



27 JAN. 2006

Note à l'attention de

Mesdames et Messieurs les directeurs et délégués d'administration centrale

**Direction de
l'administration
générale**

**Service du
personnel et des
affaires sociales**

Affaire suivie par
Céline Bredèche

poste

01 40 15 86 41
Références

SPAS/MPP/CBr-05.259

182, rue Saint-Honoré
75033 Paris Cedex 01
France

Téléphone 01 40 15 80 00
Télécopie 01 40 15 80 02

**Madame et Messieurs les préfets de région
-directions régionales des affaires culturelles-**

**Mesdames et Messieurs les préfets de départements
-services départementaux de l'architecture et du patrimoine-**

**Mesdames et Messieurs les présidents et directeurs
du Centre national des Arts plastiques et du Fond national d'art
contemporain, du Centre national du livre, du musée Guimet**

Objet : Charte d'utilisation des moyens informatiques.

La présente note a pour objet de préciser les modalités d'application de la Charte d'utilisation des moyens informatiques qui a été soumise pour avis et adoptée lors du comité technique paritaire ministériel du 2 décembre 2005.

I. Objet de la charte d'utilisation des moyens informatiques

L'article 1 de la charte rappelle que « les équipements informatiques et les moyens de communication électronique du ministère de la culture et de la communication sont une ressource commune dont la sécurité et la disponibilité dépendent de leur bon usage par chaque utilisateur.

L'objet de la présente charte est de fixer des règles d'utilisation afin d'assurer la sécurité et la performance du système d'information et de préserver la confidentialité des données. Elle est conçue dans le respect des principes généraux définis par la Commission nationale informatique et libertés.

Au-delà du respect de la loi stricto sensu, notamment sur la confidentialité des données et sur la propriété intellectuelle, l'objectif visé est, en effet, de **préserver l'outil de travail** et de **garantir l'efficacité du système d'information en définissant des bons usages d'utilisation**. C'est en particulier le cas de la messagerie, dont l'efficacité suppose qu'elle ne véhicule pas, sauf urgence, des informations professionnelles à caractère général ; a fortiori, lorsqu'il s'agit de messages à caractère personnel.

En se dotant de ce texte, le ministère entend informer les agents sur leurs droits et leurs devoirs, afin qu'ils utilisent le système d'information en se conformant à la loi et, de façon plus large, en adoptant une attitude responsable et de bon sens.

A cet égard, il convient de souligner la responsabilité des agents lorsqu'ils émettent des opinions personnelles en utilisant leur adresse électronique professionnelle. Pour éviter la confusion entre une opinion officielle et une opinion personnelle, il est prudent de faire apparaître clairement la portée de son opinion.

Par exemple, pour émettre des opinions personnelles, un agent peut :

- créer un compte sur un forum dont le nom ne mentionne pas le ministère ;
- mettre un avertissement en pied de message tel que « le contenu de ce message ne reflète que l'opinion personnelle de son émetteur. Il n'engage en rien le Ministère de la culture et la communication ».

II. Aspects spécifiques liés à la sécurité

Sur les aspects plus spécifiquement liés à la sécurité, les prescriptions de la charte ne doivent pas être comprises comme répondant à une volonté répressive de l'administration mais à un souci de protection du système d'information, du bon fonctionnement du service et de l'utilisateur lui-même.

Il en est ainsi des prescriptions relatives aux sites interdits et de celles relatives à l'ajout de programme par l'utilisateur.

1. Sites interdits

Les sites interdits peuvent être divisés en deux grandes catégories :

- les sites dont le contenu ne respecte pas la législation en vigueur (apologie des crimes contre l'humanité, pornographie enfantine, incitation à la haine raciale, à la violence et à toute forme de discrimination, stupéfiants, copies illégales de biens numériques...) et les sites contraires aux bonnes mœurs (pornographie notamment) ;
- les sites dangereux pour le système d'information (sites contrôlés par des pirates, webmail, collectes d'informations sur les habitudes ou sur les données privées des internautes...).

Concernant les tentatives de connexion à ces sites interdits, il faut opérer une distinction entre :

- les accès involontaires (virus et logiciels espions qui tentent de remonter des informations sur des sites peu recommandables, fenêtres « pop-up » de publicités, logiciels mal configurés) ;
- les accès volontaires (recherche sur un moteur de recherche comme Google : « fabrication cannabis » puis tentatives de connexion à tous les sites indiqués par le moteur de recherche).

L'utilisateur a la faculté de faire reconnaître sa bonne foi :

- en demandant la vérification et la prise de mesure de protection de son poste lorsqu'un autre utilisateur s'est connecté sur des sites interdits à partir de son poste ;
- en cas d'erreur, en avertissant le Département des systèmes d'information que le site sur lequel il souhaitait se connecter et dont l'accès lui a été interdit n'entre pas dans cette catégorie.

2. Ajout de programme par l'utilisateur

La possibilité d'installer des programmes est réduite pour l'utilisateur. Un programme gratuit ou libre ne signifie en effet pas qu'il soit « inoffensif » :

- certains logiciels gratuits comportent des « chevaux de Troie », qui espionnent ensuite le comportement de l'utilisateur ; même si les remontées d'information de ces « chevaux de Troie » vers des sites peu recommandables sont, pour beaucoup, arrêtées, le simple fonctionnement du « cheval de Troie » consomme des ressources sur le poste utilisateur et sur le réseau (jusqu'au filtre qui les arrête) ;
- des logiciels plus respectueux peuvent se révéler incompatibles avec le fonctionnement de logiciels utilisés par le ministère, conduisant à des pannes inexplicables ou à des blocages.

Le responsable informatique peut, après vérification de compatibilité, installer des logiciels que l'activité professionnelle requiert.

III. Présentation des points clés de la Charte

Après une présentation de son objet et de son champ d'application, la Charte se compose de deux grandes parties.

La première concerne les règles générales d'utilisation à savoir :

- les conditions d'accès et d'utilisation de comptes ;
- les conditions de confidentialité ;
- l'autorisation préalable à l'utilisation de données individuelles ;
- la préservation de l'intégrité des informations et des systèmes ;
- le respect du droit de la propriété intellectuelle ;
- la responsabilité de l'utilisateur.

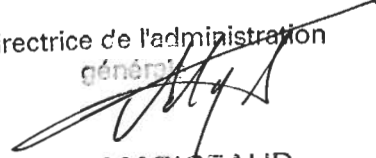
La seconde traite des règles d'utilisation plus spécifiques concernant notamment la messagerie et :

- l'obligation d'informer sa hiérarchie sur les informations échangées ;
- la responsabilité de l'agent liée aux messages électroniques ;
- le traitement des messages des citoyens.

Enfin, une annexe présente quelques mesures techniques qu'il est utile de connaître et des recommandations concrètes d'utilisation.

Je vous remercie de diffuser auprès de l'ensemble des agents affectés dans vos services la présente note et la charte d'utilisation des moyens informatiques.

La Directrice de l'administration
généraliste


Martine MARIGEAUD

Charte d'utilisation des moyens informatiques

1. OBJET DE LA CHARTE	2
2. DOMAINES D'APPLICATION.....	2
3. RÈGLES GÉNÉRALES D'UTILISATION.....	2
3.1. Condition d'accès et utilisation de comptes	2
3.2. Conditions de confidentialité	2
3.3. Autorisation préalable à l'utilisation des données individuelles	3
3.4. Préservation de l'intégrité des informations.....	3
3.5. Préservation de l'intégrité des systèmes.....	3
3.6. Respect du droit de la propriété intellectuelle.....	3
3.6.1. Protection des logiciels	3
3.6.2. Protection des données.....	3
3.7. Responsabilité de l'utilisateur.....	4
4. RÈGLES SPÉCIFIQUES D'UTILISATION (BONS USAGES)	4
4.1. Messagerie	4
4.1.1. Usage	4
4.1.2. Absence.....	4
4.1.3. Diffusion des messages.....	5
4.1.4. Lisibilité des messages.....	5
4.1.5. Corps des messages.....	5
4.1.6. Format des pièces jointes	5
4.1.7. Taille des messages.....	5
4.1.8. Signature électronique des messages	6
4.1.9. Intégrité des messages.....	6
4.2. Information de la hiérarchie	6
4.3. Responsabilité.....	6
4.4. Recommandations pour le traitement des messages des citoyens.....	6
5. MISE EN ŒUVRE ET SUIVI DE LA CHARTE	6
ANNEXE.....	7
1. Mesures techniques.....	7
2. Quelques recommandations.....	7

1. Objet de la charte

Les équipements informatiques et les moyens de communication électronique du ministère de la Culture et de la Communication sont une ressource commune dont la sécurité et la disponibilité dépendent de leur bon usage par chaque utilisateur.

L'objet de la présente charte est de fixer des règles d'utilisation afin d'assurer la sécurité et la performance du système d'information et de préserver la confidentialité des données. Elle est conçue dans le respect des principes généraux définis par la Commission nationale informatique et libertés (CNIL).

2. Domaines d'application

Ces règles de bon usage s'appliquent à toute personne, quel que soit son statut, qui utilise les moyens informatiques mis à disposition par le Ministère (administration centrale, services déconcentrés, services à compétence nationale et certains établissements publics).

Dans ce qui suit, on désignera collectivement ces moyens sous le terme de système d'information.

3. Règles générales d'utilisation

3.1. Condition d'accès et utilisation de comptes

L'autorisation d'accès est accordée par l'autorité hiérarchique compétente puis mise en place par le département des systèmes d'information (DSI) ou l'entité informatique compétente.

L'autorisation d'accès se traduit notamment par :

- une dotation en équipements informatiques quand l'agent dispose d'une station de travail personnelle,
- l'attribution à l'utilisateur de moyens d'identification et d'authentification (ex : identifiant, mot de passe) et de droits d'accès.

Le droit d'accès au système d'information est personnel et incessible.

Cet accès est limité aux activités autorisées par le Ministère. Une utilisation à titre personnel est tolérée dans les limites raisonnables et dans la mesure où elle est compatible avec l'activité du service.

L'utilisateur ne doit pas se servir des ressources du ministère pour des activités contraires à la loi.

Dans ce cadre, et en accord avec la CNIL, le ministère enregistre et peut analyser les connexions Web.

L'abus de tentatives volontaires de connexions à des sites interdits entraînera la suppression de l'accès Internet depuis le poste de l'utilisateur.

3.2. Conditions de confidentialité

Il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, sans leur accord, quand bien même ceux-ci ne les auraient pas explicitement protégées par une mention " personnel " ou " privé ".

Les fichiers conservés sur le poste de travail peuvent être accessibles, par des agents ayant les droits suffisants. Cet accès est organisé au sein de chaque service. Par ailleurs, il faut rappeler que l'utilisation de ressources partagées permet d'assurer la continuité du service en l'absence de l'agent.

3.3. Autorisation préalable à l'utilisation des données individuelles

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers nominatifs entrant dans le champ d'application de la loi n°78-17 du 6 janvier 1978 Informatique et Libertés, il devra auparavant avoir transmis une demande d'avis à la CNIL par l'intermédiaire de la direction de l'administration générale/sous-direction des affaires juridiques et en avoir reçu l'autorisation.

Cette autorisation n'est valable que pour les traitements définis précisément dans la demande.

3.4. Préservation de l'intégrité des informations

L'utilisateur s'engage à ne pas modifier ou détruire d'autres informations que celles dont il est gestionnaire, et dans le cadre des règles de la gestion de ces informations.

En particulier, il lui est interdit de modifier le ou les fichiers contenant des informations comptables ou d'identification sans respecter les procédures prévues..

L'utilisateur est invité à sauvegarder régulièrement les informations dont il est gestionnaire.

L'utilisateur ne doit pas faire disparaître ni altérer quelque information dont il est gestionnaire et dont la suppression ou la modification pourrait avoir des conséquences dommageables pour le service.

3.5. Préservation de l'intégrité des systèmes

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au système d'information par des manipulations anormales du matériel, la suppression de logiciels, ou l'introduction de logiciels non autorisés.

Le ministère filtre les messages transitant par son système de messagerie et peut arrêter ou rejeter un message sur différents critères comme l'émetteur, la machine émettrice, la non-conformité du message aux normes de messagerie, l'impossibilité de vérifier l'inocuité du message, la présence de virus.

Il est impossible pour les utilisateurs de relever des boîtes aux lettres (BAL) externes depuis le réseau ministère.

Les services en charge de la fourniture et de la maintenance installent un antivirus sur chaque poste de travail.

Le système de mise à jour automatique de l'antivirus doit être activé. Sa désactivation par l'utilisateur est interdite.

Lorsqu'un système de mise à jour de logiciel ou du système d'exploitation est mis en place par l'administration, la désactivation de celui-ci est interdite.

3.6. Respect du droit de la propriété intellectuelle

3.6.1. Protection des logiciels

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle.

3.6.2. Protection des données

Les données telles que les textes, les images, les sons, sont également protégées par la législation sur le droit d'auteur.

Que la mention d'un copyright soit explicite (« Copyright » ou « © ») ou non, leur utilisation, leur reproduction et leur exploitation sont soumises à autorisation du détenteur du droit, sauf mention explicite contraire.

Par ailleurs, les bases de données bénéficient d'un régime juridique qui leur est propre, en vertu de la loi n°98-536 du 1^{er} juillet 1998. Cette dernière sanctionne notamment l'extraction

de la totalité ou d'une partie substantielle du contenu d'une base de données, et sa réutilisation par mise à disposition du public sans autorisation de son producteur.

3.7. Responsabilité de l'utilisateur

L'utilisateur enfreignant la présente charte pourra se voir supprimer tout droit d'accès au système d'information, sans préjudice de poursuites disciplinaires, administratives, civiles ou pénales.

4. Règles spécifiques d'utilisation (bons usages)

Les règles générales d'utilisation des outils informatiques s'inscrivent dans l'application du statut de la Fonction publique qui définit les droits et obligations des fonctionnaires. Ainsi tout agent du ministère est tenu au secret professionnel et doit faire preuve de discrétion professionnelle dans le cadre de l'exercice de son activité.

L'utilisateur doit éviter toute utilisation intensive de nature à perturber l'activité normale des services.

4.1. Messagerie

4.1.1. Usage

La messagerie est destinée principalement à un usage professionnel. Toutefois, la confidentialité des messages personnels est respectée sous réserve du droit de l'administrateur de réseau de filtrer les messages et les fichiers, de les contrôler, et de prendre les mesures nécessaires si cela est justifié par des besoins de sécurité. En aucun cas, l'administrateur n'est autorisé à divulguer le contenu des messages et des fichiers.

Afin d'alléger la messagerie, toute information destinée à une large diffusion relève d'une publication sur un serveur web sauf urgence et nécessité du service. A fortiori, la diffusion large de messages non professionnels n'est pas autorisée (par exemple : petites annonces, vœux, etc.).

La sollicitation de l'envoi de messages à une même boîte aux lettres est interdite (pétition, ...).

4.1.2. Absence

Pour faire face aux périodes d'absences, le gestionnaire en charge d'une boîte aux lettres de service ou d'unité recevant ou émettant des courriers officiels devra donner des droits d'accès sur la boîte fonctionnelle à un autre agent du service.

L'annonce d'absences prévues (congrés, formations) à ses contacts privilégiés ou aux contacts sur un sujet précis, avec indication d'un intérim, est efficace. En revanche, les filtres avec renvoi et les réponses automatiques sont déconseillés : ils peuvent en effet engendrer des boucles qui saturent la messagerie, phénomène constaté à chaque période de vacances.

L'utilisation partagée d'une boîte fonctionnelle par plusieurs agents est la meilleure option pour assurer la continuité de service. La méthode de travail doit dans ce cas être adaptée pour savoir qui consulte en priorité, comment tous les utilisateurs sont au courant qu'une réponse a été envoyée, etc.

4.1.3. Diffusion des messages

L'envoi des messages est limité aux destinataires réellement intéressés ou concernés. Un nombre maximal d'adresses de destination est fixé. Au-delà de ce nombre, des listes de diffusion thématiques peuvent être constituées pour un groupe d'agents partageant un même centre d'intérêt professionnel. L'attribution de ces listes est accordée par le DSI. Chaque liste est gérée par une ou plusieurs personnes appelées gestionnaires. Elle peut être modérée : un responsable est alors chargé de valider le message. L'usage de ces listes est, selon les cas, libre ou réservé aux membres de la liste.

Ces listes offrent aux utilisateurs de la messagerie la possibilité d'abonnement et de désabonnement à l'exception de la liste générale « culture » et des listes générales à caractère structurel ou géographique ; les agents y sont abonnés d'office et ne peuvent se désabonner.

L'usage des listes générales de diffusion est réservé à l'administration. Seuls les agents habilités par leur hiérarchie peuvent utiliser ces listes en raison de l'urgence ou d'absence de publication adapté sur le portail intranet ou plus généralement sur un site Web.

4.1.4. Lisibilité des messages

- a) Le **style** utilisé doit être simple et direct et cependant courtois
- b) L'**objet** du message constitue une indication essentielle du contenu du message pour le destinataire. Il doit être systématiquement renseigné de manière parlante.

4.1.5. Corps des messages

Il est recommandé que le corps du message ne dépasse pas une page.

Si des pièces sont jointes au message, leur contenu doit être sommairement décrit dans le corps de message.

Il est souvent utile d'utiliser une « signature » en fin de message indiquant au moins l'identité, la fonction et le service de l'expéditeur. Cette signature est indicative et n'est pas la preuve de l'authenticité du message.

4.1.6. Format des pièces jointes

Il faut toujours se demander quel format (type et version) le ou les destinataires sont capables de lire.

L'utilisation d'un format pouvant contenir du code exécutable ou des macros doit être évité. Il est recommandé d'utiliser le format RTF plutôt que le format DOC pour les documents issus d'un traitement de texte et destinés à être modifiés. Pour les autres documents le format PDF est également utilisable.

Il est déconseillé d'ouvrir les pièces jointes dans des formats inconnus, dont l'extension est multiple (truc.jpg.vbs) ou qui peuvent être exécutables (.com, .bat, .lnk, .dll, .exe, .vbs, .js).

4.1.7. Taille des messages

Lorsque la taille d'un message (en-tête, corps et pièces jointes) est supérieure à la limite autorisée, l'expéditeur est avisé du rejet du message. Lorsqu'un message autorisé dépasse une taille fixée, le message n'est diffusé qu'en soirée ou la nuit, et l'expéditeur en est avisé.

Lorsque la taille du message ne permet pas le transfert par messagerie, l'utilisateur est invité à se rapprocher de son correspondant informatique, ou pour les service n'en disposant pas, du service de support aux utilisateurs, pour utiliser un moyen adapté (exemple : protocole de transfert de fichiers).

4.1.8. Signature électronique des messages

La mise en place d'outils de signature électronique permet de garantir l'identité de l'expéditeur, l'intégrité du contenu et la non répudiation. Cette garantie ne peut être obtenue qu'avec une utilisation correcte des procédures de vérification de signature.

4.1.9. Intégrité des messages

Il est interdit de retransmettre un message après l'avoir modifié, lui ou une de ses pièces jointes, sans mentionner explicitement qu'il y a eu des modifications.

4.2. Information de la hiérarchie

Informar sa hiérarchie fait partie des obligations de service.

En fonction de la nature et de l'importance des informations échangées, il convient de l'informer du contenu ou de lui transmettre une sélection judicieuse de messages aussi bien reçus qu'émis.

4.3. Responsabilité

Un message électronique peut être une preuve. En matière commerciale comme en matière administrative, le principe est celui de la liberté de la preuve qui peut être apportée par tous moyens. Un message électronique peut donc constituer une preuve susceptible d'engager la responsabilité de l'administration.

Aussi, la messagerie doit être utilisée comme outil de communication et d'information, et on veillera à ce que les messages envoyés ne puissent être considérés comme des contrats ou des actes juridiques.

De plus, un message identifié par une adresse @culture.gouv.fr peut engager la responsabilité du ministère et celle de son auteur. L'utilisateur veillera donc à éviter tout message qui pourrait nuire à l'image de l'administration en participant par exemple à des forums non professionnels.

4.4. Recommandations pour le traitement des messages des citoyens

Sur le plan des principes, rien ne s'oppose à ce que l'administration soit régulièrement saisie au moyen de demandes transmises par internet.

La circulaire du Premier ministre du 7/10/1999 fixe le délai maximal de réponse à une semaine. Il pourra s'agir d'une réponse d'attente si la question posée appelle un examen approfondi.

Par application des dispositions du décret du 28/11/1983 relatif à l'amélioration des relations avec les usagers, les messages mal adressés devront être ré-acheminés vers le service compétent.

Dans l'attente de l'adaptation du droit de la preuve aux nouvelles technologies et de la mise en œuvre des dispositifs techniques adaptés, les règles suivantes seront appliquées :

- répondre par messagerie aux demandes d'information générale,
- doubler la réponse par courrier papier pour les messages qui engagent l'administration,
- respecter les règles de délégation de signature définies dans le service.

5. Mise en œuvre et suivi de la charte

La présente charte a fait l'objet d'une concertation avec les organisations syndicales représentatives. Elle a été soumise pour avis au CTPM du 2 décembre 2005. En fonction des évolutions techniques, législatives ou réglementaires le texte de la charte pourra être révisée.

Annexe

La présente charte s'inscrit dans le système d'information du Ministère qui fait l'objet d'un schéma directeur de sécurité élaboré en liaison et en collaboration avec la direction centrale de sécurité des systèmes d'information, organisme placé sous l'autorité du secrétaire général de la défense nationale. Dès à présent, suite à des audits de sécurité et d'intrusion, un certain nombre de mesures ont été recommandées par la direction centrale de la sécurité des systèmes d'information (DCSSI).

1. Mesures techniques.

- nombre maximal d'adresses de destination d'un message : 30
- taille limite des messages 4 Mo,
- taille à partir de laquelle la transmission est retardée : 2 Mo
- interdiction de certains services Internet (IRC, ...)
- interdiction formelle de connecter une machine reliée au réseau du ministère à un autre réseau (SIT, Internet, Préfecture) via l'établissement d'une connexion physique (ligne spécialisée, ADSL, câble, boucle locale radio, WiFi ou tout autre moyen),
- le réseau du ministère étant connecté au réseau interministériel AdER, toute compromission du réseau du ministère, peut aider à l'attaque de réseaux très sensibles. Seul le haut fonctionnaire de défense peut, s'il le juge utile, prendre l'attache du secrétaire général de la défense nationale pour demander des dérogations éventuelles aux règles liées à la connexion de réseau ADER.

2. Quelques recommandations

- choisir un mot de passe non évident ; au minimum, mélanger chiffres et lettres,
- ne jamais donner son identifiant/mot de passe,
- ne pas répondre aux messages en masse ou en chaîne des messageries,
- éteindre son poste par arrêt logiciel et non pas l'interrupteur pour terminer proprement ses sessions (hors cas de blocage technique),
- ne jamais quitter son poste de travail en laissant accessible une session en cours, se déconnecter ou utiliser un écran de veille protégé par mot de passe,
- ne pas laisser à disposition des supports informatiques (disquette, cassette, CD-Rom,...) contenant des données confidentielles, dans un bureau ouvert,
- veiller à protéger contre le vol l'ordinateur portable dont on dispose,
- en cas d'incident,
- informer sans délai le correspondant informatique ou le service de support afin que celui-ci mette tout en œuvre pour traiter l'incident ; une saisine tardive rend difficile l'obtention des informations techniques susceptibles d'aider à la résolution ;.
- noter les éventuels messages d'erreur, les manipulations effectuées et les symptômes constatés,
- utiliser la fonctionnalité de filtrage des messages.

Un espace de publication sur l'intranet liste les recommandations en matière de sécurité du système d'information.