Mémo : Règles d'accès et d'utilisation du SI

Résumé de la Charte d'accès et d'usage du SI

1 Objet du document

Ce document est un résumé des règles d'accès et d'utilisation des ressources informatiques. Il est extrait de la charte d'accès et d'usage du Système d'Information (SI) qui est une annexe au règlement intérieur. Cette charte s'applique aux membres du personnel et aux personnels extérieurs. Elle est consultable sur l'Intranet et affichée dans les locaux de l'association.

2 Règles de sécurité

2.1 Accès au Système d'information

L'accès au système d'information de l'association est soumis à autorisation.
Les demandes d'accès aux ressources informatiques, Internet et de télécommunication doivent être validées par un manager ou un directeur d'établissement.
La demande se fait par l'intermédiaire d'un ticket dans le logiciel prévu à cet effet (GLPI).
Le manager précise les accès nécessaires aux collaborateur.

3 Confidentialité et obligation de discrétion

En tant qu'utilisateur du Système d'Information de l'association, vous êtes soumis au secret professionnel et/ou médical.
Vous devez donc :

- Respecter la vie privée des usagers ;
- N'échanger des informations médicales ou personnelles qu'avec des professionnels habilités et qui sont nécessaires à la coordination ou à la continuité des soins et de l'accompagnement médico-social ;
- Faire preuve d'une discrétion absolue dans l'exercice de votre mission ;
- Adopter un comportement exemplaire 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 ;
- Assurer la confidentialité des données que vous détenez.

4 Protection de l'information

- Ne pas stocker de données sur les disques durs locaux des ordinateurs qui ne sont pas sauvegardés ;
- N'utiliser que les logiciels dédiés pour stocker ou traiter des données en relation avec les usagers (Imago, Uni-T, Apologic, etc) ;
- Ne pas exposer le matériel et le contenu de matériels portables (ordinateur, tablette, smartphone) à la vue d'autrui dans des lieux publics ;
- Le matériel (ordinateur, périphériques de stockage mobiles) doit être rangé en lieu sûr ;
- Aucune donnée de santé à caractère personnel des usagers ne doit être stockée sur des postes ou périphériques personnels ;
- L'usage des clé USB et disques durs externes doit être limité et faire l'objet d'une vigilance accrue (vol, virus, perte, etc.) ;
- Ne pas transmettre de fichiers sensibles à une personne inconnue qui en fait la demande, même s'il s'agit d'une adresse électronique interne.

5 Usages des ressources informatique

5.1 Matériel

Que ce soit pour les postes de travail, smartphones, tablettes, vous devez :

- 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 (système antivol, etc.).

Vous ne devez 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 ;
- Modifier les configurations mises en place par le service informatique (matérielles ou logicielles).

5.2 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.
Vous ne devez pas :

- Utiliser des logiciels dont la licence n'a pas été acquise par l'association ;
- Effectuer des copies non autorisées ou pirater des logiciels ;
- Installer des logiciels piratés sur le poste de travail, même pour utilisation à titre personnel ;
- Installer des logiciels sans validation préalable du service informatique.

5.3 Autre

- Il est interdit d'utiliser une quelconque ressource pour télécharger, stocker ou diffuser des œuvres ou des objets protégés par un droit d'auteur ou par un droit voisin (films, musiques, etc.).

6 Usages des outils de communication

6.1 Téléphone et fax

- Ne pas communiquer des informations sensibles sans avoir vérifier au préalable l'identité des interlocuteurs.

6.2 Internet

- Ne communiquer des coordonnées professionnelles qu'en cas de strict nécessité ;
- Ne pas se connecter à Internet par des moyens autre que ceux fournis ;
- Ne pas participer à des forums, blogs et groupes de discussion 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.

6.3 Messagerie

- Ne pas 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'association ou porter atteinte à son image ;
- Ne pas ouvrir ou de lire des messages électroniques d'un autre utilisateur, sauf si ce dernier a donné son autorisation explicite.

7 Usages des équipements mobiles personnels (BYOD)

- Sauf autorisation explicite de l'établissement et du service informatique il est interdit d'utiliser du matériel personnel à des fins professionnelles ;
- Il est interdit de connecter du matériel personnel sur le réseau interne APAJH33 ;
- Seul l'accès aux services en Cloud Public (Imago, Odoo, Octime, Microsoft 365, etc.) est autorisé depuis un appareil personnel, à condition qu'il soit connecté à Internet à partir d'un réseau mobile (3G/4G/5G) ou au domicile de l'utilisateur ;
- Il est interdit d'accéder à des ressources du système d'information de l'APAJH Gironde à partir de points d'accès Wifi publics non protégés ;
- Pour utiliser un appareil personnel, l'utilisateur s'engage à :
  - Utiliser des systèmes à jour, protégés par des logiciels antivirus à jour et de chiffrement des données ;
  - Protéger ses équipements par des codes, mots de passe, schéma de verrouillage ou solution biométriques ;
  - Avertir le service informatique en cas, de vol, perte ou constat d'intrusion.