

Table des matières

I. Règles d'utilisation	1
A. Adresses électroniques	1
B. Contenu des messages électroniques	2
C. Émission et réception des messages	2
D. Statut et valeur juridique des messages	2
E. Stockage et archivage des messages	2
F. Sécurité antivirale	2
G. Traçabilité	2
H. Durée de vie des comptes	2
I. Renvoi des messages sur un compte extérieur	3
J. Limitations sur les messages	3
K. Limitations sur les boîtes	3
II. Aide à l'utilisation	3
A. Les outils	3
1. Le Webmail	3
2. Un client de messagerie (Thunderbird, Outlook,...)	3
B. Quota	4
C. Envoyer des pièces jointes de taille importante	5
D. Rediriger ma messagerie	5
E. Notifier une absence	5
F. Se protéger des spams	6
G. Détecter les messages frauduleux (phishing ou hameçonnage)	6
H. Changer de mot de passe	7

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'institution. Ainsi, chaque personnel de l'académie dispose d'une boîte mail avec une adresse du type 'prenom.nom@ac-besancon.fr'. Cette boîte permet de correspondre avec vos interlocuteurs dans le respect de la charte d'utilisation. Le ministère, votre administration et les organisations syndicales sont susceptibles de diffuser des informations par ce biais.

I. Règles d'utilisation

A. Adresses électroniques

L'institution s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'élément nominatif de l'adresse électronique constitue le prolongement de l'adresse administrative et n'a pas pour effet de retirer le caractère professionnel de la messagerie. L'attribution d'une adresse électronique peut aussi correspondre à une boîte générale fonctionnelle ou organisationnelle exploitée par un service ou un groupe d'utilisateurs. La gestion des adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe « d'utilisateurs », relève de la responsabilité exclusive de l'institution : elles ne peuvent être utilisées sans autorisation explicite.

B. Contenu des messages électroniques

Les messages électroniques permettent d'échanger principalement des informations à vocation professionnelle liées à l'activité directe de l'institution. En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux. Tout message à caractère strictement privé, reçu ou émis, doit comporter en objet la mention « Privé » ou tout autre terme indiquant sans ambiguïté le caractère privé du message. Tout message ne comportant pas cette mention est réputé être un message professionnel. Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature et notamment les contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui. Les messages échangés par les organisations représentatives des personnels sont régis par une charte spécifique relative à l'utilisation des moyens de communication électronique.

C. Émission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages. Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

D. Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, constituer une preuve ou un commencement de preuve. L'utilisateur doit en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

E. Stockage et archivage des messages

La messagerie académique est un système permettant l'échange de message, elle n'a pas pour vocation d'être un système de stockage. Chaque utilisateur est responsable de l'archivage et du classement des messages qu'il a relevés et doit donc en conséquence organiser lui-même la conservation des messages. (cf chapitre II / B Quota »).

F. Sécurité antivirale

De manière générale, il est déconseillé d'ouvrir des fichiers, de quelque nature que ce soit en provenance d'un expéditeur inconnu. Dans le cas d'un expéditeur connu, ces conseils restent valables si le texte du message d'accompagnement n'annonce pas de manière explicite le contenu de la pièce jointe. En particulier, les fichiers compressés (extension en .zip par exemple) ou exécutables (extension .exe, .com, .pif...) peuvent générer l'activation de virus informatiques, code malicieux susceptibles d'entraîner des conséquences d'une extrême gravité. Les utilisateurs sont informés que le service informatique se réserve le droit de retenir, d'isoler et/ou de supprimer tout message à l'aide de moyens automatisés et ce, sans que ces messages n'aient été nécessairement ouverts, afin de vérifier qu'ils ne comportent pas de virus. D'une manière générale les utilisateurs sont informés que tout messages bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit. Les administrateurs sont autorisés, en cas de difficultés majeures, à arrêter les services réseaux.

G. Traçabilité

L'institution est dans l'obligation légale de mettre en place un système de traçabilité (système de journalisation) de la messagerie et des données échangées. Les traces ou données de connexion font l'objet d'une déclaration auprès de la CNIL : leur durée de conservation est conforme à la réglementation en vigueur.

H. Durée de vie des comptes

Les comptes nominatifs sont supprimés un an après le départ de l'académie (mutation ou retraite). Les utilisateurs concernés recevront un message d'avertissement deux mois avant l'échéance. Les comptes non

nominatifs peuvent être supprimés dès la constatation d'une période d'inactivité de six mois. Une boîte de messagerie est considérée en activité dès que l'on constate un accès en consultation des messages reçus.

I. Renvoi des messages sur un compte extérieur.

Si l'utilisateur renvoie ses messages sur un compte de messagerie extérieur, il est demandé de ne pas conserver les messages sur le serveur académique. Dans le cas où l'option du WEBMAIL « Ne pas laisser de copie sur le serveur » n'est pas activée, l'administrateur de la messagerie peut activer celle-ci après une période d'inactivité de quatre mois.

J. Limitations sur les messages

La taille maximum d'un message en émission est de 10 méga octets. La taille maximum d'un message en réception est de 10 méga octets. Afin de lutter efficacement contre les virus, l'envoi et la réception de pièces jointes ayant les extensions .exe, .com, .pif, .reg, .scr, .vbs est interdite. Le destinataire d'un message concerné par cette interdiction sera informé de la non distribution du message. En cas d'alerte de sécurité, tous les messages concernés par cette alerte, soit du fait du contenu du message, soit du fait de l'extension des pièces jointes peuvent être temporairement interdits. Il est donc conseillé lors d'envoi volontaire de ce type de pièces jointes de renommer le fichier et d'avertir explicitement le destinataire du contenu de la pièce jointe et de l'opération de changement d'extension à effectuer.

K. Limitations sur les boîtes

Afin de garantir un fonctionnement professionnel de la messagerie électronique, la taille de chaque boîte aux lettres est limité par un dispositif de quota. La taille par défaut est de 1Go. Les utilisateurs sont avertis lorsque leur boîte atteint un seuil critique (90% de taux de remplissage) et peuvent à tout moment consulter le niveau d'utilisation via le webmail académique. Lorsqu'une boîte est saturée, plus aucun message ne lui est transmis et aucun processus de récupération de ces messages n'existe au-delà d'une période de 5 jours : ils sont donc perdus. (cf chapitre II- B Quota »).

II. Aide à l'utilisation

A. Les outils

1. Le Webmail

Le webmail est une interface web permettant de gérer vos messages par l'intermédiaire d'un navigateur. Le webmail appelé convergences est accessible via le pia : <https://pia.ac-besancon.fr> (icône « messagerie académique »)

2. Un client de messagerie (Thunderbird, Outlook,...)

Sur un ordinateur (Thunderbird ou Outlook) ou sur une tablette, un smartphone (Client par défaut apple, android...), il existe deux méthodes pour consulter les messages, le POP et l'IMAP :

	POP	IMAP
Principe	les messages sont téléchargés sur votre appareil	les messages sont conservés sur le serveur
Avantage	Stockage au-delà du quota possible sur l'appareil utilisé	les messages sont consultables depuis n'importe quel appareil fixe ou mobile
Inconvénient	les messages sont conservés sur un seul appareil	Obligation de gérer l'espace disponible (quota fixé par le serveur)

Si vous consultez votre messagerie académique depuis un appareil unique et fixe, ou que vous avez besoin de stocker un volume important de messages utilisez POP. Dans tout autre cas, utilisez IMAP en veillant à surveiller votre quota en archivant ou en supprimant les messages régulièrement

Pour paramétrer votre client, veuillez utiliser les paramètres suivants :

Paramétrage SMTP

Nom du serveur: smtps.ac-besancon.fr

Sécurité: mode sécurisé SSL

Port: 465

Authentification: mot de passe normal

Paramétrage POP

Nom du serveur: pops.ac-besancon.fr

Sécurité: mode sécurisé SSL

Port: 995

Authentification: mot de passe normal

Paramétrage IMAP

Nom du serveur: imaps.ac-besancon.fr

Sécurité: mode sécurisé SSL

Port: 993

Authentification: mot de passe normal

B. Quota

Chaque boîte de courrier électronique, qu'elle soit nominative ou fonctionnelle, dispose d'un espace disque alloué sur les serveurs. La taille de cet espace s'appelle le quota. En POP, la boîte est vidée lorsque vous vous connectez mais, en IMAP ou via le Webmail, vous devez régulièrement supprimer ou archiver vos messages.

Le quota par défaut est de 1Go pour chaque boîte Il peut être augmenté via une demande motivée sur le centre de services ABiTop accessible par Pratic+ (<https://pia.ac-besancon.fr>).

QUE SE PASSE-T-IL LORSQUE VOTRE BOÎTE DE MESSAGERIE EST PLEINE ? Les messages qui sont stockés sur le serveur académique occupent de l'espace disque pris sur ce quota. Lorsque l'espace disque utilisé atteint ce quota, c'est-à-dire lorsque votre boîte aux lettres (dans son ensemble, tous dossiers confondus) est pleine, tout nouveau message qui vous est envoyé ne vous sera plus délivré et un message d'alerte sera envoyé à l'expéditeur. Il sera mis en file d'attente pendant cinq jours. Passé ce délai, si la boîte aux lettres est toujours pleine, le message en attente sera irrémédiablement détruit. Il est donc important de veiller à ce que votre boîte de messagerie académique n'atteigne pas son quota. Pour cela, la première solution, valable dans tous les cas, consiste à supprimer de votre boîte les messages qu'il est inutile de conserver, et à archiver sur un autre support les messages anciens que vous désirez garder malgré leur ancienneté. La deuxième solution, lorsque la première ne suffit plus, est de demander l'augmentation de votre quota.

COMMENT CONNAÎTRE LE QUOTA ET LE TAUX D'UTILISATION DE VOTRE MESSAGERIE ? Le quota disponible pour une boîte de messagerie académique est visible à tout moment dans le webmail convergences.



Il peut être affiché également dans un client local comme Thunderbird si celui-ci est configuré en IMAP. (clic droit sur « courrier entrant, puis propriétés, onglet « quotas ». La plupart des autres clients de messagerie fonctionnent de la même manière. Vous pouvez aussi faire afficher de manière permanente les informations de quota dans la barre de statut du logiciel. Dans Outlook, vous réalisez cela à partir d'un clic droit sur la barre de statut, située en bas de la fenêtre de l'application. Dans les options de personnalisation

de la barre de statut, choisissez d'afficher le quota. Dans Thunderbird, installez le module complémentaire « Display quota » : <https://addons.thunderbird.net/fr/thunderbird/addon/display-quota/>.

COMMENT AUGMENTER LE QUOTA DE VOTRE MESSAGERIE ? Si votre quota actuel se révèle insuffisant et que vous souhaitez le faire augmenter, vous devez en faire la demande auprès de la DSI via le centre de services Abitop. La demande est automatiquement soumise à une approbation hiérarchique.

C. Envoyer des pièces jointes de taille importante

La taille maximum d'un message avec pièce jointe est limitée à 10 Mo. Un message d'erreur apparaît si cette limite est dépassée.

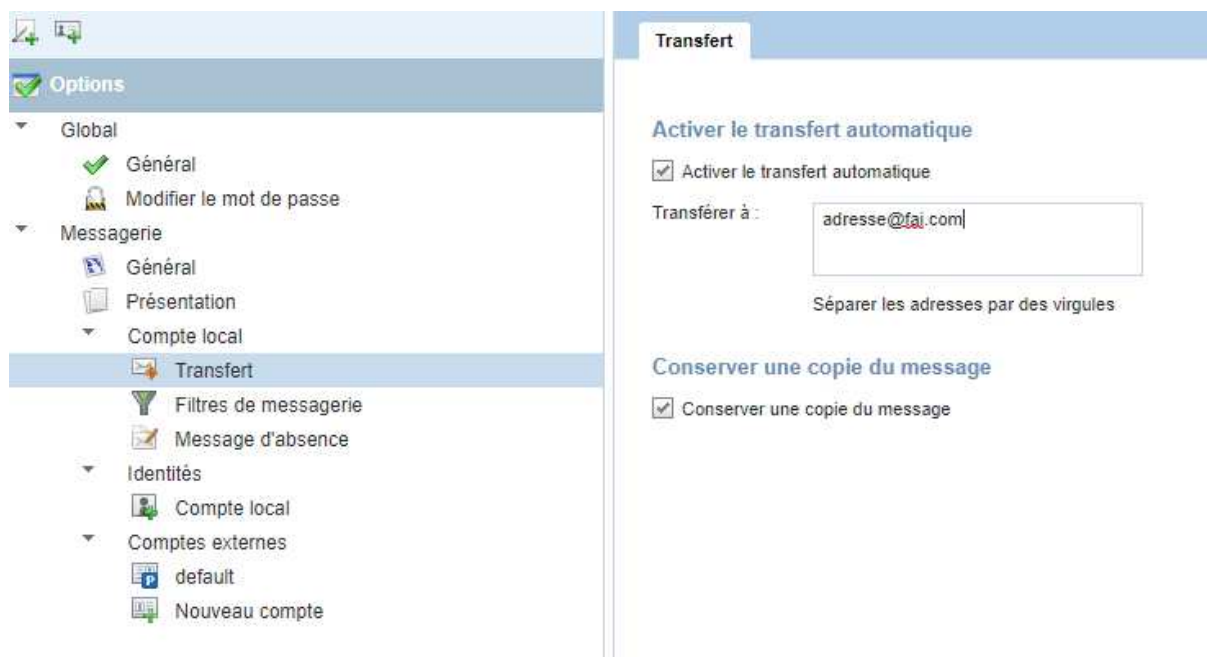
Si vous souhaitez envoyer un fichier de taille importante, utilisez le service Eviol (accessible via Pratic +)

D. Rediriger ma messagerie

Si vous possédez une adresse mail, vous pouvez mettre en place une redirection de messagerie de votre boîte académique personnelle vers votre boîte mail privée. Cette pratique est interdite pour les boîtes fonctionnelles, qu'il s'agisse d'un renvoi direct ou indirect (par l'intermédiaire d'une autre boîte académique).

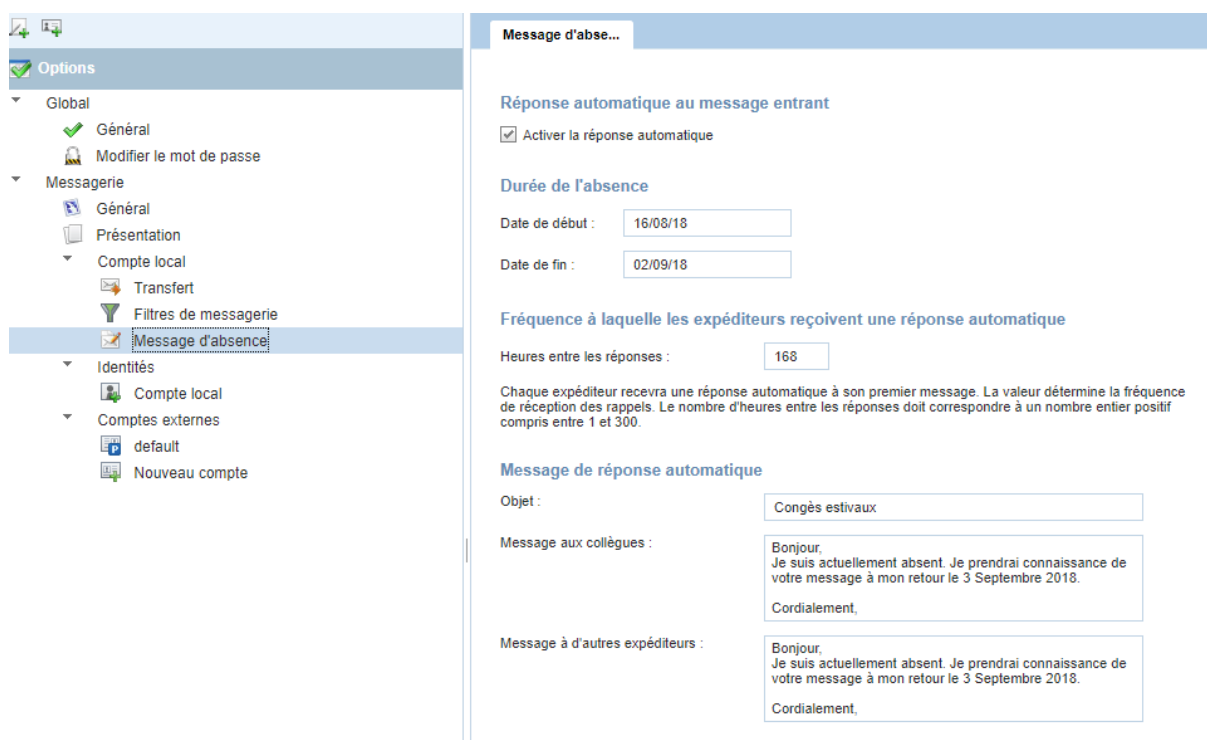
Si cette redirection est uniquement temporaire (congrés, absence ...), laissez cochée la case « Conserver une copie du message ». À noter dans ce cas, que votre boîte académique se remplira et vous devrez régulièrement vous connecter au webmail académique et faire le ménage sous peine de la saturer.

Pour mettre en place un renvoi de messagerie, cliquez sur options dans convergences.



E. Notifier une absence

Lors de vos absences, vous avez la possibilité d'avertir vos correspondants de votre absence de façon automatique. Lorsque nos serveurs recevront un message qui vous est destiné, le serveur renverra automatiquement la notification à l'expéditeur du message. Pour configurer la période et le message d'absence, allez dans les options du webmail Convergence, puis dans messagerie / compte local / Message d'absence. Vous pouvez alors remplir les différents champs en les personnalisant. Un exemple vous est donné ci-dessous :



Pour mettre en place une notification d'absence, n'oubliez pas de cliquer dans la case « activer la réponse automatique » et pour terminer cliquer sur « enregistrer les préférences ».

F. Se protéger des spams

Le spam - en français 'pourriel' - est un courrier non sollicité envoyé à un très grand nombre de personnes sans leur accord préalable. Certains sont des canulars, d'autres plus graves, des tentatives de vous extorquer de l'argent ou vos identifiants (on parle alors de 'phishing' ou hameçonnage en français).

Les règles de base pour éviter le spam :

- Évitez de diffuser votre adresse électronique en clair, sur des sites web, dans des forums ou autres ;
- N'utilisez pas votre adresse académique pour les inscriptions aux services commerciaux du web : créez plutôt un compte 'poubelle', chez un fournisseur gratuit ;
- Avant de répondre à un courriel, vérifiez l'expéditeur.

Vous pouvez signaler un spam en le transférant à l'adresse spam@ac-besancon.fr ou via le centre de services ABiTop.

G. Détecter les messages frauduleux (phishing ou hameçonnage)

Le but de ce type d'attaque, dite de « phishing » ou d'« hameçonnage », est de récupérer les identifiants et mots de passe d'utilisateurs généralement pour envoyer des spams ou pour usurper une identité.

Les domaines de messagerie institutionnels comme le sont les domaines académiques sont une cible privilégiée :

- Les adresses professionnelles des utilisateurs et des établissements sont récupérables : beaucoup sont publiques et/ou publiées sur internet (via des sites web ou annuaires). C'est la différence majeure avec une boîte personnelle qui elle est rarement diffusée ;
- La typologie de l'adresse : prenom.nom@ac-academie.fr permet de deviner l'adresse d'un utilisateur ;

- Ces domaines peuvent être attaqués symboliquement et de manière ciblée dans le cadre d'action contre l'institution ou le pays par des organisations diverses.

C'est pourquoi la gestion et le filtrage de ces messages sont spécifiques et ne peuvent être comparés aux technologies destinées au grand public.

Des mécanismes « anti-spam » sont utilisés dans l'académie. Ils visent à filtrer et détruire ces messages en se basant principalement sur la détection de mots-clés dans les mails avant qu'ils ne soient acheminés dans la boîte de l'utilisateur. La difficulté est de filtrer le maximum de ces messages sans faux positifs. C'est un curseur à placer. Plusieurs dizaines de milliers de messages indésirables sont ainsi rejetés chaque jour pour la seule académie de Besançon.

Les quatre règles de base pour se protéger du phishing :

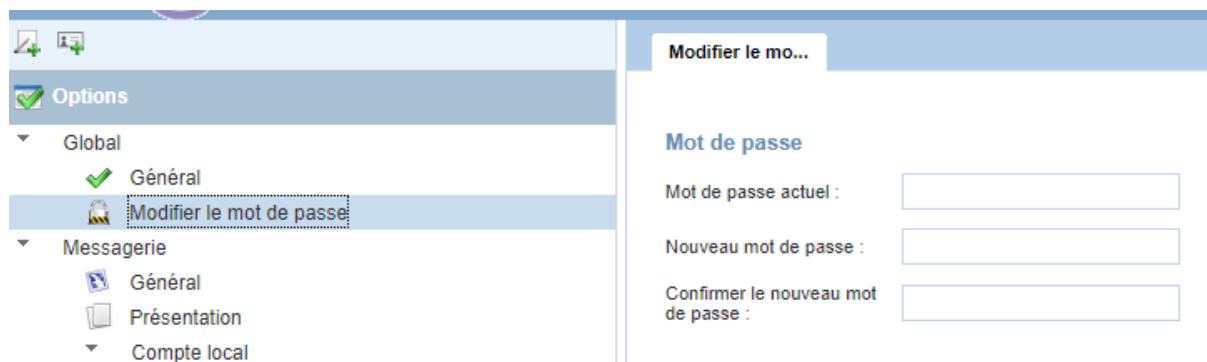
- Vérifiez l'adresse mail de l'expéditeur : il s'agit bien de l'un de vos interlocuteurs ; elle est cohérente avec le contenu du message.
- Vérifiez la pertinence des informations présentes dans le texte. Ils ne doivent pas comporter de trop nombreuses fautes de grammaire, d'orthographe ou de syntaxe.
- Vérifiez la cohérence du vocabulaire utilisé.
- Vérifiez la cohérence des informations demandées avec les us et coutumes de l'organisme (par exemple, la DSI ne demande jamais votre mot de passe)

Si vous pensez avoir été hameçonné, changez immédiatement votre mot de passe.

Plus d'informations sur www.cnil.fr ou sur www.ssi.gouv.fr.

H. Changer de mot de passe

Lors de votre première connexion ou en cas de doute sur la confidentialité de votre mot de passe, vous devez changer celui-ci. Pour cela allez dans les options de convergences :



The image shows a screenshot of a web application interface. On the left, there is a navigation menu under the heading 'Options'. The menu is expanded to show 'Global' options, with 'Général' selected. Under 'Général', the option 'Modifier le mot de passe' is highlighted. Below 'Général', there are 'Messagerie' options: 'Général', 'Présentation', and 'Compte local'. On the right side of the screen, a panel titled 'Modifier le mo...' is visible. It contains a section for 'Mot de passe' with three input fields: 'Mot de passe actuel', 'Nouveau mot de passe', and 'Confirmer le nouveau mot de passe'.

Vous devez saisir votre ancien mot de passe, en choisir un nouveau, le confirmer et valider. Une aide à la génération d'un mot de passe ou des conseils pour en déterminer un de bonne qualité peuvent être trouvés à cette adresse : <https://www.cnil.fr/fr/generer-un-mot-de-passe-solide>.