1. OBJET DE LA CHARTE

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet de l'association APAEI de la Côte Fleurie et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.
Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information de l'association, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par l'association et au Règlement Général de la Protection des Données (RGPD) en vigueur depuis mai 2018.
Cette Charte a été validée par la Direction générale de l'association. Les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance. La Charte est mise à leur disposition sur la Gestion Documentaire informatisée de l'association et dans le livret d'accueil du nouveau salarié. Elle est remise à chaque nouveau collaborateur.

2. CHAMP D'APPLICATION

La présente Charte concerne les ressources informatiques, les services Internet et téléphoniques de l'APAEI de la Côte Fleurie ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électroniques interne ou externe. Il s'agit principalement des ressources suivantes :

- ✓ Ordinateurs de bureau,
- ✓ Ordinateurs portables,
- ✓ Terminaux,
- ✓ Imprimantes simples ou multifonctions,
- ✓ Tablettes, ou IPad,
- ✓ Smartphones/ Téléphones portables,
- ✓ Téléphones fixes,

Cette Charte s'applique à l'ensemble des professionnels des établissements et des services du siège, tous statuts confondus, et concerne notamment les agents permanents ou temporaires (stagiaires, internes, doctorants, prestataires, fournisseurs, sous-traitants, bénévoles…) utilisant les moyens informatiques de l'établissement et les personnes, d'accéder au système d'information à distance, directement ou à partir du réseau administré par l'établissement.
Dans la présente Charte, sont désignés sous les termes suivants :

- **Ressources informatiques** : les moyens informatiques, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entité ;
- **Outils de communication** : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses (web, messagerie, forum, etc.) ;
- **Utilisateurs** : les personnes ayant accès ou utilisant les ressources informatiques et les services Internet de l'association.

3. CADRE REGLEMENTAIRE

Le cadre réglementaire de la sécurité de l'information est complexe. Il porte sur les grands thèmes suivants :

- Le traitement numérique des données, et plus précisément :
  - ✓ Le traitement de données à caractère personnel et le respect de la vie privée, ✓ Le traitement de données personnelles de santé.
  - ✓ Le droit d'accès des usagers et des professionnels de santé aux données médicales,
  - ✓ L'hébergement de données médicales,
  - ✓ Le secret professionnel et le secret médical,
  - ✓ La signature électronique des documents,
  - ✓ Le secret des correspondances,
  - ✓ La lutte contre la cybercriminalité,
  - ✓ La protection des logiciels et des bases de données et le droit d'auteur.

La présente Charte d'accès et d'usage du système d'information tient compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux utilisateurs.

4. CRITÈRES FONDAMENTAUX DE LA SÉCURITÉ

4.1 PRINCIPES

L'APAEI de la Côte Fleurie héberge des données et des informations médicales et administratives sur les usagers (dossier administratif, dossier médical, dossier de soins, dossier images et autres dossiers médico-techniques…), et sur les personnels (paie, gestion du temps, évaluations, accès à Internet et à la messagerie…).
L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, imprimée sur des films (images), transmise par des réseaux informatiques privés ou Internet, par la poste, oralement et/ou par téléphone...

La **sécurité de l'information** est caractérisée comme étant la préservation de :

- ✓ Sa disponibilité : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin,
- ✓ Son intégrité : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie,
- ✓ Sa confidentialité : l'information ne doit être accessible qu'aux personnes autorisées à y accéder,
- ✓ Sa traçabilité : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

4.2 UNE MISSION SECURITE

L'APAEI de la Côte Fleurie fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble, c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances. Elle doit aussi protéger les intérêts économiques de l'association en s'assurant que ces moyens sont bien au service de la production de l'accompagnement et du soin. Elle doit donc caractériser et empêcher les abus.

4.3 UN ENJEU TECHNIQUE ET ORGANISATIONNEL

Les enjeux majeurs de la sécurité sont la qualité et la continuité de l'accompagnement et des soins, le respect du cadre juridique sur l'usage des données personnelles et de santé. Pour cela l'APAEI de la Côte Fleurie déploie un ensemble de dispositifs techniques, mais aussi organisationnels. En effet, au-delà des outils, la bonne utilisation des moyens informatiques est essentielle pour garantir un bon niveau de sécurité. La sécurité peut être assimilée à une chaîne dont la solidité dépend du maillon le plus faible. Certains comportements humains, par ignorance des risques, peuvent fragiliser le système d'information.

4.4 UNE GESTION DES RISQUES

L'information médico-sociale et médicale, qu'elle soit numérique ou non, est un composant sensible qui intervient dans tous les processus de prise en charge des usagers. Une information manquante, altérée ou indisponible, peut constituer une perte de chance pour l'usager (exemples : erreur dans l'identification d'un usager [homonymie par exemple], perte de données à la suite d'une erreur d'utilisation d'une application informatique…). La sécurité repose sur une gestion des risques avec des analyses des risques potentiels, des suivis d'incidents, des dispositifs d'alertes. La communication vers les utilisateurs est un volet important de cette gestion. La présente Charte d'accès et d'usage du système d'information s'inscrit dans ce plan de communication.

5. RÈGLES DE SÉCURITÉ

L'accès au système d'information des établissements est soumis à autorisation de la direction de celui-ci.

- **Pour le personnel**, y compris les personnels libéraux, mis à disposition et stagiaires, les droits d'accès au système d'information informatique et au système de téléphonie sont déterminés selon le poste occupé , conformément à la réglementation, l'accès au dossier personnel est attribué sur demande écrite, pour la durée strictement nécessaire à la consultation du dossier personnel exclusivement et sur place ; les codes d'accès sont attribués par les cadres de l'établissement ; la présente Charte d'accès et d'usage du système d'information est remise au personnel lors de la procédure de recrutement contre signature ; elle figure également sous forme résumée dans le livret d'accueil du personnel .
- **Pour les prestataires**, Une demande préalable écrite est ainsi requise pour l'attribution d'un accès aux ressources informatiques, aux services Internet et de télécommunication ; la

demande exprimée par l'utilisateur est au préalable validée par son manager, qui précise les accès nécessaires à son collaborateur, et la transmet par écrit à la DSI. Les droits d'accès sont déterminés et attribués selon le contrat signé ; la présente Charte d'accès et d'usage du système d'information est annexée au contrat. Ce droit d'accès est strictement personnel et concédé à l'utilisateur pour des activités exclusivement professionnelles. Il ne peut être cédé, même temporairement à un tiers. Tout droit prend fin lors de la cession, même provisoire, de l'activité professionnelle de l'utilisateur. Le non-respect des dispositions de la présente Charte par l'utilisateur entraine systématiquement une sanction disciplinaire pour le personnel et une rupture du contrat pour le prestataire. Le mauvais usage des droits d'accès est aussi susceptible d'être sanctionné par la loi.

- **Pour les usagers**, les droits d'accès à l'informatique conformément à la réglementation sur l'informatique et les libertés sont attribués sur demande écrite et pour la durée strictement nécessaire à la consultation du dossier personnel exclusivement et en présence d'un agent chargé d'interrompre la consultation en cas de mauvais usage du droit d'accès. Le droit d'accès ne peut être cédé, même temporairement à un tiers. L'obtention d'un droit d'accès au système d'information de l'établissement entraîne pour l'utilisateur les droits et les responsabilités précisées dans les paragraphes ci-dessous.

5.1 CONFIDENTIALITÉ DE L'INFORMATION ET OBLIGATION DE DISCRÉTION

Les personnels de l'établissement sont soumis au secret professionnel et/ou médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données de santé. Les personnels doivent faire preuve d'une discrétion absolue dans l'exercice de leur mission. Un comportement exemplaire est exigé dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux qui sont publics ou partagés. Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électronique dont l'utilisateur n'est ni directement destinataire, ni en copie.

L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielles couvertes par le secret professionnel.

5.2 PROTECTION DE L'INFORMATION

Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Il est important de ne stocker aucune donnée ni aucun document médical sur ces postes (disques durs locaux). Les bases de données associées aux applications sont implantées en partie sur des serveurs centraux situés dans une salle protégée, et en partie stockées dans des sites externalisés. De même, les

documents bureautiques produits doivent prioritairement être stockés sur le serveur de fichiers. Cet espace est à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.
Le cas échéant, ceux qui utilisent un matériel portable (exemples : poste informatique, tablette, smartphone…) ne doivent pas le mettre en évidence pendant un déplacement ni exposer son contenu à la vue d'un tiers ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, disquette, clé, disque dur…). Aucune donnée de santé à caractère personnel des usagers ne doit être stockée sur des postes ou périphériques personnels.
Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.
Les médias de stockage amovibles (exemples : clés USB, CD-ROM, disques durs…) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données. Leur usage doit faire l'objet d'une très grande vigilance. L'établissement se réserve le droit de limiter, voire d'empêcher, l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques, en cas d'utilisation itérée de clés USB potentiellement contaminées sans autorisation de la direction.
L'utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaîtrait pas, même s'il s'agit d'une adresse électronique interne à l'établissement. Il doit vérifier systématiquement la fiabilité des mails qu'il reçoit avant leur ouverture.

5.3 USAGES DES RESSOURCES INFORMATIQUES

Seules des personnes habilitées de l'association ou par son intermédiaire la société avec laquelle elle a contracté) ont le droit d'installer de nouveaux logiciels, de connecter de nouveaux PC au réseau de l'établissement et, plus globalement, d'installer de nouveaux matériels informatiques.
L'utilisateur s'engage à ne pas modifier la configuration des ressources (matériels, réseaux, …) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées de l'établissement (ou par son intermédiaire la société avec laquelle il a contracté).
Les logiciels commerciaux acquis par l'association ne doivent pas faire l'objet de copies de sauvegarde par l'utilisateur, ces dernières ne pouvant être effectuées que par les personnes habilitées de l'association.
L'utilisation de matériels ou logiciels personnels doit impérativement être autorisée préalablement.

- **Le poste de travail**
  Dans le cadre de sa mission, un collaborateur peut se voir fournir un ou plusieurs postes de travail, fixes ou nomades. Il est de son devoir d'appliquer les règles de bonne pratique liées à ce type de matériel.
  Notamment, le collaborateur doit:

- ✓ Veiller à conserver en bon état de fonctionnement le matériel et les logiciels mis à sa disposition,
- ✓ Veiller à ce que les règles de verrouillage de session soient bien appliquées sur son matériel,
- ✓ Signaler tout dysfonctionnement ou anomalie sur le matériel,
- ✓ S'engager à sécuriser son matériel avec les moyens mis à disposition par la structure.

Le collaborateur ne doit pas :

- ✓ Utiliser les équipements pour un usage personnel, sauf dans les limites fixées par la structure si elle l'a autorisé explicitement,
- ✓ Faire usage de postes de travail pour lesquels il n'a pas été explicitement autorisé. Dans ce cas de figure, les professionnels sont tenus de respecter les règles de sécurité et de protection des données définies par la politique de sécurité du système d'information de l'établissement.

- **Les logiciels et les applications**

L'utilisation de logiciels du commerce est soumise au respect du code de la propriété intellectuelle défini par le législateur. Chaque collaborateur doit avoir conscience:

- ✓ Que l'utilisation de logiciels est soumise à l'acquisition par l'entreprise de licences d'utilisation,
- ✓ Que la loi protège les logiciels contre la copie,
- ✓ Que sa responsabilité civile et pénale sera engagée en cas de copie non autorisée ou de piratage de logiciel,
- ✓ Qu'un logiciel utilisé sans licence, qu'il soit gratuit ou non, est une contrefaçon ou une source d'infection virale, voire d'intrusion par un tiers,
- ✓ Qu'aucune installation de logiciel piraté sur le poste de travail, même pour utilisation à titre personnel, ne sera admise.

- **Les équipements mobiles et de stockage**

L'usage de périphériques type clés USB ou disques externes doit rester exceptionnel :

- ✓ Seuls les périphériques de stockage fournis par la structure sont autorisés,
- ✓ Tout périphérique de ce type doit faire l'objet d'un scan par l'antivirus à chaque utilisation par le collaborateur.

5.4 USAGE DES OUTILS DE COMMUNICATION

Les outils de communication tels que le téléphone, le fax, Internet ou la messagerie sont destinés à un usage exclusivement professionnel. L'usage à titre personnel, dans le cadre des nécessités de la vie privée, est toléré à condition qu'il soit très occasionnel et raisonnable, qu'il soit conforme à la législation en vigueur et qu'il ne puisse pas porter atteinte à l'image de marque de l'association. Il ne doit en aucun cas être porté à la vue des usagers ou de visiteurs et accompagnants.

- **Usage du téléphone et du fax**

  Le téléphone et le fax sont des moyens potentiels d'échanges de données qui présentent des risques puisque l'identité de l'interlocuteur qui répond au téléphone ou de celui qui réceptionne un fax n'est pas garantie.

  Il ne faut ainsi communiquer aucune information sensible par téléphone, notamment des informations nominatives, médicales ou non, ainsi que des informations ayant trait au fonctionnement interne de l'établissement. Exceptionnellement, une communication d'information médicale peut être faite après avoir vérifié l'identité de l'interlocuteur téléphonique. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié, le cas échéant, dans les annuaires d'usagers ou de professionnels.

  La communication d'informations médicales (exemples : résultats d'examens…) aux usagers et aux professionnels extérieurs est strictement réglementée. Les utilisateurs concernés doivent se conformer à la réglementation et aux procédures de l'association en vigueur.

- **Usage d'Internet**

  L'accès à l'Internet a pour objectif d'aider les personnels à trouver des informations nécessaires à leur mission usuelle, ou dans le cadre de projets spécifiques.

  Il est rappelé aux utilisateurs que, lorsqu'ils « naviguent » sur l'Internet, leur identifiant est enregistré. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de l'Internet et de ne pas mettre en danger l'image ou les intérêts de l'établissement.

  Par ailleurs, les données concernant l'utilisateur (exemples : sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'utilisateur…) peuvent être enregistrées par des tiers, analysées et utilisées à des fins, notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle ni aucune coordonnée professionnelle, sur l'Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.

  Il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par l'établissement. Il est interdit de participer à des forums, blogs et groupes de discussion, réseaux sociaux à des fins non professionnelles, et de se connecter sur des sites à caractère injurieux, violent, raciste, discriminatoire, pornographique, diffamatoire ou manifestement contraire à l'ordre public.

  Tous les accès Internet sont tracés, enregistrés et conservés par un dispositif de filtrage et de traçabilité. Il est donc possible pour l'établissement de connaître, pour chaque salarié, le détail de son activité sur l'Internet.

  Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment les sites dangereux pour la sécurité du réseau. Il permet de détecter, de bloquer et/ou de signaler les accès abusifs (en matière de débits, volumes, durées), ou les accès à des sites illicites et/ou interdits.

- **Usage de la messagerie**

  L'usage de la messagerie est autorisé à l'ensemble du personnel. La messagerie permet de faciliter les échanges entre les professionnels de l'établissement.

  Les utilisateurs doivent garder à l'esprit que leurs messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant, constituer une preuve ou un commencement de preuve par écrit, ou valoir offre ou acceptation de manière à former un contrat entre l'établissement et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.

  Un usage privé de la messagerie est toléré s'il reste exceptionnel. Les messages personnels doivent comporter explicitement la mention « privé » dans l'objet. À défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « privé » ne doivent pas comporter de signature d'ordre professionnel à l'intérieur du message.

  L'usage des listes de diffusion doit être strictement professionnel.

  Il est strictement interdit d'utiliser la messagerie pour des messages d'ordre commercial ou publicitaire, du prosélytisme, du harcèlement, des messages insultants ou de dénigrement, des textes ou des images provocants et/ou illicites, ou pour propager des opinions personnelles qui pourraient engager la responsabilité de l'établissement ou porter atteinte à son image. Les utilisateurs sont tenus par leurs clauses de confidentialité et de loyauté contractuelles qui encadrent le contenu des informations qu'ils peuvent transmettre par email.

  Afin de ne pas surcharger les serveurs de messagerie, les utilisateurs doivent veiller à éviter l'envoi de pièces jointes volumineuses, notamment lorsque le message comporte plusieurs destinataires. Seules les pièces jointes professionnelles sont autorisées. Il est rappelé que le réseau Internet n'est pas un moyen de transport sécurisé. Il ne doit donc pas servir à l'échange d'informations médicales nominatives en clair. En l'absence de dispositif de chiffrement de l'information de bout en bout, les informations médicales doivent être rendues anonymes. Il est strictement interdit d'ouvrir ou de lire des messages électroniques d'un autre utilisateur, toutefois pour des raisons de continuité de service, l'adresse mail peut être réattribuée en cas d'absence prolongée d'un collaborateur ou de départ définitif

5.5 USACE DES LOGIN ET DES MOTS DE PASSE

Chaque utilisateur dispose d'un compte nominatif lui permettant d'accéder aux applications et aux systèmes informatiques de l'établissement. Ce compte est personnel. Il est strictement interdit d'usurper une identité en utilisant, ou en tentant d'utiliser, le compte d'un autre utilisateur, ou en agissant de façon anonyme dans le système d'information.

Pour utiliser ce compte nominatif, l'utilisateur, dispose d'un login et d'un mot de passe.

Le mot de passe choisi doit être robuste (8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit être changé tous les 6 mois. Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie, même pour une situation temporaire.

Chaque utilisateur est responsable de son compte et son mot de passe, et de l'usage qui en est fait. Il ne doit ainsi pas mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de l'établissement dont il a l'usage. La plupart des systèmes informatiques et des applications de l'établissement assurent une traçabilité complète des accès et des opérations réalisées à partir des comptes sur les applications médico-sociales, médicales et médico-techniques, les applications administratives, le réseau, la messagerie, l'Internet… Il est ainsi possible pour l'établissement de vérifier *a posteriori* l'identité de l'utilisateur ayant accédé, ou tenter d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.
C'est pourquoi il est important que l'utilisateur veille à ce que personne ne puisse se connecter avec son propre compte. Pour cela, sur un poste dédié, il convient de fermer ou verrouiller sa session lorsqu'on quitte son poste. Il ne faut jamais se connecter sur plusieurs postes à la fois. Pour les postes qui ne sont pas utilisés pendant la nuit, il est impératif de fermer sa session systématiquement avant de quitter son poste le soir.
Il est interdit de contourner, ou de tenter de contourner, les restrictions d'accès aux logiciels. Ceux-ci doivent être utilisés conformément aux principes d'utilisation communiqués lors de formations ou dans les manuels et procédures remis aux utilisateurs.
L'utilisateur s'engage enfin à signaler toute tentative de violation de son compte personnel.

5.6 IMAGE DE MARQUE DE L'ÉTABLISSEMENT

Les utilisateurs de moyens informatiques ne doivent pas nuire à l'image de marque de l'établissement à travers la communication d'informations à l'extérieur, via les moyens informatiques auxquels ils ont accès, en interne ou en externe, ou du fait de leur accès à Internet.

6. INFORMATIQUE ET LIBERTÉS

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès du directeur de l'établissement qui étudie la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévues, les destinataires des données, le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour protéger les données. Le directeur procède ensuite aux opérations de déclaration et d'information réglementaires.
Il est rappelé que l'absence de déclaration de fichiers comportant des données à caractère personnel est passible de sanctions financières et de peines d'emprisonnement.
En cas de non-respect des obligations relatives à la loi Informatique et Libertés, le directeur serait informé et pourrait prendre toute mesure temporaire de nature à mettre fin au traitement illégal ainsi qu'informer la direction générale de l'utilisateur à l'origine du traitement illégal.

7. SURVEILLANCE DU SYSTÈME D'INFORMATION

Les utilisateurs du système d'information de l'établissement sont soumis à plusieurs obligations en ce qui concerne les modalités de mise en œuvre du traitement des données à caractère personnel. De façon générale, les utilisateurs doivent respecter les principes de protection des données de santé et des données à caractère personnel (finalité, pertinence et proportionnalité, conservation limitée, sécurité et confidentialité et respect des droits des personnes).

L'établissement doit par ailleurs se conformer aux procédures liées à l'entrée en vigueur du règlement général de la protection des données (RGPD), et notamment :

Désigner un Délégué à la protection des données) **Mme. Stéphanie Humbert joignable par téléphone au 02 31 23 34 06 ou par Mail : dpo@apaeicf.org ,**

- **Informer les personnes concernées par un traitement de données** (usagers, personnes participant à une recherche, etc.) : l'information doit être délivrée de façon concise, transparente, compréhensible et aisément accessible. Elle doit pouvoir être abordable par le « grand public »,
- **Tenir un registre décrivant les traitements** mis en œuvre et les mesures de mise en conformité de ces traitements.
- **Réaliser une analyse de l'impact du traitement de données,** portant tant sur les risques sécurité et techniques que sur les risques juridiques pour les personnes, avant de mettre en œuvre certains traitements, notamment ceux portant sur des données de santé à grande échelle (dispositifs de télémédecine, traitements portant sur les dossiers des usagers). La liste des types de traitements pour lesquels une analyse d'impact est requise est disponible sur le site de la CNIL.

Dans ce cadre, les utilisateurs doivent notamment :

- **Déclarer les nouveaux traitements de données à caractère personnel** auprès du délégué à la protection des données (DPO) de l'établissement soit le directeur,
- **S'assurer auprès du DPO que l'encadrement contractuel des prestations des tiers fournisseurs** est conforme au RGPD lorsqu'il est chargé du recours à un prestataire de service,
- **Se conformer aux règles de sécurité et de confidentialité des données** définies au sein de l'établissement, dans le respect de la politique générale de sécurité des systèmes d'information), et aux obligations liées à la conservation des données,
- **Signaler auprès du DPO les incidents de sécurité** impliquant des données personnelles.

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment du RGPD et de la loi Informatique et Libertés.

La direction assure la traçabilité de l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition, pour des raisons d'exigence réglementaire de

traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.
Par conséquent, les applications de l'établissement, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- ✓ L'identifiant de l'utilisateur ayant déclenché l'opération,
- ✓ L'heure de la connexion,
- ✓ Le système auquel il est accédé,
- ✓ Le type d'opération réalisée,
- ✓ Les informations ajoutées, modifiées ou supprimées des bases de données en réseau et/ou des applications de l'établissement,
- ✓ La durée de la connexion (notamment pour l'accès Internet).

La direction respecte la confidentialité des données et des traces auxquelles elle est amenée à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.
Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou, de façon plus générale, toute suspicion d'atteinte à la sécurité ou tout manquement substantiel à cette charte, doit être signalé au Responsable de la Sécurité du Système d'Information **Mme. Aurélie Monnier joignable par téléphone au 02 31 91 21 54 ou par Mail : amonnier@apaeicf.org** ainsi qu'une Fiche d'Evènement Indésirable
La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains. Chaque utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les usagers bénéficient d'une prise en charge sécurisée et que leur vie privée, ainsi que celle des personnels, soit respectée.

8. RESPONSABILITES ET SANCTIONS

Les règles définies dans la présente Charte ont été fixées par la Direction générale de l'association dans le respect des dispositions législatives et réglementaires applicables.
L'établissement ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services Internet décrites dans la Charte. En cas de manquement aux règles de la présente Charte, la personne responsable de ce manquement est passible de sanctions pouvant être :

- Un rappel ou un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, de l'accès aux moyens informatiques,
- Un licenciement et, éventuellement, des actions civiles ou pénales, selon la gravité du manquement.

Outre ces sanctions, la Direction de l'établissement est tenue de signaler toute infraction pénale commise par son personnel au procureur de la République.

Engagement de respect de la charte informatique de l'APAEI de la Côte Fleurie

Je soussigné/e Monsieur/Madame , exerçant les fonctions de au sein de l'APAEI de la Côte Fleurie (ci-après dénommée « l'association »), étant à ce titre amené/e à utiliser des outils informatiques de l'APAEI de la Côte Fleurie, déclare reconnaître avoir pris connaissance de la présente charte.

Je m'engage par conséquent à respecter la charte informatique de l'APAEI de la Côte Fleurie.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires

Fait à , le / / , en 2 exemplaires

Nom :

Prénom

Signature :

Engagement de respect de confidentialité

Je soussigné/e Monsieur/Madame , exerçant les fonctions de au sein de l'APAEI de la Côte Fleurie (ci-après dénommée « l'association »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage 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 du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ✓ Ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes 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 mes fonctions ;
- ✓ Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- ✓ Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- ✓ M'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- ✓ En cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur.

Fait à , le / / , en 2 exemplaires

Nom :

Prénom :

Signature :