

Guide des bonnes pratiques de la Messagerie

Guide to good messaging practice

Les principes généraux

Tout utilisateur doit se conformer aux règles définies dans les différentes chartes Informatiques en vigueur. (Ministère, fournisseur d'accès, Etablissement)

La messagerie est un service mis à la disposition des agents et des étudiants de l'établissement pour faciliter la communication et les échanges d'informations professionnelles et institutionnelles.

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, constituer une preuve ou un commencement de preuve.

Chaque utilisateur est responsable des outils Informatiques mis à sa disposition, notamment du contenu de sa boîte aux lettres (BAL), de la manière dont il utilise le courrier électronique et en particulier des messages qu'il envoie. Pour que la messagerie reste sûre et efficace, les utilisateurs doivent appliquer les règles de sécurité, de prudence et de bon usage et respecter l'éthique et la législation.

Chacun doit veiller à garder secret les mots de passe qui donnent accès d'une part à son poste de travail et d'autre part au réseau et à la messagerie.

Pour éviter un travail de lecture inutile aux correspondants, on veillera à ne diffuser chaque message qu'aux interlocuteurs réellement concernés.

On veillera à supprimer sans les ouvrir les messages suspects (émetteur inconnu, objet inexistant ou étrange) provenant de l'extérieur, à ne pas y répondre et à ne pas les transférer à d'autres destinataires.

Aucun message émis ne doit porter atteinte à la personnalité, à la vie privée ou à l'activité professionnelle d'aucune personne.

Le stockage et la diffusion de messages ou de documents de contenu diffamatoire, discriminatoire (raciste, sexiste ...), pornographique ou incitant à la violence ou la haine raciale sont interdits et réprimés par la loi.

La messagerie est un outil de communication professionnelle. L'usage à des fins personnelles n'est admis que s'il est exercé à titre ponctuel et raisonnable et dans le respect des principes notamment déontologiques applicables au service public.

General principles

All users must comply with the rules defined in the various IT charters in force. (Ministry, access provider, School)

Email is a service made available to the school's staff and students to facilitate communication and the exchange of professional and institutional information.

Electronic messages exchanged with third parties may, from a legal point of view, form a contract, constitute evidence or a prima facie case.

Each user is responsible for the IT tools made available to him/her, in particular the content of his/her mailbox (BAL), the way in which he/she uses electronic mail and in particular the messages he/she sends. To ensure that email remains secure and efficient, users must apply the rules of security, prudence and good usage and respect ethics and legislation.

Everyone must take care to keep secret the passwords which give access on the one hand to his workstation and on the other hand to the network and the e-mail.

To avoid unnecessary reading by correspondents, each message should only be sent to the people actually concerned.

Suspicious messages (unknown sender, non-existent or strange subject) from outside the company should be deleted without being opened, not replied to and not forwarded to other recipients.

No message sent must infringe the personality, private life or professional activity of any person.

The storage and distribution of messages or documents containing defamatory, discriminatory (racist, sexist, etc.) or pornographic content or inciting violence or racial hatred are prohibited and punishable by law.

Messaging is a professional communication tool. It may only be used for personal purposes on a one-off and reasonable basis and in compliance with the ethical principles applicable to the public service.

1/Les ressources de la messagerie

1/Messaging resources

1.1 LES BOITES AUX LETTRES NOMINATIVES (INDIVIDUELLES): BAL.

Les BAL nominatives sont individuelles et leur usage est analogue à celui du téléphone, le contenu d'un message engage le signataire ou à défaut l'expéditeur.

Le nom des BAL nominatives est défini par la convention de nommage suivante : prenom.nom@oniris-nantes.fr

En cas d'homonymie, l'autre agent se verra attribuer une BAL nominative de type: prenom.nom2@oniris-nantes.fr

1.1 NOMINATIVE (INDIVIDUAL) MAILBOXES: BAL.

Nominative mailboxes are individual and their use is similar to that of the telephone. The content of a message commits the signatory or, failing that, the sender.

The name of nominative mailboxes is defined by the following naming convention: prenom.nom@oniris-nantes.fr

In the event of a homonym, the other agent will be assigned a nominative mailbox of the following type: prenom.nom2@oniris-nantes.fr

1.2 LES LISTES DE DIFFUSION

Les listes de diffusion Oniris sont exclusivement réservées à l'usage interne des agents et des étudiants d'Oniris et ne doivent être utilisées que pour un motif professionnel. Elles ne doivent en aucun cas être communiquées à l'extérieur de l'établissement.

Un message adressé à des listes de diffusion a un caractère informationnel et n'appelle pas de réponse, sauf si l'émetteur le demande. Dans ce cas particulier, il ne faut répondre qu'à l'émetteur et donc ne pas utiliser la fonctionnalité « répondre à tous »

Le nom des listes de diffusion suit une convention de nommage et débute par liste. Par exemple, la liste du service des Ressources Humaines:

liste.service-rh@oniris-nantes.fr

1.2 MAILING LISTS

Oniris mailing lists are for the exclusive internal use of Oniris staff and students and may only be used for professional purposes. Under no circumstances may they be communicated outside the institution.

Messages sent to mailing lists are for information only and do not require a reply, unless the sender requests one. In this particular case, you should only reply to the sender and not use the "reply to all" function.

The names of mailing lists follow a naming convention and begin with list. For example, the Human Resources department list:

liste.service-rh@oniris-nantes.fr

1.3 LATAILLE DES BOITES AUX LETTRES

L'espace de stockage disponible sur les serveurs est limité à 200 Mo.

1.3 MAILBOX SIZE

The storage space available on the servers is limited to 200 MB.

1.4 LA LIMITATION DE LA TAILLE DES MESSAGES

Dans un message, il est possible d'insérer une ou plusieurs pièces jointes, de préférence en format compressé, en respectant les contraintes détaillées des messages décrites ci-après.

La taille des messages émis dépend du dimensionnement de la boîte destinataire ; à Oniris elle est limitée à 20 Mo. Les limites de taille des BAL et des messages sont susceptibles d'évoluer au cours du temps.

1.4 LIMITING THE SIZE OF MESSAGES

One or more attachments, preferably in compressed format, may be inserted in a message, subject to the message size restrictions described below.

The size of messages sent depends on the size of the recipient mailbox; at Oniris it is limited to 20 MB. Mailbox and message size limits may change over time.

2/Quel émetteur ? Quels destinataires ?

2/Who should be the sender? To whom?

21 UNE SIGNATURE EXPLICITE

L'émetteur d'un message est responsable de son contenu et engage également la responsabilité de son service et de l'établissement. Il doit donc signer le message.

2.1 AN EXPLICIT SIGNATURE

The sender of a message is responsible for its content and is also responsible for his or her department and the institution. They must therefore sign the message.

22 LA DIFFUSION VERS LA HIERARCHIE DE L'EMETTEUR ET DES DESTINATAIRES

L'émetteur doit s'assurer que le contenu de son message est conforme à la politique de son service. Pour les sujets importants, il consultera ses responsables et leur adressera ensuite une copie de son message.

2.2 DISTRIBUTION TO THE SENDER'S HIERARCHY AND RECIPIENTS

The sender must ensure that the content of his message complies with his department's policy. For important subjects, they should consult their managers and then send them a copy of their message.

23 UNE DIFFUSION MESUREE DES MESSAGES ET DES REPONSES

La principale difficulté liée à l'usage de la messagerie réside maintenant dans le grand nombre de messages reçus quotidiennement par chaque utilisateur et donc dans le temps nécessaire pour lire ces messages. Il faut donc :

• Limiter le nombre de destinataires Répondre
seulement en cas de nécessité

• N'utiliser qu'exceptionnellement la fonctionnalité **Répondre à tous**

• Ne transférer de message qu'aux personnes réellement susceptibles d'être intéressées

• Ne demander d'accusés de réception ou de confirmations de lecture qu'en cas de nécessité.

2.3 MEASURED DISTRIBUTION OF MESSAGES AND REPLIES

The main difficulty in using email now lies in the large number of messages received daily by each user, and therefore in the time needed to read these messages. You therefore need to :

Limit the number of recipients Reply only when necessary

Only ever use the Reply to All function

Only forward messages to people who are genuinely likely to be interested

Only request acknowledgement of receipt or read confirmation when necessary.

2.4 UNE PRUDENCE PARTICULIERE POUR LES MESSAGES ADRESSES A L'EXTERIEUR

Tout courrier électronique adressé à des destinataires extérieurs doit, plus que tout autre, respecter les principes déontologiques du secret et de la discrétion professionnelle, les règles de validation hiérarchique en vigueur et le devoir de réserve.

L'envoi d'informations confidentielles à l'extérieur transite sur Internet où le niveau de sécurité est particulièrement faible.

Tout renvoi automatique (ex absence prolongée) du courrier arrivant dans une BAL d'Oniris vers une BAL extérieure est fortement déconseillé pour des raisons de

sécurité.

Pour les mêmes raisons, aucun message ne doit être adressé simultanément à une liste interne de diffusion et un destinataire extérieur et aucun message contenant une adresse de liste interne de diffusion ne doit être posté à l'extérieur.

2.4 PARTICULAR CAUTION FOR MESSAGES SENT TO EXTERNAL RECIPIENTS

Any electronic mail sent to external recipients must, more than any other, comply with the ethical principles of professional secrecy and discretion, the rules of hierarchical validation in force and the duty to act in a reserved manner.

Confidential information sent externally is sent over the Internet, where the level of security is particularly low.

Any automatic forwarding (e.g. prolonged absence) of mail arriving in an Oniris mailbox to an external mailbox is strongly discouraged for security reasons.

For the same reasons, no message should be sent simultaneously to an internal mailing list and an external recipient, and no message containing an internal mailing list address should be posted externally.

3/La sécurité et les règles de prudence

3/Safety and safety rules

31 L'AUTHENTIFICATION

Le système d'authentification (identifiant et mot de passe) permet de s'assurer que la personne qui utilise une boîte aux lettres de la messagerie est bien autorisée à le faire. Chaque utilisateur doit donc respecter le caractère confidentiel de son mot de passe.

3.1 AUTHENTICATION

The authentication system (identifier and password) ensures that the person using a mailbox is authorised to do so. Each user must therefore respect the confidential nature of their password.

32 LA PROTECTION EVENTUELLE DES PIÈCES JOINTES ENVOYÉES

Un utilisateur transmettant des documents en pièces jointes d'un message peut souhaiter qu'ils ne soient pas modifiés. Pour les protéger au mieux des modifications, il peut les transmettre sous forme de fichier en lecture seule (PDF, Word, Excel...)

3.2 POSSIBLE PROTECTION OF SENT ATTACHMENTS

A user who sends documents as attachments in a message may not want them to be modified. To protect them as much as possible from modification, they can send them as read-only files (PDF, Word, Excel, etc.).

33 LA SÉCURITÉ DES FICHIERS SENSIBLES

Il appartient à l'utilisateur d'assurer la protection des informations jugées sensibles qu'il reçoit ou émet. Si l'utilisateur copie un fichier sensible sur son poste de travail ou sur un espace réseau partagé, il doit en assurer la sécurité en l'enregistrant en lecture seule et en prévoyant un mot de passe pour la lecture et la modification.

3.3 SECURITY OF SENSITIVE FILES

It is the user's responsibility to ensure the protection of information deemed sensitive that he receives or sends. If the user copies a sensitive file onto his workstation or onto a shared network space, he must ensure its security by saving it as read-only and by providing a password for reading and modification.

34 LA PRÉVENTION DES VIRUS

Pour se protéger, l'établissement a mis en place des boucliers successifs (logiciels anti-virus). Si un message comporte un virus, il est supprimé; l'expéditeur et le destinataire sont avertis par courriel, par le logiciel anti-virus, de l'action qui a été menée.

3.4 VIRUS PREVENTION

To protect itself, the school has put in place successive shields (anti-virus software). If a message contains a virus, it is deleted; the sender and recipient are notified by e-mail, by the anti-virus software, of the action taken.

35 SUPPRIMER SANS LES OUVRIR LES MESSAGES SUSPECTS PROVENANT DE L'EXTÉRIEUR, NE PAS LES TRANSFÉRER ET NE PAS Y RÉPONDRE

Il faut supprimer sans les ouvrir les messages et leurs éventuelles pièces jointes provenant d'émetteurs extérieurs Inconnus dont le libellé d'objet est vide, non pertinent ou incompréhensible.

D'une façon générale, il ne faut fournir aucune information confidentielle (par exemple son adresse mail, son numéro de carte bancaire...) sur un site web auquel on aurait eu accès par un lien dans un message non sollicité.

3.5 DELETE SUSPICIOUS MESSAGES FROM OUTSIDE WITHOUT OPENING THEM, DO NOT FORWARD THEM AND DO NOT REPLY TO THEM

Messages and any attachments from unknown external senders with empty, irrelevant or incomprehensible subject lines should be deleted without opening them.

In general, you should not provide any confidential information (e.g. your e-mail address, bank card number, etc.) on a website accessed via a link in an unsolicited message.

36 LE RESPECT DE LA CONFIDENTIALITÉ

Les personnes qui assurent l'administration technique de la messagerie sont des agents du service informatique. Tous sont soumis au secret professionnel.

L'accès au contenu d'une BAL nominative, par un administrateur de la messagerie, n'est possible que si l'utilisateur donne son accord écrit préalable. Cette autorisation d'accès a un caractère provisoire afin de permettre la résolution d'un problème technique.

En cas de problème de réception, à la demande d'un utilisateur, les administrateurs de la messagerie peuvent utiliser des outils permettant d'assurer la traçabilité des messages reçus dans une BAL.

3.6 RESPECT FOR CONFIDENTIALITY

The persons responsible for the technical administration of the messaging system are members of the IT department. All are bound by professional

secrecy.

Access to the contents of a named mailbox by a mailbox administrator is only possible if the user gives prior written consent. This access authorisation is temporary to allow a technical problem to be resolved.

In the event of a reception problem, at the request of a user, email administrators may use tools to ensure the traceability of messages received in a mailbox.

4/ Les bons usages

4/ Good practice

41 GESTION REGULIERE DU CONTENU DE LA BAL

Il est conseillé de ne garder que les informations utiles à un usage ultérieur et de les classer dans des sous dossiers.

4.1 REGULAR MANAGEMENT OF THE BALL'S CONTENTS

It is advisable to keep only information that is useful for future use and to file it in sub-folders.

42 STOCKAGE ET ARCHIVAGE DES MESSAGES ELECTRONIQUES

Chaque utilisateur est responsable de la sauvegarde des messages sur son poste de travail.

4.2 STORING AND ARCHIVING ELECTRONIC MESSAGES

Each user is responsible for saving messages on their workstation.

43 UTILISATION OU GESTIONNAIRE D'ABSENCE

En cas d'absence, le webmail permet de paramétrer un « Gestionnaire d'absence », pour informer automatiquement vos interlocuteurs. Un transfert interne des messages est possible.

4.3 USE OR ABSENCE MANAGER

In the event of absence, webmail allows you to set up an "Absence Manager" to automatically inform your contacts. Messages can be forwarded internally.

44 ACCESSIBILITE AUX INFORMATIONS

L'accessibilité concerne plus particulièrement les personnes ayant un handicap qui utilisent des outils informatiques spécifiques pour consulter les messages et documents transmis.

Dans ce cas particulier, il faut veiller à joindre des documents aux formats compatibles (traitement de texte, tableur ...).

4.4 INFORMATION ACCESSIBILITY

Accessibility is particularly important for people with disabilities who use special IT tools to consult messages and documents.

In this particular case, you should attach documents in compatible formats (word processing, spreadsheets, etc.).

Les textes de référence (liste indicative et non exhaustive)

Reference texts (indicative and non-exhaustive list)

Lol n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004, décret d'application n°2005-1309 du 20 octobre 2005.

Conformément à la loi du 6 janvier 1978, les informations nominatives relatives aux utilisateurs de l'établissement, disponibles dans la messagerie, ont reçu l'agrément de la CNIL.

Code de la propriété intellectuelle (loi 94-361 du 10 mai 1994 concernant la protection juridique des programmes d'ordinateur).

Code pénal - articles 323-1, 323-2, 323-3, 323-7 relatifs à l'accès frauduleux ou à l'entrave ou au faussement du fonctionnement d'un système de traitement automatisé de données.

Loi 83-634 du 13 juillet 1983 portant statut des fonctionnaires (art.26) et art 226-13 du code pénal.

Law no. 78-17 of 6 January 1978 on data processing, data files and individual liberties, amended by Law no. 2004-801 of 6 August 2004, implementing decree no. 2005-1309 of 20 October 2005.

In accordance with the law of 6 January 1978, the nominative information relating to users of the establishment, available in the messaging system, has been approved by the CNIL.

Intellectual Property Code (law 94-361 of 10 May 1994 on the legal protection of computer programmes).

Penal Code - articles 323-1, 323-2, 323-3, 323-7 relating to fraudulent access to or interference with or distortion of the operation of an automated data processing system.

Law 83-634 of 13 July 1983 on the status of civil servants (art.26) and art 226-13 of the Criminal Code.

Date et signature :