



Guide des bonnes pratiques pour l'usage des outils numériques par les personnels de l'académie de Toulouse

Rectorat de l'académie de Toulouse
CS 87703
31 077 Toulouse cedex 4

Table des matières

1. Préambule	3
2. Poste de travail	3
2.1 La sécurisation du poste de travail	3
2.2 Le compte de l'utilisateur	3
2.3 La protection logicielle : anti-virus et pare-feu (« firewall »).....	4
2.4 La sauvegarde des données	4
2.5 L'utilisation du poste en mode « administrateur ».....	4
2.6 L'utilisation du matériel nomade	4
2.7 L'utilisation d'outils personnels	5
2.8 Le téléchargement	5
2.9 L'utilisation des services en ligne	5
3. Messagerie électronique	5
3.1 Caractéristiques et limitations de la messagerie électronique.....	5
3.2 La gestion de la messagerie en cas d'absence	6
3.3 Stockage et archivage des messages	6
4. Mots de passe	6
4.1 La gestion des mots de passe.....	7
4.2 Comment changer de mot de passe	7
5. Assistance Informatique	7

1. Préambule

Le présent guide des bonnes pratiques a pour objet d'accompagner les utilisateurs dans l'usage des outils numériques.

En complément de charte¹, Il expose les pratiques et le comportement que l'utilisateur doit adopter afin de respecter les exigences d'usage du système d'information préconisées par l'académie de Toulouse.

Pour rappel la charte s'applique à l'ensemble des utilisateurs du système d'information de l'académie de Toulouse.

On se reportera à la charte pour la définition d'un utilisateur.

Par outils numériques on entend l'ensemble du matériel, logiciel, outils informatiques et services numériques mis à la disposition de l'utilisateur par l'académie de Toulouse.

2. Poste de travail

Par définition un poste de travail est considéré comme étant l'ensemble des moyens techniques (écran, ordinateur, imprimante, portable, téléphone fixe, téléphone mobile, ...) mis à la disposition de l'utilisateur. Ce matériel nécessite une utilisation vigilante et raisonnable dans le cadre des missions professionnelles de l'utilisateur.

2.1 La sécurisation du poste de travail

Il est obligatoire pour chaque utilisateur de sécuriser son poste de travail par un mot de passe fort et non communiqué, devant être renouvelé régulièrement

Lorsque l'utilisateur décide d'utiliser des supports amovibles tels que des clés USB, ces derniers doivent être soumis à une analyse de l'antivirus.

Lorsque l'utilisateur quitte momentanément son poste, il doit le verrouiller (Ctrl+Alt+Suppr ou touche Windows+L) ainsi que configurer et activer l'écran de veille avec protection par mot de passe. En fin de journée, il est conseillé à tout utilisateur d'arrêter son poste de travail.

Les ordinateurs portables mis à disposition des personnels peuvent être protégés au moyen d'un logiciel de chiffrement préconisé par l'académie. L'objectif est que les données sensibles stockées sur ces matériels ne soient accessibles que par le détenteur du mot de passe spécifique.

2.2 Le compte de l'utilisateur

L'utilisateur possède un compte d'identification pour accéder au contenu de son poste et aux applications personnelles. Cet identifiant et ce mot de passe sont strictement personnels et confidentiels. L'utilisateur est responsable de leur conservation et s'engage à ne pas les divulguer et à ne pas s'approprier ceux d'un autre utilisateur.

Le mot de passe attribué par défaut doit être modifié (voir section 3.2).

¹ Charte régissant l'usage du système d'information de l'académie de Toulouse par les personnels

2.3 La protection logicielle : anti-virus et pare-feu (« firewall »)

Un anti-virus est un logiciel de protection qui permet d'identifier, neutraliser et éliminer les intrusions de logiciels malveillants tel que les virus informatiques.

L'anti-virus analyse la mémoire, les disques durs, les matériels amovibles (clé USB, CD, ...), le courrier électronique.

Il est obligatoire pour chaque poste de travail de l'académie, de disposer de l'anti-virus académique. Il est interdit de désactiver cet anti-virus.

Un pare-feu ou firewall permet de protéger l'ordinateur des tentatives d'attaques effectuées via Internet ou Intranet. Il est interdit de désactiver le pare-feu.

2.4 La sauvegarde des données

L'académie de Toulouse met à disposition des utilisateurs :

- des espaces de stockage de documents professionnels communs aux services et à l'académie ;
- un espace de stockage de documents professionnels propre à chaque utilisateur.

Ces lecteurs servent uniquement à stocker des documents professionnels. Tout stockage de documents privés est interdit sur ces supports.

Pour des raisons de maintenance de l'espace disque, les équipes techniques se réservent le droit d'analyser l'espace pris par l'utilisateur et le cas échéant de lui demander d'optimiser l'espace qu'il occupe.

Il est vivement recommandé de ne conserver sur ce lecteur que les fichiers ayant un intérêt pour l'activité professionnelle.

Les supports amovibles en particulier les clés USB ne doivent pas être utilisés comme un moyen de stockage principal (risque de perte/vol important).

2.5 L'utilisation du poste en mode « administrateur »

L'utilisation d'un compte avec des droits « administrateur » offre des droits étendus à l'utilisateur. En effet l'administrateur dispose d'un accès total à l'ordinateur et peut effectuer toutes les modifications souhaitées. Ce mode de paramétrage ouvre la brèche à de nombreux programmes malveillants tentant d'accéder aux ressources du poste de travail. La configuration en mode « administrateur » sera limitée et devra être motivée par le chef de service.

Afin d'éviter toute contamination, les postes sont configurés en mode « standard ». Ce mode d'utilisation permet aux utilisateurs d'utiliser la plupart des logiciels.

2.6 L'utilisation du matériel nomade

L'académie de Toulouse met à disposition de certains utilisateurs des ordinateurs portables, téléphones portables, tablettes ...

- Ces outils sont réputés n'être utilisés que dans le cadre professionnel et uniquement par son bénéficiaire. Le dit bénéficiaire est seul responsable du matériel, de ce fait il doit :
- veiller à son entretien courant et à sa bonne conservation.

- En cas de détérioration, de perte ou de vol de ce matériel, l'utilisateur est tenu d'en informer son responsable hiérarchique dans les plus brefs délais.
- Toute fausse déclaration est passible de sanctions disciplinaires et/ou de poursuites pénales

2.7 L'utilisation d'outils personnels

La connexion de matériels portables personnels au réseau interne de l'académie de Toulouse n'est pas autorisée.

Seul le matériel fourni par l'académie est autorisé à se connecter au réseau de l'académie de Toulouse.

Les matériels portables personnels peuvent, sur autorisation, se connecter au réseau Wi-Fi invité du rectorat de Toulouse. Il est nécessaire pour cela de se rapprocher de l'accueil du rectorat pour les instructions de connexion ou de consulter la documentation disponible sur le site de la Direction de Systèmes d'Information² à la rubrique Wi-Fi.

2.8 Le téléchargement

L'utilisateur s'engage à ne pas installer de logiciels sans y être autorisé. Tout téléchargement de logiciel doit se faire avec vigilance et dans le respect du droit de la propriété intellectuelle.

L'utilisation d'un logiciel tiers nécessaire pour l'accomplissement des missions doit faire l'objet d'une validation de la DSI avant son installation.

2.9 L'utilisation des services en ligne

L'utilisateur s'engage à utiliser les services (messagerie, partage de gros fichiers, sondages de rendez-vous, agenda ...) mis en place par l'académie. L'utilisation de services en ligne externes est contraire aux bonnes pratiques recommandées par l'académie.

3. Messagerie électronique

3.1 Caractéristiques et limitations de la messagerie électronique

L'académie de Toulouse n'exerce aucune surveillance ni aucun contrôle éditorial sur les messages envoyés dans le cadre de la messagerie électronique. L'académie ne pourra, de ce fait, en être considérée responsable.

L'utilisateur est tenu d'informer le RSSI de l'académie³ de tout message suspect ou d'utilisateurs non identifiés.

Le compte d'accès à la messagerie est constitué d'un identifiant et d'un mot de passe strictement personnels et confidentiels. L'utilisateur est responsable de leur conservation et s'engage à ne pas les divulguer et à ne pas s'approprier ceux d'un autre utilisateur. Il est nécessaire de noter que ce couple d'identifiant est également nécessaire pour accéder à la plupart des applications informatiques et des applications « métier » de l'académie de Toulouse.

Le mot de passe doit être renouvelé régulièrement. L'académie de Toulouse préconise son changement au minimum une fois par an. L'outil académique MA-MAMIA peut être utilisé à cet effet comme stipulé en section 3.2.

² <https://dsi.ac-toulouse.fr>

³ Contact via le formulaire du portail SSI sur <https://ssi.ac-toulouse.fr>

L'adresse électronique fonctionnelle ou organisationnelle peut être mise en place si elle est exploitée par un service ou un groupe d'utilisation.

L'académie de Toulouse conserve durant une période d'une année, les entêtes (destinataire, émetteur, sujet et le nombre de pièces jointes) de tout message transmis par la messagerie électronique de l'académie.

Toutefois, il est conseillé de conserver les messages durant le temps nécessaire afin de garantir l'exercice de ses activités et de constituer un élément de preuve.

3.2 La gestion de la messagerie en cas d'absence

Lorsque l'utilisateur s'absente pour une période prolongée, afin de garantir la continuité du service, il est nécessaire d'activer le système de message de notification d'absence.

Cette activation s'opère via le webmail⁴ dans l'onglet « Option » puis « message de notification d'absence », il est nécessaire de compléter les dates du congé ainsi que le message de réponse automatique afin d'orienter si nécessaire l'expéditeur vers un interlocuteur habilité à assurer la correspondance.

3.3 Stockage et archivage des messages

Chaque utilisateur doit organiser et assurer la conservation des messages pouvant être indispensables à l'exercice de ses activités ou simplement utiles en tant qu'éléments de preuve.

La messagerie des personnels n'est pas sauvegardée Les utilisateurs doivent donc procéder à un archivage personnel.

Chaque utilisateur reste responsable de l'archivage et du classement des messages qu'il a relevés.

Chaque utilisateur doit en conséquence organiser lui-même la conservation de ces éléments en décidant :

- de la périodicité de l'archivage;
- du choix des fichiers et messages conservés et de ceux qui sont détruits ;
- de la méthode et de la durée de stockage.

4. Mots de passe

Pour accéder aux outils informatiques, mis à disposition par l'académie de Toulouse l'utilisateur dispose d'identifiants qui lui sont propres et qui lui permettent de s'authentifier :

- un compte utilisateur (soit 1ère lettre du prénom suivi du nom d'usage soit l'adresse de la messagerie professionnelle)
- un mot de passe dont le changement est impératif lors de la première utilisation du poste de travail.

⁴ <https://messagerie.ac-toulouse.fr>

4.1 La gestion des mots de passe

L'utilisateur s'engage à respecter la politique de gestion des mots de passe de l'académie afin de lutter contre les vols de mot de passe. Les principaux éléments à prendre en compte sont :

- d'utiliser un mot de passe différent du mot de passe que vous utilisez pour vos services privés. En particulier, l'utilisation d'un même mot de passe pour la messagerie professionnelle et pour la messagerie personnelle est à proscrire ;
- choisir un mot de passe qui n'a aucun lien avec l'utilisateur (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ou avec un mot du dictionnaire ;
- Pour renforcer la sécurité de votre compte, votre mot de passe doit contenir au moins 8 caractères, au moins une minuscule et une majuscule, au moins un chiffre et au moins un caractère non-alphanumérique (&,#,*,|,,\$,...).ne pas demander à un tiers de générer un mot de passe préfabriqué ;
- ne pas afficher ses mots de passe (exemple sur un post-it) ;
- modifier immédiatement les mots de passe attribués par défaut ;
- renouveler les mots de passe à une fréquence raisonnable. Au minimum tous les ans pour les systèmes contenant des données professionnelles et sensibles;
- ne jamais stocker les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : connecté à internet), encore moins sur un papier facilement accessible ;
- l'académie de Toulouse préconise l'utilisation du logiciel libre dénommé KeePass : ce logiciel est un coffre-fort numérique pour tous les mots de passe. Il permet de stocker les mots de passe dans un même et seul fichier et ceci de manière sécurisée. Néanmoins, il est important de protéger le logiciel par un mot de passe fort. Ce mot de passe ne doit pas être oublié afin de ne pas bloquer l'accès au logiciel et par suite perdre tous ses autres mots de passe ;
- ne jamais communiquer oralement, par écrit ou par mail ses identifiants et mots de passe, y compris au service informatique ;
- attention aux messages piégés : un service informatique ne vous demandera jamais vos mots de passe par mail, par téléphone ou via un formulaire, pour quelque raison que ce soit ;
- configurer les logiciels, y compris son navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe.

4.2 Comment changer de mot de passe

L'outil académique « MA-MAMIA », disponible sur le site de la Direction des Systèmes d'Information de l'académie de Toulouse, permet de modifier le mot de passe de messagerie, lprof, Intranet de l'académie, portail d'applications métiers ARENA, ...

Pour toute autre question relative aux mots de passe, rendez-vous sur le portail⁵ de la Sécurité des systèmes d'information de l'académie de Toulouse.

5. Assistance Informatique

Vous pouvez contacter l'assistance académique pour tout problème technique rencontré :

⁵ <https://ssi.ac-toulouse.fr> également accessible via le portail de la DSI rubrique SSI <https://dsi.ac-toulouse.fr>

- par téléphone : 0810 000 282 (N° Azur, prix d'un appel local)

- par email : assistance@ac-toulouse.fr

L'assistance académique est disponible du lundi au vendredi, sauf jours fériés, de 8h00 à 18h00.

Le service est interrompu pendant 5 semaines à partir du 15 juillet ainsi que du 25 décembre au 1er janvier.