Guide pour la gestion des courriels (mails, courriers électroniques) et des données numériques

Conseil synodal de l'Église catholique-chrétienne de la Suisse

Ci-après nous utilisons « @christkatholisch.ch » pour l'adresse e-mail. Cependant, cette adresse doit être entendue comme désignant toutes les adresses « catholiques-chrétiennes » comme par exemple @catholique-chretien.ch ou @ckjs.ch etc.

1. Pourquoi @christkatholisch.ch ?

Avec une adresse @christkatholisch.ch nous soulignons le fait qu'il s'agit d'une communication électronique professionnelle et qu'elle ne vient pas d'une personne privée. Pour le travail au sein de l'Église catholique-chrétienne ce sont les seules adresses à utiliser.

Ainsi, nous respectons les dispositions strictes de la protections des données et des droits personnels.

2. Pourquoi un compte-mail et pas de retransmission ?

La retransmission d'une adresse @christkatholisch.ch à une adresse e-mail privée n'est pas permise parce que la réponse à un tel message retransmis viendrait d'une adresse e-mail privée et par conséquent ne respecterait pas le point 1.

Pour votre travail au sein de l'Église catholique-chrétienne nous mettons à votre disposition un compte-mail. Ce service, ainsi qu'une éventuelle assistance sont gratuits pour vous. Vous pouvez donc répondre en utilisant l'adresse @christkatholisch.ch

3. Adresse e-mail privée contre adresse de fonction

Les adresses e-mail personnelles sont attribuées à des personnes ; une adresse e-mail de fonction est une adresse « impersonnelle » par exemple « finanzverwaltung.fricktal@christkatholisch.ch ».
L'avantage des adresses de fonction est que ces adresses peuvent être indiquées dans des publications. Au cas de changement de personnes au sein de cette administration, l'adresse ne doit pas être changée. Le compte e-mail peut facilement être transféré à une nouvelle personne qui, par conséquent, dispose de toute la correspondance à ce jour.

4. Envoi à tous les destinataires / CCI

Si vous envoyer un message à beaucoup de personnes, veuillez utiliser le mode CCI de votre messagerie ou messagerie web (webmail) et non le mode « à ». Tous les destinataires peuvent voir les adresses aux champs À ou CC. Cela pourrait inviter un éventuel auteur de messages indésirables de profiter de ces adresses. Si vous reprenez les destinataires au champ CCI, les adresses sont invisibles. CCI veut dire « copie conforme invisible » ou « copie cachée » (BCC = Blind Carbon Copy).

5. Listes de diffusion

Une tout autre chose sont les listes de diffusion : vous pouvez vous faire organiser une liste de diffusion par votre équipe web. Cela pourrait être utile par exemple pour le conseil de paroisse, une commission ou pour un bulletin d'information. Vous pouvez alors envoyer un message à toutes les adresses mail figurant sur la liste de diffusion. Vous pouvez aussi faire organiser la façon d'envoyer une réponse (de nouveau aux adresses de la liste ou à une autre adresse).

En utilisant une liste de diffusion pour le bulletin d'information, les personnes intéressées peuvent s'abonner elles-mêmes à cette liste. Cette possibilité peut être mise en œuvre sur le site web de votre paroisse.

6. Messagerie web (Webmail)

Naturellement, chaque compte-mail est aussi accessible en ligne par webmail. Ouvrez la page https://webmail.hostpoint.ch et connectez-vous avec votre nom d'utilisateur et votre mot de passe. Ensuite vous pouvez accéder à tous vos messages.

7. Intégrer votre compte-mail

Vous pouvez intégrer votre compte-mail dans l'ordinateur personnel ou Mac ou bien votre smartphone. Les instructions sont disponibles sur notre page d'assistance → Lien (possibilités de prise de contact voir point 11). Pour l'intégration il est conseillé d'utiliser toujours le « protocole IMAP ». Ainsi, les messages restent sur le serveur-mail christkatholisch et tous les appareils intégrés sont au point.

Une fois intégrés, vous pouvez sans problèmes écrire des messages avec pour expéditeur @christkatholisch.ch.

Si vous êtes en vacances, vous pouvez, pendant ce temps, tout simplement masquer le compte professionnel dans votre messagerie ou votre appli mail.

8. Répondeur automatique / réponses automatiques d'absence

Tous nos comptes-mail @christkatholisch vous offrent la possibilité d'envoyer un message automatique aux personnes vous envoyant un courriel. Pour l'organiser, il vous faut vous connecter en ligne à votre compte-mail via notre webmail (voir point 6).

9. Messages indésirables

Malheureusement notre infrastructure mail n'est pas à l'abri de messages indésirables (spam mail). Nous travaillons en étroite collaboration avec notre hébergeur (Hostpoint) et nous essayons de bloquer autant de messages indésirables que possible. Il est regrettable que les auteurs de messages indésirables deviennent de plus en plus malins et ont mis au point un éventail de plus en plus large de méthodes pour diffuser leurs messages indésirables.

Dans votre compte-mail les messages indésirables sont déposés dans le dossier spam et effacés après trois jours.

Veuillez noter svp les autres informations à ce sujet sous le point 12.2.

10. Gestion de mot de passe

Il est conseillé d'utiliser un mot de passe unique pour chaque compte en ligne. Cela ne s'applique non seulement aux comptes-mail, mais aussi à tous les comptes en ligne que vous avez auprès de maisons de vente par correspondance, auprès de médias sociaux etc.

Pour ne pas perdre le contrôle, il y a des gestionnaires de mots de passe respectivement des applis (par exemple KeePass etc.). Ces gestionnaires sauvegardent tous les mots de passe qu'il vous faut pour vous connecter à des pages web et ils sont protégés par un mot de passe maître. Les gestionnaires vous aident aussi à créer des mots de passe sûrs.

Intégrés dans votre logiciel de navigation (Firefox, Chrome etc.) les gestionnaires entrent automatiquement le mot de passe correspondant lors de la connexion aux pages choisies. Il vous faut alors seulement mémoriser le mot de passe maître.

11. Contact avec l'équipe web / assistances

Si vous avez une question ou une préoccupation, n'hésitez pas à vous adresser à notre équipe web avec l'adresse support@christkatholisch.ch

Vous trouverez également de l'assistance sur notre site support https://christkatholisch.ch/support

12. D'autres conseils utiles au sujet d'e-mail, Internet et mots de passe

12.1 Gestion de mot de passe

1. Les mots de passe de tous les comptes-mail devraient être changés une fois par an au minimum et toutefois pas en même temps.

2. Les nouveaux mots de passe (état 2019) devraient avoir une longueur de 8 caractères au moins.

3. La séquence de caractères devrait être composée (si techniquement possible) de majuscules, minuscules, caractères spéciaux (/ - !+ ? etc) ainsi que de chiffres.

4. Les caractères ne devraient pas se répéter à l'intérieur d'un mot de passe (« 555222nN=== » serait un mot de passe très faible).

5. Les mots de passe doivent être conservés en lieu sûr.

   1. Au cas où vous utilisez un fichier électronique pour ce faire, vous ne devriez pas le sauvegarder sur un ordinateur relié à Internet, mais plutôt sur un disque dur externe, une clé USB qui est seulement utilisée lorsque l'ordinateur est temporairement déconnecté d'Internet.

   2. Alternativement, vous pouvez utiliser un logiciel de gestion de mot de passe qui entre les mots de passe, s'il le faut, automatiquement dans les pages de connexion par votre navigateur (par exemple KeePass).

   3. Le mot de passe maître de ce logiciel doit être choisi de manière extra sûre.

12.2 Gestion de messages

1. Pour des raisons de sécurité il est déconseillé d'ouvrir des courriels provenant d'expéditeurs inconnus.

2. Il faut toujours vérifier si le nom indiqué dans l'entête du message (par exemple « CHK Webmaster ») correspond avec l'adresse indiquée à droite (par exemple « webmaster@christkatholisch.ch »).
   Les courriels indésirables ou spam-mails contiennent souvent des noms faux (par exemple « prénom.nom@christkatholisch.ch). A leur droite se trouve l'adresse réelle de l'auteur du spam-mail (par exemple « conem@infoflood.co.uk »).

3. N'effacer pas simplement les spam-mails. Si possible, marquez-les en tant que spam dans votre messagerie, déplacez-les dans votre dossier spam et effacez-les là. Ainsi, au fil du temps, votre messagerie apprendra à mieux reconnaître les messages indésirables.

4. Dans l'idéal, les pièces-jointes sont d'abord sauvegardées sur l'ordinateur et ouvertes après. Le logiciel de sécurité de votre ordinateur peut vérifier la pièce jointe au moment qu'elle est ouverte.

12.3 État de sécurité

Le portail Internet https://haveibeenpwned.com donne la possibilité aux internautes de vérifier si et quand une adresse mail d'une base de données protégées (par exemple auprès d'une boutique en ligne) a été compromise à la suite d'une violation de données par des pirates informatiques (hacker). Si cela est arrivé récemment, le mot de passe pour cette boutique en ligne devrait être changé immédiatement.

12.4 Internet

1. Il est vivement conseillé d'installer un moteur antivirus sur votre ordinateur ! Ces moteurs parcourent les programmes téléchargés à la recherche de virus et de logiciels malveillants. Une mise à jour à base régulière du moteur antivirus fait partie d'une gestion responsable.

2. En principe, le téléchargement (download) d'Internet est potentiellement dangereux. S'il le faut, les fichiers ou dossiers téléchargés peuvent être vérifiés après le téléchargement à l'aide d'un moteur antivirus en ligne (par exemple https://www.virustotal.com). Cet outil examine vos téléchargements avec plus de 50 différents antivirus, toujours actualisés. Pour faire cela, il vous faut charger (upload) votre fichier à vérifier à l'auditeur. Par conséquent, il n'est pas conseillé de faire examiner des fichiers privés.

3. Il est possible que des sites web ont été compromises par des pirates informatiques (hacker). Pour être sûr que l'on voie le site désiré quand on ouvre un site via l'adresse Internet (par exemple www.christkatholisch.ch), on peut cliquer sur l'information concernant le certificat de sécurité (dans le navigateur à gauche de l'adresse Internet). Là, vous trouvez, entre autres, des informations sur le « propriétaire » du certificat de sécurité. Si ces informations s'écartent fortement de ce que vous présumer de l'exploitant du site, il est possible que le site ait été compromis.

4. Il existe une adresse Internet https://www.whois.com qui peut vous fournir des informations sur un exploitant respectivement un propriétaire d'un site web.