

2009/2010

CHARTRE DE BON USAGE DE L'INFORMATIQUE ET DU RESEAU DU STIFT

Les équipements informatiques du STIFT, et de ses annexes - paroisse St Thomas et foyer Wilhelmitana - (réseaux filaires et/ou wifi et salle informatique) sont dédiés principalement au travail de bureautique. Tout utilisateur doit respecter certaines règles de sécurité et de bonne conduite, l'imprudence, la négligence ou la malveillance d'un utilisateur pouvant avoir des conséquences graves pour les autres. La charte définit les droits et les devoirs de chacun et représente un engagement mutuel entre l'utilisateur et le STIFT :

Les différents acteurs.

Du point de vue informatique, il faut distinguer quatre catégories d'acteurs dans l'activité du réseau :

- les utilisateurs : les résidents du STIFT et de ses annexes - paroisse St Thomas et foyer Wilhelmitana –
- les administrateurs systèmes et/ou réseau, responsables techniquement du bon fonctionnement des outils informatiques;
- les responsables fonctionnels : l'Aumonier et le Responsable de gestion, le Directeur et les Administrateurs de Chapitre de St-Thomas.
- Les correspondants sécurité du réseau qui sont les prestataires de service ayant réalisé l'installation et assurant sa maintenance.

Chacun a des droits et des devoirs identiques dans l'esprit mais différents dans la pratique.

Les droits de tous.

Chacun a droit à :

- la mise à disposition de la charte,
- l'information relative aux ressources et aux services communs offerts par le STIFT,
- l'information lui permettant d'utiliser au mieux les moyens mis à sa disposition,
- l'information sur la sécurité du système qu'il utilise et son fonctionnement.

- l'information quant à la responsabilité engagée de l'utilisateur,
- l'accès 24h/24h aux réseaux filaires et/ou wifi
- l'accès 24h/24h de la salle informatique (tout en y respectant une limite d'une demi-heure d'utilisation en cas d'affluence et d'attente), d'y imprimer tout document que vous avez créé ou que vous avez le droit de posséder,
- d'explorer les sites légaux du réseau Internet, sans enfreindre la Loi, tout en respectant aussi les devoirs et toutes les règles et conseils énoncés ci-après.

Les devoirs de chacun.

- Chacun doit accepter la présente charte par un document signé et déposé chez le Responsable de gestion pour avoir un accès autorisé au réseau et à la salle informatique.
- Chacun a le devoir de respecter les règles et conseils de sécurité applicables au système qu'il utilise ; ces règles consistent en la présente charte illustrée par des annexes régulièrement actualisées selon vos propositions; ces règles sont tenues à la disposition de chaque utilisateur par le responsable fonctionnel ou l'administrateur système.
- Chacun doit respecter la propriété intellectuelle et commerciale conformément à la législation en vigueur (interdiction formelle de violer le copyright et/ou les droits d'auteur consciemment ou inconsciemment).
- Chacun doit s'informer sur la légalité de ses actes.
- Chacun s'engage à ne pas prendre connaissance d'informations appartenant à autrui sans son accord, à ne pas communiquer à un tiers de telles informations, ou des informations non

publiques auxquelles il peut accéder, mais dont il n'est pas propriétaire (par ex: sur les comptes communs).

- Chacun doit s'identifier clairement, nul n'a le droit d'usurper l'identité d'autrui ou d'agir de façon anonyme. Nul ne peut céder ses droits à autrui.
- Chacun doit s'efforcer de parvenir à son but par le moyen le moins "coûteux" en ressources communes qui vous seront mises à disposition (espace disque, impressions, occupation des postes de travail, transferts réseau, occupation de serveurs...).
- Chacun doit contribuer à l'amélioration du fonctionnement et de la sécurité des outils informatiques, en respectant les règles et conseils de sécurité, en signalant immédiatement aux responsables toute anomalie constatée, en sensibilisant les autres utilisateurs aux problèmes dont il a connaissance.
- Chacun doit se limiter à un usage personnel simple des équipements communs mis à sa disposition et respecter la fonction qui leur est assignée, ce qui exclut l'utilisation dans un but commercial et toute utilisation abusive.
- Nul ne peut modifier un équipement, tant du point de vue matériel que logiciel. Il est donc de même interdit d'ouvrir les unités centrales des ordinateurs de la salle informatique.

Droits et devoirs spécifiques des administrateurs système et/ou du réseau.

Sur de nombreux systèmes, l'administrateur a techniquement tous les pouvoirs, il a de ce fait des devoirs importants, en particulier celui de ne pas abuser de ses pouvoirs. D'après le code pénal, l'administrateur système est personnellement responsable de la sécurité de la machine et/ou du réseau dont il a la charge.

Tout administrateur système a le droit :

- d'être informé des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible,
- d'accéder aux informations privées à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations,

- d'établir des procédures de surveillance de toutes les tâches exécutées, afin de déceler les violations ou les tentatives de violation de la présente charte, après autorisation de son responsable fonctionnel et en relation avec le correspondant sécurité du réseau...
- d'effectuer des tests permettant de mesurer et éventuellement d'améliorer les barrières mises en place et d'éprouver par la même les caractéristiques et la sécurité du réseau dont il a la charge.

Tout administrateur système a le devoir :

- d'informer les utilisateurs sur l'étendue des pouvoirs dont lui-même dispose techniquement de par sa fonction, ceci au moyen de la présente charte, des annexes, d'affiches et/ou de messages informatifs sur les postes,
- d'informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître les règles de sécurité à respecter, aidé par le correspondant sécurité du réseau de la Fondation,
- de respecter les règles générales d'accès aux réseaux,
- de respecter les règles de confidentialité, en limitant l'accès à l'information confidentielle au strict nécessaire et en respectant un "secret professionnel" sur ce point,
- de respecter, s'il est lui-même utilisateur du système, les règles qu'il est amené à imposer aux autres utilisateurs,
- de modifier le système dans le sens d'une meilleure sécurité, dans l'intérêt des utilisateurs,
- d'informer son responsable fonctionnel et/ou le correspondant sécurité de l'exécution d'une phase de test ou d'une action visant à déceler d'éventuelles infractions à la charte.
- d'informer immédiatement son responsable fonctionnel et le correspondant sécurité de toute tentative (fructueuse ou non) de modification des installations (tant en ce qui concerne le matériel que les logiciels), ou de tout comportement dangereux d'un utilisateur ou en cas d'attaque extérieure impliquant le réseau qu'il administre.

Droits et devoirs spécifiques des responsables fonctionnels.

Les responsables fonctionnels de systèmes informatiques ont le droit :

- d'interdire l'accès aux outils informatiques à un utilisateur qui ne respecte pas la présente charte,
- d'informer le CDM.
- De faire appel aux correspondants de sécurité du réseau en cas de problème d'administration ou de maintenance.
- De permettre aux administrateurs l'accès momentané aux données personnelles d'utilisateurs à des fins de contrôles ou de tests.

Les responsables fonctionnels de systèmes informatiques ont le devoir :

- d'informer tous les acteurs, de diffuser la présente charte par tous moyens appropriés,
- de communiquer, au correspondant sécurité du réseau, le nom des responsables système et réseau de toutes les machines,

Règles et conseils de sécurité:

Les règles et les conseils de sécurités ne sont pas exhaustifs, il appartient à votre bon sens, votre appréciation et votre responsabilité personnelle d'agir en conséquence des situations tout en respectant les termes de la charte dans sa totalité.

La salle informatique et les réseaux filaires et/ou wifi servent principalement à écrire vos documents, les imprimer, gérer vos courriels, effectuer des recherches pour vos études, vos travaux (sauf professionnels) ou vos loisirs, tant que les sites consultés restent légaux.

- Il est interdit de stocker, de lire, de consulter ou de créer tout site ou fichier dont le contenu fait appel à la haine ou au meurtre (même pour rire), touchant au racisme, à la pornographie et à la pédophilie et à toute autre activité illégale (crack, warez...). De même il est interdit d'utiliser des mots-clés répondant à ces domaines dans les moteurs de recherche. Des contrôles pourront être effectués qui permettront de retrouver l'auteur de ces tentatives.

- Les virus n'étant pas des jouets il est

- de soutenir de leur autorité les administrateurs système dans leur travail de mise en application de cette charte.

Sanctions encourues en cas de non respect :

Le non respect des règles définies dans cette charte peut entraîner des sanctions de nature :

- disciplinaire :
Les responsables fonctionnels ont pleine autorité pour prendre les mesures conservatoires nécessaires en cas de manquement à la présente charte et interdire aux utilisateurs fautifs l'accès aux moyens informatiques et au réseau.
- pénale :
L'évolution des techniques électroniques et informatiques a conduit le législateur à définir des sanctions pénales d'une grande sévérité à la mesure du risque que peut faire courir aux libertés individuelles, l'usage incontrôlé des fichiers ou des traitements informatiques.

interdit d'en mettre ou d'en faciliter la circulation. D'une manière générale, n'oubliez donc pas de vous assurer que les fichiers contenus dans vos disquettes, clés USB, CD's, courriels ou autres soient vierge de toute infection (volontaire ou involontaire).

- Le Spamming et le Fishing (vol d'informations personnelles) sont des pratiques prohibées. Veillez à effacer ces SPAM, à signaler tout site de fishing aux administrateurs et à protéger vos informations personnelles de telles menaces.

Vos documents htm, html, xls, ods... peuvent contenir des macro-virus qui sont des sous-programmes inscrits en Java ou Visual Basic (VBA), ils ont la puissance d'ordonner l'écrasement de données, voir de toutes ou de les transformer/corrompre; il est donc interdit de créer des applications

VBA ou Java qui font ce genre d'action. Il est aussi déconseillé d'accepter le démarrage de macros que vous n'avez pas créés et/ou qui sont de source incertaine.

- L'installation sauvage de programmes est interdite. Il vous est donc demandé de consulter les administrateurs-système pour toute proposition d'amélioration du système d'exploitation et de ses composants. Cette mesure est aussi nécessaire pour respecter le droit de propriété (Copyright). Les médias et programmes protégés par les lois de copyright ne doivent pas être violés par le téléchargement et l'enregistrement de MP3 et/ou DivX...

- Seules les personnes ayant remis cette charte signée au Responsable de gestion auront un accès autorisé à la salle et aux réseaux filaires et/ou wifi, vous ne pouvez

permettre à un non-Stiftien non accompagné d'utiliser les installations informatiques du Stift et de ses annexes - paroisse St Thomas et foyer Wilhelmitana. Veuillez signaler tout intrus au Responsable de gestion ou à l'aumonier.

- Le Stift ainsi que les administrateurs systèmes, les responsables fonctionnels et les correspondants réseau ne portent en aucun cas la responsabilité de vos actes faisant appel aux sanctions énoncées.

L'outil informatique offre de multiples possibilités et opportunités, mais vous devez savoir en mesurer les chances et les risques.

Pour tout problème rencontré veuillez vous adresser aux responsables fonctionnels.

Cette charte, partie intégrante du règlement interne du STIFT et de ses annexes - paroisse St Thomas et foyer Wilhelmitana - est portée à la connaissance de tous les utilisateurs et s'impose à tous.

Adoptée par le Conseil de Maison le 10 janvier 2005, modifiée en août 2008 et en juin 2009

Ajouter paraphe au bas des trois pages précédentes

Ajouter la mention manuscrite : « Lu et approuvé »

à : le :

Nom :

Prénom :

Chambre :

Signature