6. Soyez vigilant

6.1 Chaque utilisateur peut contribuer, à son niveau, à la sécurité du système d'information. Il doit alerter sans retard sa hiérarchie et/ou ses correspondants techniques dès qu'il constate une anomalie, un dysfonctionnement ou s'il est à l'origine d'une erreur d'utilisation du système d'information.

6.2 Chaque utilisateur a un devoir de confidentialité à l'égard des informations et documents disponibles dans le système d'information.

6.3 La tendance aujourd'hui est d'utiliser ses appareils numériques personnels au bureau (smartphones, tablettes, portables).
Il est par conséquent important de maintenir un niveau de sécurité optimal sur ces appareils avec notamment un suivi des mises à jour du système d'exploitation. Ces matériels peuvent le cas échéant présenter une menace pour l'ensemble de notre système d'information. En cas de synchronisation de données avec nos systèmes d'information, les pertes ou vols de ces appareils doivent être signalés à la DSI.

7. Préservez vos données et votre poste

7.1 Ayez conscience des menaces

les virus : ils se propagent instantanément et peuvent détruire ou altérer les données stockées sur votre poste.

les logiciels espions (Spyware) : il s'agit de programmes malveillants espions installés à votre insu sur votre poste, par exemple lors de vos navigations sur internet. Ils peuvent:
- enregistrer vos identifiants, mots de passe, numéros de compte etc... (cas des "keyloggers"). Vos données ainsi piratées pourront servir à commettre des actes illégaux en votre nom.
- collecter des informations sur vos usages (adresses des sites visités, votre profil d'utilisateur, adresses de vos contacts messagerie, etc...).
- permettre de contrôler à distance votre poste de travail pour l'intégrer à un réseau de piratage de type "botnet".

les ransomwares : ce sont des logiciels malveillants qui prennent en otage vos données personnelles. Ces logiciels chiffrent les données puis demandent à leur propriétaire une somme d'argent en échange de la clé qui permettra de les déchiffrer.
Avant toute intervention, il faut impérativement contacter le service d'assistance informatique de la DSI.

7.2 Evitez les comportements à risques
A titre d'exemple :
- avec la messagerie (cf. §4)
- aux cours de vos navigations sur internet, ne donnez surtout pas vos coordonnées sur n'importe quel site. N'acceptez pas les pop-ups non sollicitées.
- utilisez vos supports de stockage USB avec prudence. Dans la mesure du possible, privilégiez la messagerie pour des échanges de fichiers de taille inférieure à 30 mégaoctets.

7.3 Utilisez un anti-virus
Protégez l'ensemble de vos postes de travail, y compris ceux de votre domicile. Vous pouvez bénéficier à des fins personnelles de l'antivirus Trend acquis par le ministère de l'EN

https://pia.ac-dijon.fr
(Onglet « Espace documentaire »
puis Rubrique « Téléchargement d'applications »)

7.4 Veillez à ce que les systèmes d'exploitation (Windows, Linux) de vos PC soient à jour.

8. Ayez un comportement éco-citoyen

8.1 Vous vous absentez : éteignez votre micro et votre écran. Ayez également ce réflexe à la pause méridienne et bien sûr en fin de journée. Au-delà des économies d'énergie générées, cette consigne est un des éléments de la sécurité d'accès au SI.

8.2 Dans la mesure du possible, privilégiez les éditions **recto/verso.**

8.3 Jugez de la nécessité de lancer une impression ou de faire des copies papier.

9. Cherchez des informations et organisez votre bureau

Utilisez le **PIA** (Portail Intra Académique) : https://pia.ac-dijon.fr avec, à votre disposition :

- des services numériques de base
- un bureau à organiser à partir d'une bibliothèque de « widgets »
- un espace documentaire

10. N'hésitez pas à demander de l'assistance

Pour tout problème technique ou pour des conseils :

Faire une demande sur le serveur d'assistance :
accessible depuis la page d'accueil du PIA,
Rubrique « Services pratiques »

Conception / réalisation :
D.S.I.
DIRECTION DES **S**YSTEMES D'**I**NFORMATION
DE L'ACADEMIE DE DIJON

académie Dijon

MINISTÈRE
DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

TIC SUR DIX

10 bonnes praTICs pour l'utilisation du numérique dans les services académiques

TIC sur Dix !

1. Respectez les règles de base

Vous disposez d'un accès à une ou des applications « métiers », d'une adresse électronique et d'un accès à internet.
Ces moyens mis à disposition par le Rectorat sont destinés à un usage professionnel pour assurer les missions qui vous sont confiées.
Vous devez les utiliser en respectant les principales obligations qu'impose le statut général des fonctionnaires.
L'usage à des fins personnelles est toléré à condition d'être exceptionnel et de ne pas gêner les activités du service.

2. Identifiez-vous ! Pour cela, il vous faut un login et un mot de passe

En informatique, on appelle identifiant (ou login en anglais) les informations permettant à une personne d'accéder à un système informatique. Votre identifiant est UNIQUE et strictement PERSONNEL. Il est associé à un mot de passe qui doit être particulièrement SECURISE pour ne pas être usurpé.

Comment choisir un bon mot de passe ?
Pas de mot de passe simple.
Le mot de passe doit être robuste : 8 caractères minimum, 1 ou 2 caractères spéciaux conseillés. En outre, il ne doit correspondre à aucun mot de dictionnaires (français/anglais notamment).
Ne l'affichez pas. Ne le confiez à personne.
Consultez les recommandations :

https://pia.ac-dijon.fr
(Onglet « Espace documentaire »,
Rubriques : « Recueil des publications » puis « TIC »
et « Sécurité »)

Un identifiant, pour qui, pour quoi ?
Cet identifiant vous sert à accéder à votre messagerie personnelle, votre dossier administratif, votre portail académique (PIA), vos applications.

Ces identifiants et mots de passe vous donnent accès à des données privées et/ou confidentielles. Les diffuser volontairement ou accidentellement peut vous engager personnellement.

3. Utilisez correctement le réseau

3.1 Déconnectez-vous systématiquement des applications lorsque vous quittez momentanément votre PC.
3.2 Fermez ou verrouillez la session quand l'ordinateur reste allumé et que vous vous absentez.
3.3 Eteignez votre poste, une fois votre travail terminé.
3.4 Ne tentez pas d'accéder à des ressources informatiques pour lesquelles vous ne bénéficiez pas d'une habilitation.
3.5 N'installez pas et ne téléchargez pas sur les postes informatiques un logiciel inutile ou sans licence d'utilisation.
3.6 Le téléchargement de vidéo et de musique ou l'écoute de radio en ligne peuvent sérieusement perturber le fonctionnement du réseau et sont interdits à des fins personnelles.

4. Utilisez correctement la messagerie

4.1 Attention aux messages reçus !
Afin de ne pas fragiliser l'ensemble du système d'information, soyez très prudent avec les messages que vous recevez.
Ils peuvent être **vecteurs de virus** mais aussi servir à **subtiliser vos coordonnées de connexion ("messages de phishing") !**

4.2 Contre la propagation des virus
Vérifiez que l'objet du message ou son contenu sont en rapport avec la ou les pièce(s) jointe(s) annoncée(s). En cas de doute sur la nature de la pièce jointe, ne l'ouvrez pas et transférez le message pour analyse à l'adresse électronique : spam@ac-dijon.fr

4.3 Contre le "phishing" ou l' "hameçonnage"
Méfiez-vous des messages qui, sous un prétexte quelconque (changement de messagerie, taille de boîtes aux lettres, réinitialisation des mots de passe etc...), vous invitent à répondre en communiquant vos identifiants et mots de passe.
Sous aucun prétexte, il ne faut les transmettre par écrit (mail) ou par oral (par exemple en réponse à un appel téléphonique).

De même, dans votre intérêt, ignorez les messages qui demandent vos coordonnées bancaires ou votre code de carte bancaire.

4.4 Quelques règles pour l'envoi de vos messages
Ciblez votre message : l'objet doit refléter le contenu de votre message.
Soignez le contenu : soyez prudent dans vos formulations : vos messages vous engagent et peuvent engager le Rectorat.
Rédigez vos messages de manière claire et concise. Ce qui ne vous dispense pas d'être courtois (cf. nétiquette).
Annoncez les pièces jointes : signalez les dans le corps de vos messages pour éviter toute ambiguïté sur leur nature (virus, codes malveillants).
Soyez attentif à la taille des fichiers joints : un message trop volumineux peut être rejeté par le serveur de messagerie. La limite est de 30 mégaoctets dans l'académie de Dijon.

Ciblez vos destinataires : notamment lorsque vous répondez à un message diffusé à une liste de diffusion, vérifiez bien si vous vous adressez à l'auteur -en réponse privée donc- ou à l'ensemble de la liste.
Ne multipliez pas l'envoi de messages : ils ne seront plus lus.
Donnez toutes les citations, références et sources et respectez les accords de Copyright.

5. Faites un bon usage d'internet

5.1 Charte
Elle précise de manière contractuelle les droits et devoirs de l'utilisateur et de l'administration en rappelant notamment la législation liée à la protection de la vie privée et au respect de la propriété intellectuelle. Elle s'inscrit dans un objectif de sensibilisation et de responsabilisation. Vous pouvez en prendre connaissance sur l'espace documentaire du PIA, à l'adresse :

https://pia.ac-dijon.fr
(Onglet « Espace documentaire »
Rubriques « Recueil des publications et documentation » puis « TIC »
et « Aspects juridiques »)

5.2 Respectez la loi - Adoptez un comportement responsable
La loi est applicable sur internet, comme dans la vie courante : un délit sur internet est passible de la même peine qu'un délit « réel ». Le code civil est complété par des textes spécifiques, comme la Loi de Confiance dans l'Economie Numérique (LCEN), accessibles notamment à l'adresse :

http://www.cnil.fr

5.3 Signalez les contenus illicites ou douteux

Vous pouvez signaler des contenus de sites web illicites à l'adresse électronique : internet-signalement@ac-dijon.fr