Charte Informatique du Diocèse d'Annecy

1- Domaine d'application

Les règles et obligations définies dans cette charte s'appliquent à tout utilisateur des moyens informatiques du diocèse d'Annecy ainsi que des ressources extérieures accessibles via les réseaux informatiques : Internet, Intranet, transferts de fichiers ftp, messagerie électronique, forums électroniques (news), espaces de discussion (chat), etc.…

L'utilisateur d'un service informatique est une personne physique (personne humaine à laquelle sont attribués des droits) pouvant être salariée, en mission ou bénévole. Cette personne après identification utilise un outil informatique ou tout système permettant d'effectuer un traitement d'information pour consulter, modifier ou créer des données dans le système d'information existant.

2 - Conditions d'accès

Le droit d'accès à un système informatique est soumis à autorisation ; il peut être personnel ou générique ; il est incessible et disparaît lorsque les raisons de cet accès disparaissent. Ce droit est limité à des activités conformes aux missions de l'établissement (enseignement, recherche, administration).

La connexion d'un système informatique au réseau doit se faire avec l'approbation de la personne en charge des réseaux informatiques du lieu où se connecte le matériel informatique mais également du responsable du Service informatique du diocèse d'Annecy lorsque les informations consultées proviennent des serveurs de l'évêché ou de toute source d'hébergement sous contrat avec le diocèse d'Annecy.

Les mots de passe permettant à un utilisateur de se connecter au réseau sont uniques, personnels et confidentiels. Ils ne doivent pas être divulgués à un tiers, l'utilisation qui en est faite est limitée à des fins professionnelles. Elle se fait sous l'entière responsabilité de son détenteur.

En cas de perte ou de vol de son identifiant et mot de passe, la personne doit informer, dans les plus brefs délais par écrit (courrier, email ou fax) le Service Informatique du diocèse d'Annecy pour que son compte soit suspendu ou pour procéder à la génération d'un nouveau mot de passe.

3 - Confidentialité

Chaque utilisateur doit veiller à ne pas diffuser d'informations sensibles ou confidentielles sur les activités du diocèse d'Annecy.

Les fichiers d'un utilisateur doivent être considérés comme privés même s'ils sont accessibles à d'autres utilisateurs.

L'utilisation des fichiers d'un utilisateur exige l'accord formel de ce dernier.

La confidentialité et l'intégrité des données véhiculées sur Internet ne sont pas garanties.

Les documents personnels ne doivent en aucun cas figurer sur le réseau. Il est cependant toléré que des documents personnels soient ponctuellement stockés sur le poste informatique en local sous réserve que les données stockées respectent de par leurs contenus et leurs origines les règles légales en vigueurs et que ces données de par leurs quantités ne nuisent pas aux performances du matériel hébergeant ces informations. Dans ce cas l'utilisateur est seul responsable de la pérennité des informations stockées.

Les membres du Service informatique du diocèse d'Annecy ainsi que tout prestataire intervenant pour le compte du diocèse d'Annecy, sont tenus de respecter la confidentialité des informations dont ils pourraient avoir à prendre connaissance lors de leur travail.

4 - Respect des règles de la déontologie informatique

Chaque utilisateur s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- De s'approprier le mot de passe d'un autre utilisateur ;

- D'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau sans leur autorisation ;
- De porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocantes ;
- D'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ;
- De modifier ou de détruire des informations sur un des systèmes ;
- De se connecter ou d'essayer de se connecter sur un site sans y être autorisé ;
- D'utiliser ou de réaliser un programme informatique ayant comme finalité le piratage ou l'accès à des informations non autorisées.

Tout utilisateur est responsable de l'utilisation des ressources informatiques ; il s'engage à ne pas effectuer des opérations pouvant nuire au bon fonctionnement du réseau, à l'intégrité de l'outil informatique et aux relations internes et externes du lieu où il se connecte.

Ceci concerne notamment l'utilisation des espaces disques sur les serveurs du réseau du diocèse d'Annecy : les répertoires utilisateurs sont dédiés au stockage des données, ils font l'objet de quotas étant donné que les espaces disques sont limités et afin d'assurer une répartition la plus équitable possible des ressources entre tous.

Ces répertoires utilisateurs en réseau ne sont pas destinés à l'installation de logiciels (uniquement des données), contactez le Service Informatique du diocèse d'Annecy pour de telles demandes.

L'usage de la messagerie électronique est à caractère professionnel. Il est également soumis aux règles déontologiques habituelles, les boîtes aux lettres des abonnés sont limitées en taille afin de ne pas saturer les serveurs et garantir un service équitable pour tous. Les pièces jointes éventuellement annexées aux messages e-mail sont tenues de respecter une taille et un format adéquat afin de ne pas engorger les réseaux, les serveurs de messagerie sont de garantir au destinataire du message un temps de téléchargement raisonnable. Les utilisateurs peuvent suivant les cas soit récupérer leurs e-mails via un logiciel de messagerie classique soit les consulter directement sur le serveur messagerie via un navigateur internet solution appelée Webmail. Dans ce cas, les données de messagerie sont conservées sur le serveur messagerie ; l'utilisateur a en charge de veiller à nettoyer régulièrement sa boîte e-mail afin d'éviter qu'elle ne soit saturée et quelle ne puisse recevoir de nouveaux messages.

La sécurité est l'affaire de tous, chaque utilisateur du réseau informatique du diocèse d'Annecy doit y contribuer et mettre en application les règles de bon sens et les recommandations fournies par les membres du Service informatique du diocèse d'Annecy.

Des audits de sécurité sur l'infrastructure réseau (serveurs, analyses réseau) peuvent être effectuées par le personnel du service informatique en cas d'anomalie ou dans le cadre de prévention des risques.

L'utilisateur est responsable de l'usage qu'il fait des données qu'il récupère sur internet par l'intermédiaire du réseau informatique du diocèse d'Annecy, notamment en termes de droit de reproduction, d'utilisation, de détournement éventuel de ces informations, et sur la nature de ces informations.

5 – Utilisation des données personnelles

Dans le cadre du Règlement Générale pour la Protection des Données applicable et opposable depuis le 25 mai 2018, la réalisation de fichier intégrant des données à caractère personnel doit respecter le cadre de ce règlement. Ce traitement doit être documenté dans une fiche de registre de traitement et doit être présente dans le registre des traitements qui regroupe l'ensemble des traitements de données à caractère personnel de l'association diocésaine. Pour cela la réalisation de liste ou de fichier de données personnelles devra être soumis à l'approbation du responsable de traitement ou du délégué à la protection des données (DPO).

6 – Utilisation de logiciels

L'utilisateur ne peut pas installer de logiciel sans en faire la demande au service informatique du diocèse d'Annecy.

Tout logiciel non vérifié ni approuvé par le service informatique sera supprimé. Les logiciels comme MSN, de Chat ou de téléchargement sont formellement interdits.

L'utilisateur ne devra en aucun cas :

- Installer des logiciels à caractères ludiques ;

- Faire une copie d'un logiciel commercial ;
- Contourner les restrictions d'utilisation d'un logiciel ;
- Développer des programmes constituants ou s'apparentant à des virus ;
- Se connecter sur des sites à caractère raciste, pornographique, pédophile, moralement répréhensibles ou illégaux.

7 – Information des utilisateurs sur la gestion des systèmes et réseaux informatiques

7.1 - Responsabilités des administrateurs systèmes / réseau / SGBD

Les administrateurs sont les personnes qui gèrent les ordinateurs connectés au réseau du diocèse d'Annecy ainsi que les serveurs sur lesquels sont installés les différents services mis à disposition des utilisateurs (services internet, application de gestion comptable et paroissiale, …).

Les administrateurs ont la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Ils ont le droit d'entreprendre toute démarche nécessaire au bon fonctionnement des moyens informatiques.

Les administrateurs ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.

Les administrateurs ont la possibilité pour certaines interventions de prendre en main à distance le poste informatique des utilisateurs, sous réserve de l'accord donné par les utilisateurs à chaque opération.

Les administrateurs s'engagent à respecter la confidentialité des fichiers des utilisateurs.

7.2 - Fichiers de traces

L'ensemble des services utilisés génère, à l'occasion de leur emploi, « des fichiers de traces ». Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations comme, par

exemple : les heures de connexion aux applications, numéro de la machine depuis laquelle les services sont utilisés, etc.

Ce type de traces existe pour l'ensemble des services Internet et Intranet. Ces fichiers ne sont utilisés que pour un usage technique et pour identifier toutes anomalies pouvant mettre en péril la sécurité du réseau. Toutefois, dans le cadre d'une procédure judiciaire et après accord de l'économe diocésain, ces fichiers peuvent être mis à la disposition ou transmis à la justice.

Le Service informatique du diocèse d'Annecy, dans le cadre de sa mission, s'assure du bon fonctionnement de l'ensemble des moyens informatiques, sous couvert de son responsable, l'économe diocésain. Il est habilité à effectuer des audits sur leurs contenus pour des besoins techniques et de sécurité, de contacter l'utilisateur en cas d'abus et d'engager des actions pour y remédier (dépassement des quotas de stockage, présence de programmes en violation avec les droits du copyright, à caractère moralement répréhensible ou de logiciels à usage de piratage informatique).

7.3 - Les virus

Des outils sont également mis en place pour protéger les postes des utilisateurs contre les virus.

- Les logiciels antivirus sur les postes des utilisateurs sont paramétrés avec la stratégie suivante : si un virus est détecté, le logiciel tente de réparer le fichier, si la tentative échoue, le fichier est mis en quarantaine et les administrateurs sont prévenus.
- Un logiciel d'antivirus est également mis en place sur les serveurs.
- D'autres logiciels pourront être mis en place pour protéger au mieux les données des utilisateurs et les applications.

7.4 - Les sauvegardes

Les données situées sur les serveurs sont elles-mêmes sauvegardées sur plusieurs sources de sauvegarde afin d'assurer un niveau maximum de sécurité. Ces sauvegardes sont sous la responsabilité du Service Informatique du diocèse d'Annecy. Seule, la sauvegarde des données locales d'un poste est autorisée.

Les copies illicites constituent un délit de contrefaçon.

8 - Informatique et Libertés & Règlement général pour la Protection des données (RGPD)

Si l'utilisateur d'un système informatique veut mettre en place, conserver, divulguer un fichier de données à caractère personnel, il doit respecter le cadre légal et notamment, effectuer les formalités requises si besoin et requérir l'autorisation de l'intéressé sous peine de poursuites notamment pour atteinte à l'intimité de la vie privée. (Articles 226-16 et 226-22 du code pénal).

Depuis le 25 mai 2018, date de la mise en place du Règlement Général pour la Protection des Données (RGPD), toute structure ou établissement a l'obligation de tenir à jour pour chaque traitement, qui concerne des données à caractère personnel, une fiche de registre de traitement simplifié. Dans cette fiche sera spécifié notamment : le nom du responsable de traitement, sa finalité, la durée de conservation des données, les services impliqués et les destinataires, l'intervention de sous-traitant et les échanges hors de Union Européenne. L'ensemble dans un registre de traitements. Ces pièces seront à fournir en cas de contrôle par la CNIL.

Pour plus d'informations, contacter le Service informatique du diocèse d'Annecy ou le délégué à la protection des données (DPO) à Evêché – 5 Bis Avenue de la Visitation – 74000 – ANNECY – Email : dpo@diocese-annecy.fr.

Sanctions applicables

La loi, les textes règlementaires, le règlement intérieur, tout document contractuel ou ordre de mission annexant la présente charte définissent les droits et obligations des personnes utilisant les moyens informatiques.

Tout utilisateur n'ayant pas respecté la loi pourra être poursuivie pénalement. Les utilisateurs ne respectant pas les règles et obligations définies dans la charte sont également passibles d'une procédure disciplinaire inhérente à leur statut ainsi qu'au retrait de l'accessibilité à leur compte informatique.

Lois françaises

Cette charte s'appuie sur les lois actuelles en vigueur et sur toutes évolutions futures faisant référence à ces lois. Ces informations sont consultables via internet sur les sites en référence ou directement auprès du Service Informatique du diocèse d'Annecy.

Lois relatives à l'informatique, aux fichiers et aux libertés.

(cf. http://www.cnil.fr)

- loi n° 78-17 du 6 janvier 1978
- loi n°2004-801 du 6 août 2004

Règlement Général pour la Protection des Données (Règlement Européen applicable le 25 mai 2018)

(https://www.cnil.fr/fr/rgpd-notions-cles-et-bons-reflexes)

La législation relative à la fraude informatique (article 323-1 à 323-7 du Code pénal)

(cf. http://www.legifrance.gouv.fr/citoyen/code.ow, puis "code pénal", "chapitre III : Des atteintes aux systèmes de traitement automatisé de données")

La législation relative à la propriété intellectuelle

(cf.http://www.legifrance.gouv.fr/citoyen/code.ow puis "code de la propriété intellectuelle")

La législation applicable en matière de cryptologie

(cf.http://www.telecom.gouv.fr/francais/activ/techno/crypto0698_1.htm)