

CHARTRE INFORMATIQUE

à l'usage des permanents et enseignants

Cette charte informatique fixe les règles à respecter individuellement pour utiliser les ressources informatiques mises à votre disposition, dans le cadre de la **politique de sécurité du système d'information** du groupe scolaire LA CROIX ROUGE LA SALLE

Elle engage personnellement le signataire et, en cas de manquement aux règles définies, l'expose à des sanctions au sens de l'article R 6352-3 du Code du travail.

1. DÉFINITIONS

Sont utilisés dans la présente charte les termes suivants :

SYSTÈME D'INFORMATION : *l'ensemble des ressources* (personnel, logiciels, processus, données, matériels, équipements informatiques et de télécommunication...) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion des informations (textes, images, sons, vidéo...) visant à assurer la mission d'enseignement et les fonctions support au sein du groupe scolaire.

POSTE DE TRAVAIL : ordinateur, tablette ou téléphone mis à disposition par le groupe scolaire LA CROIX ROUGE LA SALLE dans le cadre professionnel.

COMPTE : Ensemble des ressources informatiques attribuées à un UTILISATEUR pour travailler sur un ou plusieurs postes de travail. Un COMPTE est exploité en s'enregistrant auprès d'un système à l'aide de son identifiant et d'un authentifiant tel qu'un mot de passe.

SUPPORT AMOVIBLE : équipement électronique (disque dur externe, clé USB, carte) utilisé pour stocker les données numériques.

ADMINISTRATEUR : membre du service informatique détenant des droits d'installation, de modification ou de mise à jour de logiciels et de configuration sur les postes de travail.

UTILISATEUR : collaborateur ne possédant que des droits restreints de configuration sur les postes de travail.

MESSAGERIE ÉLECTRONIQUE : service permettant la communication interne et externe d'informations, à titre professionnel, par courrier électronique.

DONNÉE A CARACTÈRE PERSONNEL : dénomination, numéro ou une image contribuant à l'identification d'une personne : élève (fichier de classe, évaluations), enseignant, numéro de téléphone, email, collaborateur, vidéosurveillance, image.

CHIFFRER : action de transformer par une opération un fichier numérique pour le rendre illisible par une personne non autorisée. Au sein de société, le cryptage est associé à un mot de passe et le décryptage ne peut s'effectuer qu'à l'aide du mot de passe.

2. RESSOURCES.

Ces règles concernent :

- Les infrastructures informatiques de la CROIX ROUGE LA SALLE et des écoles primaires du groupe : serveur, réseau.
- Le matériel mis à votre disposition : ordinateurs, périphériques, tablettes , vidéoprojecteur ...
- Les logiciels fournis par l'école.
- La messagerie et l'accès internet.
- Le stockage.

Les informations accessibles depuis votre compte d'UTILISATEUR sont personnelles. Le partage et la diffusion de ces informations vous sont personnels.

3.

ENJEUX.

La **politique de sécurité du système d'information** a pour but :

- De protéger le groupe scolaire LA CROIX ROUGE LA SALLE face aux risques de cyberattaques ;
- De garantir la conformité avec le règlement européen 2016/679 du 27 avril 2016 (RGPD) relatif à la protection des personnes physiques à l'égard des traitements de DONNÉES À CARACTÈRE PERSONNEL.
-

En particulier, l'activité scolaire conduit la communauté à manipuler un volume important de DONNÉES À CARACTÈRE PERSONNEL, concernant majoritairement des mineurs. Il est essentiel d'œuvrer collectivement pour préserver la confidentialité de ces données en les manipulant dans le cadre de la sécurité mise en place par le groupe scolaire.

4. USAGES

Les ressources informatiques sont mises à votre disposition par la CROIX ROUGE LA SALLE pour vous fournir les moyens numériques nécessaires à l'enseignement et l'organisation des activités du groupe scolaire. Elles sont normalement adaptées aux besoins.

L'usage des ressources est normalement professionnel. La consultation de sites internet non interdits au paragraphe est autorisée si elle n'a pas d'influence négative sur le travail et la sécurité numérique de l'entreprise.

L'usage des ressources informatiques est encadré par des lois indiquées sur le site de la CROIX ROUGE LA SALLE à l'endroit suivant.

5. SUPPORTS AMOVIBLES ET DONNÉES A CARACTÈRE PERSONNEL

Le fonctionnement *en mode cloud* (hébergement distant) ne nécessite normalement pas l'usage de SUPPORTS AMOVIBLES. Sauf accord du responsable informatique.

Si des SUPPORTS AMOVIBLES contiennent ou sont amenés à contenir des DONNÉES A CARACTÈRE PERSONNEL : ils sont délivrés par le service informatique et disposent d'un marquage **ROUGE**.

Les fichiers numériques contenant des DONNÉES À CARACTÈRE PERSONNEL ne sont stockés sur les POSTES DE TRAVAIL ou des SUPPORTS AMOVIBLES que s'ils sont CHIFFRES.

6. USAGE DE LA MESSAGERIE ÉLECTRONIQUE

L'usage de la MESSAGERIE ÉLECTRONIQUE est professionnel. Les échanges entre adresses de messagerie professionnelle et personnelle sont interdits.

Les messages reçus sur la MESSAGERIE ÉLECTRONIQUE dont l'origine est douteuse sont effacés. Tout fichier bureautique reçu en pièce jointe d'un mail n'est ouvert qu'avec vigilance, en particulier en interdisant l'exécution de « macros ».

Tout message demandant l'exécution d'opération financière ou de communication d'information confidentielle doit faire l'objet d'une vérification quant à l'origine effective de l'émetteur. En cas de doute vous contactez le service informatique.

7. USAGE D'INTERNET

Il est formellement interdit de consulter des sites de rencontres privés, des sites à caractère pornographique, des sites donnant accès à des prestations interdites par la loi (darkweb) et des sites de jeux depuis les POSTES DE TRAVAIL.

Toute consultation de sites faisant l'objet d'une recommandation de blocage de la part du serveur de filtrage (proxy web) est immédiatement interrompue.

Les fenêtres de navigateur s'ouvrant automatiquement signalant la présence d'un virus ou une baisse de performance sont immédiatement fermées.

Il ne faut pas accepter que le navigateur internet propose de conserver vos identifiants et mots de passe pour un compte utilisé sur le navigateur internet.

8. DISPOSITIFS DE SÉCURITÉ

Les dispositifs et logiciels de sécurité installés sur les POSTES DE TRAVAIL ne doivent en aucune circonstance être désactivés.

Les mesures de sécurité physique (fermeture des locaux, stockage dans une armoire fermée à clef) participent à la sécurité. Elles doivent être appliquées dans la mesure du possible.

Le respect de ces mesures peut faire l'objet d'un contrôle de la direction du groupe scolaire et du service informatique à des fins de sécurité de l'entreprise.

9. RÈGLES DE CONFIDENTIALITÉ

La discrétion de la communauté éducative constitue un pan important de la sécurité du SYSTÈME D'INFORMATION. Elle participe également à la cohésion des acteurs.

Dans le cadre privé, les collaborateurs et les enseignants ne communiquent pas sur les réseaux sociaux des informations sur leurs activités au sein du groupe scolaire mettant en danger la sécurité des personnes et des biens ou portant atteinte à la vie privée d'autres membres de la communauté : élèves et parents d'élève en particulier.

Il est interdit de communiquer un mot de passe à une personne directement par mail ou par téléphone même sous la pression d'une personne représentante de l'autorité : tout accès étranger à votre compte s'effectue selon les règles du paragraphe 10 sous le contrôle du **service informatique**.

10. DÉONTOLOGIE DU SERVICE INFORMATIQUE

Le **service informatique** de la CROIX ROUGE LA SALLE a l'accès technique aux ressources. Ses membres sont soumis à une obligation professionnelle de confidentialité.

Dans le respect de la protection des DONNÉES À CARACTÈRE PERSONNEL, le **service informatique** n'effectue pas de surveillance systématique des comptes mis à disposition des UTILISATEURS.

Le **service informatique** peut être amené à conduire des investigations techniques pour détecter l'origine et résoudre un problème de sécurité.

Le **service informatique** peut être amené à faire des contrôles sur des ressources personnelles à la demande du directeur ou des forces de police pour prévenir ou détecter des usages interdits ou des délits.