit des règles ainsi édictées qui doit guider le comportement de chacun dans des situations non envisagées.

La présente charte est accessible dans l'Intranet ou sur le serveur de fichiers dans S:\Informatique\Public. Elle est annexée au règlement intérieur. Tout utilisateur est tenu d'en prendre connaissance.

Le Service Informatique représenté par le Directeur des Systèmes d'Information (DSI) et les techniciens appartenant au service, tels que défini dans l'organigramme CC Coëvrons/Ville d'Evron, sont les garants de la bonne application de cette charte. Pour cela, le Service Informatique peut faire appel à des prestataires tiers, qui, mandatés par la DSI, peuvent avoir toute prérogative pour assumer le rôle et actions de la DSI ci-après décrits.

2. CHAMP D'APPLICATION

2.1. Utilisateurs concernés

Les règles figurant dans la présente charte, de même que l'obligation de respecter la législation en vigueur, s'appliquent à l'ensemble des utilisateurs, quel que soit leur statut.

S'entend par utilisateur, toute personne ayant accès aux moyens informatiques et de communication :

- les élus du conseil communautaire de la 3C et des conseils municipaux des communes membres ;
- les agents (agents stagiaires et titulaires, agents contractuels de droit public, agents sous contrat de droit privé) ;
- les stagiaires extérieurs (collège, lycée, université…) ;
- les personnels de l'Education Nationale, les élèves ;
- le personnel des prestataires de services intervenant sur un site physique et/ou utilisant les moyens de télémaintenance ;
- les représentants des organisations syndicales ou représentatives ;

- les membres des associations ;
- les bénévoles ;
- les membres du CODEV ;
- les utilisateurs des postes informatiques mis à disposition ou du wifi public ;
- toutes personnes (physiques ou morales) utilisant les moyens informatiques et de communication.

Sont également visés par la présente charte l'ensemble des moyens informatiques et de communication électronique qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité de service.

2.2. Système d'information et de communication

Le système d'information et de communication est l'ensemble des ressources de la collectivité qui permet la gestion de l'information. Il est généralement associé aux technologies (matériel, logiciel et communication), aux processus qui les accompagnent et aux personnes qui les supportent.

Le système d'information et de communication de la collectivité est, entre autre, constitué des éléments matériels suivants : ordinateurs fixes ou portables, périphériques y compris clés USB, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, imprimantes, téléphones, smartphones, tablettes, clés 3G, bornes wifi, logiciels, fichiers, données et bases de données, système de messagerie, connexion Internet, intranet, extranet, etc.

S'ajoute à ces moyens tout ce qui entre en interconnexion avec le système d'information et de communication tels que les objets connectés, caméras, badgeuses, alarmes, barrières de sécurité, bornes, tableaux interactifs, systèmes de visioconférence, écrans d'affichage, etc.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des utilisateurs connecté au réseau de la collectivité, ou contenant des informations à caractère professionnel concernant la collectivité.

3. CONDITIONS D'UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATION ELECTRONIQUE

L'usage des moyens informatiques et de communication électronique est présumé être en lien avec son affectation. Ainsi le matériel mis à disposition ne doit pas être détourné de son utilisation initiale.

Toute utilisation des moyens informatiques et de communication électronique à des fins personnelles peut être tolérée à condition de :

- ne gêner en rien les activités du service ;
- rester très modérée ;
- ne pas poursuivre un but lucratif ou ludique ;
- ne pas être susceptible d'engager la responsabilité du service.

Dans tous les cas, l'usage des moyens informatiques et de communication électronique à des fins sans lien avec le service relève de la seule et entière responsabilité de l'utilisateur, qui dégage en conséquence la collectivité de toute responsabilité.

3.1. Le matériel

Il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et d'en prendre soin.

Par mesure d'hygiène et de protection du matériel mis à disposition, il est formellement interdit de consommer des aliments ou boissons au-dessus ou à proximité immédiate des outils informatiques.

Le vol ou le détournement d'un matériel doivent être signalés aussi rapidement que possible au Service Informatique.

L'utilisateur doit enregistrer les données sur les serveurs prévus à cet effet et ne stocker sur un support autre (ordinateurs fixes ou portables, téléphones mobiles, clés USB…) que le strict nécessaire. Ces fichiers doivent être enregistrés sur les serveurs dès que possible.

L'agent ne doit pas installer/tenter d'installer de logiciels ou de copier des fichiers susceptibles de créer des risques d'atteinte à la sécurité au sein de la collectivité.

Il est rappelé que le matériel n'appartient pas à un agent ou à un service mais à la collectivité. De ce fait, chaque agent peut s'y connecter avec ses propres droits d'accès pour y travailler en cas d'absence de son utilisateur principal et après accord du supérieur hiérarchique de ce dernier. De plus, le Service Informatique peut à tout moment remplacer le matériel attribué. En cas de sous-utilisation du matériel, le Service Informatique pourra le réattribuer.

L'utilisation de caméra, webcam, nomade ou sur ordinateur portable, ou tout autre matériel permettant l'enregistrement audio et/ou vidéo est autorisée seulement dans un cadre normal tel que la visioconférence.

Toutes installations dissimulées pourra faire l'objet de sanction.

Le Service Informatique a accès à tous les lieux nécessaires à la bonne réalisation de ses missions.

3.2. La navigation sur Internet

Seuls les sites Internet présentant un lien direct et nécessaire avec l'activité de service, ainsi qu'une utilité au regard des fonctions exercées ou des missions à mener, ont vocation à être consultés.

La navigation à des fins personnelles, depuis le lieu de travail, est tolérée pendant les temps de pause ou pour des besoins urgents de la vie privée de l'utilisateur et à condition que la navigation n'entrave pas l'accès professionnel.

La tolérance sous conditions suscitées d'utiliser la navigation sur Internet à des fins personnelles peut être limitée ou suspendue par le Service Informatique, à tout moment et sans préavis, pour un ou plusieurs utilisateurs, dans son principe ou ses modalités d'exercice (exemple : blocage d'accès à certains sites Internet).

Les débits disponibles étant limités et partagés avec d'autres technologies, l'utilisation de chacun est conditionnée par celle de l'autre. L'écoute de radio Internet, la visualisation de flux vidéo, le téléchargement ou autre utilisation qui ne relèvent pas de l'utilisation en lien avec le service sont donc interdits.

Les pare-feu vérifient tout le trafic entrant et sortant de la collectivité. Ils détiennent toutes les traces de l'activité qui transite : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels), ordinateur et compte utilisé.

3.3. Les données informatiques

Les données contenues dans le système d'information doivent également être en lien direct et nécessaire avec l'activité de la collectivité. Ces données sont la propriété de la collectivité et n'ont pas lieu à être exploitées autrement.

Sont proscrites notamment sur le poste de travail ou les serveurs, toutes données contraires à la loi, aux bonnes mœurs ou pouvant porter préjudice à la collectivité ou à son image.

Toute information est présumée être en lien direct et nécessaire avec l'activité de la collectivité à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. En effet, il appartient à l'utilisateur de procéder au stockage de ses données à caractère personnel dans un répertoire de données nommé « Personnel » ou « Privé », répertoire qui ne sera pas inclus dans les sauvegardes du système d'information.

Le caractère « Personnel » ou « Privé » du répertoire informatique clairement identifiable ne fait pas obstacle à ce que :

- le Service Informatique puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour l'administration en termes notamment de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée ;
- ces éléments fassent l'objet de conservation technique dans le cadre des procédures de sauvegarde ou plans de continuité ou reprise d'activité mises en œuvre au sein de la collectivité ;
- soit procédé à la mise en quarantaine ou, le cas échéant, à la suppression d'un élément quelconque qui comporte ou comporterait un code malveillant ;
- un administrateur accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des moyens informatiques et de communication électronique, ce notamment dans le cadre d'opération de maintenance ;
- la collectivité puisse, dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur.

3.4. La messagerie électronique

L'accès à la messagerie électronique se fait par le biais du portail Office 365.

Au même titre que pour le courrier ou le téléphone, les utilisateurs sont responsables des messages envoyés et doivent utiliser la messagerie dans le respect des délégations de signature, des missions et fonctions qui leur sont dévolues et des règles élémentaires de politesse et de courtoisie.

Les utilisateurs dotés d'une messagerie professionnelle @coevrons.fr, @evron.fr, @coevrons-tourisme.com, @eau-coevrons.fr ont l'obligation d'utiliser celle-ci pour leurs échanges professionnels.

La messagerie électronique doit être utilisée avec modération pour ne pas surcharger les destinataires, pour rester un outil performant et non pas devenir une contrainte mais aussi et surtout pour maintenir les relations et les contacts verbaux directs entre les utilisateurs. L'utilisation des groupes d'adresses doit être réfléchie.

L'adresse de messagerie électronique nominative pour les utilisateurs concernés est composée, en règle générale, de la façon suivante : « 1ère lettre du prénom »« nom »@coevrons.fr

L'adresse de messagerie doit être conforme aux données d'état civil enregistrées par le Service des Ressources Humaines. Les homonymes parfaits seront traités au cas par cas.

En cas de changement de nom d'un utilisateur, et quelle qu'en soit la raison, celui-ci est tenu d'en informer le Service Informatique dans les meilleurs délais, afin de procéder à la modification de l'intitulé de l'adresse de messagerie.

L'utilisation de l'option de transfert du courrier électronique dans Office 365 peut être tolérée pour les personnes dont ce n'est pas l'adresse électronique principale (exemple : les élus).

Le Service Informatique tolère un usage personnel modéré de la messagerie électronique. A cet égard, et selon les recommandations de la CNIL, les messages à caractère privé doivent être identifiés dans l'objet, autant en émission qu'en réception, avec la mention « Personnel » ou « Privé ».

L'adresse électronique est strictement réservée au fonctionnement du service.

Les agents doivent utiliser la charte graphique et la signature personnalisée fournies par le Service Communication.

L'inscription sur des listes de diffusion permettant la réception automatique et périodique d'informations est également réservée à un usage en lien avec le service. Elle est basée sur un principe d'autodiscipline des utilisateurs, destinée à s'assurer d'une part, de la pertinence et de la nécessité d'une telle inscription et d'autre part, des conséquences de celle-ci (fréquence de réception de messages, poids des messages, encombrement des réseaux, ...).

La diffusion de l'adresse électronique sur des sites Internet (chats, forums, blogs, réseaux sociaux, ...), doit être réfléchie et en rapport avec l'activité du service pour éviter la diffusion de cette dernière sur des listes de courrier indésirable.

La messagerie électronique n'est en aucun cas un support publicitaire servant de promotion à un quelconque produit ou prestation de service qui n'émanerait pas de l'institution. Aucune démarche commerciale ne saurait être tolérée.

L'agenda sous Office 365 est par défaut partagé pour tout le monde et ne doit pas être désactivé.

La taille globale de la boîte aux lettres est limitée. Au-delà de cette taille, l'utilisateur ne peut plus créer d'éléments nouveaux dans sa boîte aux lettres. Ceci implique un nettoyage régulier de l'ensemble des éléments la composant afin d'éviter tout dysfonctionnement dû au dépassement de taille (y compris les éléments envoyés et les éléments supprimés). Il est important de sauvegarder au préalable sur le serveur de fichiers les messages engageants ainsi que les pièces jointes.

Dans le cadre d'un envoi interne de fichiers volumineux, l'émission d'un message à une liste de diffusion est à éviter. Sont à privilégier les outils de publication sur les serveurs d'échanges en vigueur sur le réseau interne.

Des listes de diffusion sont constituées et accessibles à l'ensemble des utilisateurs de la messagerie Office 365. Elles sont mises à jour par le Service Informatique.

3.5. Les systèmes d'impression

Il est recommandé de n'utiliser les impressions qu'en cas de réel besoin pour des raisons écologiques et économiques. Les photocopieurs sont de fait à privilégier en imprimant de préférence en noir et blanc et en recto/verso. Le Service Informatique n'installera donc des imprimantes individuelles que si elles ont une utilité spécifique (ex : PMR, accueil, etc.).

Les sites disposants d'un photocopieur sont autonomes sur l'alimentation en papier ou en toners. Si les niveaux de couleurs sont bas sans toner d'avance, il est préférable de prévenir le Service Informatique, au moins 48 heures avant, pour qu'il s'assure de la bonne remontée automatique des alertes auprès des fournisseurs.

Les utilisateurs sont responsables de leurs impressions et pour la confidentialité, ne doivent pas les laisser dans la machine ; il est conseillé dans ce cas d'utiliser l'impression protégée avec un code.

Il en est de même pour les documents numérisés. Un programme informatique peut être installé afin de supprimer automatiquement les fichiers à fréquence régulière.

Une impression ou photocopie peut nécessiter l'utilisation d'un identifiant avec un code géré par le Service Informatique.

Toutes les impressions sont tracées et listées dans un historique dans lequel peut apparaître pour chaque impression : le nom de l'utilisateur, l'ordinateur utilisé, le nom du document imprimé, les réglages appliqués. Cet historique pourra servir à des fins statistiques mais aussi afin de s'assurer de la bonne utilisation des matériels par les agents.

L'impression de documents personnels est régie par l'article 61 du règlement intérieur du personnel.

4. GESTIONS DES ARRIVEES, DES ABSENCES ET DES DEPARTS DES UTILISATEURS

4.1. **Arrivées**

Les moyens informatiques et de communication électronique sont mis à disposition de l'utilisateur par le Service Informatique sur demande de son autorité hiérarchique. Cette demande doit intervenir au minimum deux semaines avant la date prévue. Le bénéficiaire devient responsable des moyens ainsi mis à sa disposition. Le Service Informatique jugera du matériel à fournir le plus approprié au poste de l'utilisateur.

Les droits d'accès de l'utilisateur sont définis en fonction de son affectation (direction, service, niveau hiérarchique, niveau « technique » dans l'accès aux logiciels métiers et aux serveurs de fichiers…).

La sécurité des moyens informatiques mis à disposition impose :

- de respecter la gestion des accès, en particulier de ne pas utiliser les identifiants et mots de passe d'un autre utilisateur, ni chercher à connaître ces informations ;
- d'avertir le Service Informatique de tout dysfonctionnement technique constaté, de toute anomalie découverte ou de toute possibilité technique d'accès à une ressource informatique qui ne correspond pas à son habilitation ;
- de s'interdire d'accéder ou tenter d'accéder à des fichiers ou programmes informatiques pour lesquels l'utilisateur ne bénéficie pas d'une habilitation expresse de la part de son autorité hiérarchique même si cet accès est techniquement possible ;
- ne pas sortir les matériels attribués des locaux prévus et/ou ne pas les intervertir/déplacer sans l'autorisation du Service Informatique ;
- de ne pas installer de périphériques non fournis par la collectivité sans l'autorisation du Service Informatique ;
- de ne pas installer, télécharger ou utiliser sur les matériels informatiques un logiciel et/ou un progiciel sans l'accord du Service Informatique ;
- de prendre soin du matériel fourni et d'assurer la sécurité physique des équipements et des supports informatiques ;
- de ne pas laisser les équipements informatiques sans surveillance dans un lieu public, un transport en commun, un véhicule.

4.2. Absences

En cas d'absence de l'utilisateur, pour quelque raison et durée que ce soit, la collectivité par le biais du Service informatique se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques et plus généralement tous documents en lien avec le service de l'utilisateur, ayant recours en tant que de besoin.

L'utilisateur doit mettre en place l'indicateur d'absence de la messagerie et spécifier à quelle adresse devront être éventuellement envoyés les messages. Si l'utilisateur n'a pas mis en place de lui-même cette option, le Service Informatique s'autorise à réaliser cette opération à la demande de son supérieur hiérarchique.

Ses accès peuvent être également désactivés au-delà de 31 jours consécutifs.

4.3. Départs

La suppression du compte utilisateur (fin d'activité au sein de la collectivité) est réalisée par le Service Informatique dès que ce dernier est alerté par le Service des Ressources Humaines ou par le service de l'utilisateur.

D'une manière générale, lors du départ de l'utilisateur, aucun élément ne doit être protégé par un code d'accès ou un mécanisme de protection quelconque.

Lors de son départ, l'utilisateur se doit de supprimer son répertoire « Personnel » ou « Privé ». A défaut, il sera supprimé par le Service Informatique.

L'utilisateur doit, avant de quitter la collectivité, remettre le matériel mis à disposition par le Service Informatique. Si l'utilisateur a bénéficié d'un moyen d'authentification à distance, il s'engage également à le restituer.

A défaut de restitution des outils, un titre exécutoire du montant de leur remplacement à neuf au moment du départ de l'intéressé est émis à son encontre.

Ce départ entraîne également la fermeture de sa boîte aux lettres électronique. L'utilisateur doit mettre en place l'indicateur d'absence de la messagerie et spécifier à quelle adresse devront être éventuellement envoyés les messages. Si l'utilisateur n'a pas mis en place de lui-même cette option, le Service Informatique s'autorise à réaliser cette opération à la demande de son supérieur hiérarchique.

L'utilisateur ne doit pas quitter la collectivité avec des documents du service et en aucun cas les supprimer des lecteurs réseaux mis à sa disposition sous peine de poursuites judiciaires.

En cas de décès d'un utilisateur, ou d'un empêchement fort de le contacter, les actions énoncées ci-dessus seront effectuées par le Service Informatique après concertation avec le supérieur hiérarchique de la personne concernée.

5. CONFIDENTIALITE

Chaque utilisateur doit respecter une obligation générale et permanente de confidentialité et de discrétion professionnel à l'égard des informations disponibles dans son système d'information.

Chaque utilisateur doit veiller à ce que les personnes hors collectivité n'aient pas connaissance d'informations confidentielles et ne doit pas rechercher ou ouvrir un fichier pour lequel il ne dispose pas des droits.

La cryptographie est interdite si elle n'a pas été expressément autorisée et mise en place par le Service Informatique.

5.1. Mot de passe

L'utilisation de mots de passe est obligatoire pour les accès au système d'information et de communication.

Chaque utilisateur doit veiller à la sécurité de son mot de passe personnel qui est constitué d'un code alphanumérique permettant l'accès à un ou plusieurs environnements informatiques ainsi qu'à la messagerie.

L'identification sur les postes de travail engage la responsabilité de l'utilisateur, pour toutes les actions qui seront effectuées (serveurs, accès aux applications, messagerie, navigation sur Internet…).

C'est pourquoi l'utilisateur doit veiller à ce que cette identification ne soit pas usurpée, notamment par l'utilisation illicite de son poste de travail en cas d'absence momentanée ou prolongée.

Ainsi, en cas d'absence, l'utilisateur doit verrouiller son poste de travail ou fermer sa session de connexion. A la fin de la journée de travail, l'utilisateur doit arrêter les applications, arrêter le système et éteindre son ordinateur.

Il est rappelé à chaque utilisateur que :

- il est personnellement responsable de son mot de passe ;
- il ne doit pas communiquer son mot de passe ni l'écrire sur un document facilement accessible ;
- il doit avoir un mot de passe sûr, n'ayant aucun lien avec son environnement familier ;
- il doit changer de mot de passe selon la périodicité définie par le Service Informatique.

Les mots de passe choisis par l'utilisateur devront comportés au minimum 8 caractères alphanumériques.

Pour le choix d'un bon de mot de passe, il est fortement conseillé de suivre les préconisations de l'ANSSI.

5.2. Accès à distance

Un accès à distance peut être accordé après autorisation hiérarchique.

Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à utiliser, à l'exclusion de tout autre, les moyens techniques d'authentification qui lui seront remis.

En termes de sécurité et de confidentialité, l'utilisateur est soumis aux mêmes obligations que celles visées pour la gestion des identifiants et devra suivre toutes les prescriptions complémentaires qui lui seront signifiées.

Il devra aviser, sans délai, le Service Informatique de la perte ou du vol des moyens d'authentification à distance.

L'accès à certains services en ligne tels que la messagerie, l'Intranet ou certaines applications métiers, peuvent se faire à distance via une connexion et du matériel personnel.

6. PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre de la mise en conformité au regard du droit des données à caractère personnel, cette charte vise également à informer les utilisateurs des « bonnes pratiques » à adopter.

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée (Loi Informatique et Libertés) et le Règlement européen n°2016/679 du 27 avril 2016 sur la protection des données personnelles (RGPD) donnent une définition d'une donnée à caractère personnel comme suit : *« toute information se rapportant à une personne physique identifiée ou identifiable [...] ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée »* (ci-après désignées comme les « Données personnelles »).

A ce titre, le RGPD définit les conditions selon lesquelles les traitements de données à caractère personnel doivent être effectués :

- les données personnelles doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (principe de licéité, de loyauté et de transparence) ;
- elles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (principe de limitation des finalités) ;
- elles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données) ;
- elles doivent être exactes et, si nécessaire, tenues à jour : toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (principe d'exactitude) ;
- elles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de limitation de la conservation) ;
- elles doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (principe d'intégrité et de confidentialité).

La diffusion de données à caractère personnel à l'attention de tiers extérieurs à la collectivité doit être rigoureusement autorisée. Que ce soit une diffusion électronique, physique ou orale.

7. TELEPHONIE

L'utilisation des équipements téléphoniques (fixe ou mobile) est réservée à un usage en lien direct et nécessaire avec le service. Toutefois, un usage privé est toléré s'il reste exceptionnel et s'il n'occasionne pas de dépense supplémentaire.

Pour la bonne gestion des ressources téléphoniques :

- sur certains sites, un autocommutateur ou un PABX peut enregistrer, à partir de chacun des postes téléphoniques fixes, les éléments de la communication (date, heure, durée et numéros appelés) ;
- pour les moyens informatiques et de communication électronique nomades (téléphone portable, smartphone, ...), les mêmes informations sont disponibles via les opérateurs téléphoniques mobiles, à travers les services de suivi des consommations qu'ils proposent.

Les informations ainsi disponibles, qui sont principalement dédiées à l'analyse des consommations, peuvent en tout état de cause être utilisées pour démontrer toutes utilisations contrevenantes aux termes de la présente charte ou pour servir de preuve d'un fait manifestement illicite.

La collectivité peut être amenée à demander à l'utilisateur le remboursement du coût d'une ou plusieurs communications téléphoniques considérées comme passées à titre privé et/ou abusives.

Le Service Informatique est garant de la gestion de la téléphonie. A ce titre, il peut intervenir sur les moyens mis au service des utilisateurs, soit en attribuant, remplaçant, modifiant ou supprimant du matériel, forfait, lignes téléphoniques, etc.

L'enregistrement des conversations téléphoniques, fixe ou mobile, est strictement interdit.

L'utilisation du « partage de données » ne doit être utilisée qu'exceptionnellement en cas de non accès au réseau. En cas d'utilisation abusive, le Service Informatique peut restreindre son utilisation.

8. PROTECTION DE LA PROPRIETE INTELLECTUELLE

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

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

- utiliser les logiciels, applications, dans les conditions de la licence souscrite par la collectivité ;
- ne pas effectuer de copie illicite de logiciel, d'applications et, à fortiori, ne pas tenter d'installer des logiciels pour lesquels la collectivité ne possèderait pas un droit d'usage ;
- ne pas reproduire et utiliser les bases de données, pages web ou autres créations de la collectivité ou de tiers protégés par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création de la collectivité.

9. MOBILITE

Dans le cadre de ses déplacements de service ou de télétravail, quelle que soit leur durée ou leur fréquence, l'utilisateur assure la garde et la responsabilité des moyens informatiques et de communication électronique.

Cet usage de moyens informatiques et de communication électronique dits « nomades » impose à l'utilisateur un niveau de surveillance et de confidentialité renforcée.

En particulier, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations et des ressources du système d'information de la collectivité qu'il pourrait être amené à manipuler ou à échanger.

Il doit également veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens, les utiliser ou accéder à leurs contenus.

En cas non seulement d'incident avéré mais également de doutes, l'utilisateur doit immédiatement en aviser le Service Informatique.

Les appareils mobiles sont gérés, protégés et sécurisés par le Service Informatique. L'ensemble de la flotte est équipée de systèmes de protections gérées à distance tels que antivirus, limitation des téléchargements des applications, cryptage, blocage, désactivation et suppression des données à distance, localisation en cas de vol, etc.

10. SECURITE

Les moyens informatiques et de communication électronique sont exclusivement installés, configurés et paramétrés par le personnel du Service Informatique.

A des fins de précaution, certaines configurations peuvent être verrouillées par le Service Informatique (poste de travail, accès au réseau, accès Internet, etc.).

La mise en place d'outils de sécurité par le Service Informatique ne doit pas dispenser les utilisateurs d'une obligation de vigilance à cet égard.

En effet, tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens informatiques et de communication électronique mis à sa disposition, principalement en évitant l'introduction de virus ou codes malveillants susceptibles d'endommager le système d'information.

Cette vigilance passe notamment par le respect des règles de conduite suivantes :

- ne pas ouvrir ni faire suivre les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ou douteux ;
- même chose pour les liens contenus dans ces messages ;
- détruire les messages du type chaîne de solidarité, appels à la solidarité, alertes de sécurité ;
- ne pas tenter de se désabonner des courriers indésirables ;
- en cas de doute, demander conseil au Service Informatique.

L'utilisateur s'interdit également de :

- toute installation ou utilisation de matériels, logiciels, progiciels, même gratuits, non expressément autorisés par le Service Informatique ; si ces logiciels ou matériels lui semblent nécessaires pour l'exercice de sa mission, il en fait part au Service Informatique ;
- modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit ;
- mettre à la disposition d'utilisateurs non autorisés un accès au système d'information et de communication ;
- utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués, ou masquer son identité ;
- effectuer des opérations pouvant nuire aux relations internes ou externes de la collectivité ;
- contourner les protections réseaux en utilisant des techniques telles que l'utilisation de VPN, partage de données d'un smartphone, connexion personnelle, etc.
- accéder ou tenter d'accéder aux locaux, salles serveurs ou baies informatiques ;

- brasser des prises réseau, utiliser un switch ou un répéteur wifi ;
- de faire obstacle à l'accès, par la Direction des services d'information, aux moyens mis à disposition des agents.

L'utilisateur est tenu d'informer, sans délai, le Service Informatique de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les moyens informatiques et de communication électronique. Il est tenu, en particulier, de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus.

11. MESURES D'URGENCE ET PLAN DE CONTINUITE D'ACTIVITE

L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, le Service Informatique peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'utilisateur pourra être amené à la demande du Service Informatique à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure :

- une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, ... ;
- la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion Internet, accès applicatifs, éléments relatifs au poste de travail, ...) ;
- la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au système d'information, travail à distance, déplacement sur des sites de secours tiers, ...).

12. MAINTENANCE

La mise à disposition des moyens informatiques et de communication électronique implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité des systèmes d'information. Elles se distinguent en cela des opérations de contrôle et d'audit.

Ces opérations peuvent nécessiter l'intervention d'une personne habilitée soit :

- sur site, ce qui sous-entend que le Service Informatique a accès à tous les locaux ;
- à distance, conduisant la personne habilitée à « prendre la main à distance ».

Il est rappelé que, dans ce cadre, la personne habilitée peut être amenée à prendre connaissance de l'ensemble des éléments présents sur le poste de l'utilisateur, ainsi que des données de connexion, qu'il s'agisse d'un usage de service ou privé.

Si, à l'occasion d'opérations de maintenance, une utilisation anormale et/ou un contenu illicite ou préjudiciable est identifié, la collectivité prendra les mesures adéquates.

Seule la maintenance du matériel professionnel, et dans les locaux de la collectivité, est assurée par les techniciens.

13. CONTROLE ET AUDIT

Les opérations de contrôle et d'audit se distinguent des opérations de maintenance en ce qu'elles portent sur la régularité de l'utilisation des moyens informatiques et de communication électronique.

Ainsi, le Service Informatique peut contrôler l'activité des utilisateurs et en particulier, le respect par eux de la présente charte. L'utilisation des moyens informatiques et de communication électronique pourra ainsi faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation, ou encore de mener des analyses statistiques.

Pour satisfaire aux obligations qui lui incombent, tenant à sa capacité à apporter la preuve, le cas échéant, du bon usage des moyens informatiques et de communication électronique mis à la disposition des utilisateurs, et à prévenir tout usage illicite de ces mêmes moyens, le Service Informatique procède à la mise en place :

- d'outils de traçabilité (journaux de connexions) de l'ensemble des moyens informatiques et de communication électronique ;
- d'outils de filtrage (contenus, URL, protocoles, ...) permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre ou d'interdire l'accès à Internet ou à certaines catégories de sites Internet.

Toute tentative de détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdite.

Le Service Informatique se réserve ainsi le droit, notamment :

- de vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information ;
- de contrôler l'origine licite des logiciels installés ;
- de conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

En outre, en cas d'incident, le Service Informatique se réserve le droit de :

- surveiller le contenu des informations qui transitent sur son système d'information ;

- vérifier le contenu des disques durs, clés USB, cartes mémoires, etc… des ressources du système d'information attribuées aux utilisateurs ;
- procéder à toute copie utile pour faire valoir ses droits.

Ces opérations de contrôle et d'audit relèvent des fonctions du Service Informatique qui a la charge de la qualité, de la protection et de la sécurité des moyens informatiques et de communication électronique fournis aux utilisateurs.

En particulier, dans le cadre de ses fonctions, le Service Informatique exerce un contrôle notamment des durées de connexion et des sites les plus visités. En cas de perturbation induite par l'apparition intempestive d'alertes suite à des tentatives d'infection des systèmes à l'aide de virus informatiques, le Service Informatique est habilité à mener toutes les investigations qu'il jugera utiles aux fins d'éradiquer lesdits virus.

Tout intervenant du Service Informatique ou intervenant extérieur doit impérativement respecter la confidentialité des échanges électroniques et des fichiers des utilisateurs, et sont tenus à la discrétion professionnelle.

En cas de faisceau d'indices laissant supposer qu'un utilisateur met en cause l'image, les intérêts ou la sécurité de la collectivité, en ne respectant pas les règles instituées par la présente charte, le Service Informatique peut fournir à la Direction Générale de la collectivité les traces individuelles des connexions incriminées sur une période d'une année.

Suivant la gravité des faits et sans préjudice d'éventuelles sanctions disciplinaires et/ou pénales, les droits d'accès de l'utilisateur concerné pourront être suspendus temporairement ou définitivement.

Tout matériel installé illicitement sera supprimé ou désactivé par le Service Informatique dès le constat de leur présence non autorisée.

14. REGLES DE CONSERVATION ET DE SAUVEGARDE

L'utilisateur est dans l'obligation de respecter la politique de conservation et d'archivage mise en œuvre au sein de la collectivité. Il est nécessaire de se rapprocher du service Archives de la collectivité, car "les archives sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité (article L211.1 du Code du Patrimoine).

Il est impératif de contacter le Service Informatique dans le but de conserver des contenus multimédias (sons, films) afin de mettre en œuvre correctement les ressources de stockage nécessaires à ces fichiers très volumineux.

Les fichiers dont la durée d'utilité administrative a expiré et qui ne doivent pas être versés au service Archives doivent être supprimés par les utilisateurs selon la procédure en vigueur après visa du Directeur des Archives départementales de la Mayenne (§ note de procédure interne sur les demandes

d'éliminations). De plus, leur stockage risque d'encombrer les serveurs et les sauvegardes qui sont effectuées.

Les traces détaillées d'activité sont conservées pendant les durées réglementaires, à l'issue desquelles elles sont détruites.

Ces traces valent preuve de l'utilisation des moyens informatiques et de communication électronique.

Elles peuvent être fournies aux autorités compétentes selon les dispositions légales et réglementaires en vigueur.

15. SANCTIONS

Tout contrevenant à ces règles d'utilisation des moyens informatiques et de communication électronique s'expose aux sanctions suivantes :

- en cas de violations mineures des règles fixées par la Charte, le Service Informatique avertira directement l'utilisateur concerné afin que soit mis un terme à la violation constatée ;
- en cas de violations graves des règles d'utilisation des moyens informatiques et de communication électronique ou en cas de récidives quel que soit le non-respect constaté (mineur/grave), le Service Informatique informera le responsable hiérarchique afin que soit mis un terme à la violation constatée et que soient prises les sanctions appropriées (restriction ou suspension de l'utilisation des moyens, poursuites disciplinaires…) ;
- en cas de non-respect des dispositions de la charte relevant de nouvelles récidives et surtout de fautes pénalement répréhensibles, le Service Informatique présentera un rapport à la Direction Générale de la collectivité afin que soient mises en œuvre les mesures appropriées (poursuites disciplinaires et/ou pénales…).

Si l'urgence le justifie, le Service Informatique peut sans délai :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques ;
- prévenir la Direction Générale de la collectivité et/ou le responsable hiérarchique de l'utilisateur concerné.

16. EVOLUTION DE LA CHARTE

La présente charte pourra être mise à jour compte tenu de la perpétuelle évolution du système d'information et des règles juridiques.