

CHARTRE NUMERIQUE STAGIAIRE

Utilisation des ressources informatiques

Objectif	Comprendre les règles simples pour utiliser les ordinateurs, Internet, le réseau et les outils numériques de l'ADEA.
Principe	J'utilise les outils numériques pour apprendre, travailler et communiquer dans un cadre respectueux et sécurisé.

1. A quoi sert cette charte ?

Cette charte explique les règles à respecter quand j'utilise les ressources informatiques de l'ADEA. Elle concerne les ordinateurs, les tablettes, les imprimantes, le réseau, le Wi-Fi, Internet, les logiciels, les fichiers, les services en ligne et les outils mis à disposition pendant ma formation. Elle s'applique aussi quand j'utilise un compte, un accès ou un matériel fourni par l'ADEA.

A retenir	Les outils numériques de l'ADEA sont faits pour la formation. Je les utilise avec respect, prudence et responsabilité.
------------------	--

2. Mes engagements simples

- Je respecte les personnes, leur vie privée et leur image.
- Je respecte le matériel et les logiciels de l'ADEA.
- Je garde mes identifiants et mes mots de passe pour moi.
- Je demande de l'aide si je ne sais pas quoi faire.
- Je signale rapidement tout problème, message suspect ou incident informatique.

3. Ce qui est interdit

Je ne dois pas utiliser les ressources informatiques de l'ADEA pour consulter, télécharger, créer, copier ou diffuser des contenus interdits par la loi.

- Je ne diffuse pas de propos injurieux, diffamatoires, racistes, discriminatoires, violents ou haineux.
- Je ne consulte pas et je ne diffuse pas de contenus pornographiques, violents ou dangereux.
- Je ne provoque pas à commettre des actes illicites ou dangereux.
- Je ne porte pas atteinte à la vie privée ou à l'image d'une personne.
- Je ne télécharge pas illégalement de musique, de films, de photos, de livres, de logiciels ou d'autres oeuvres protégées.
- Je ne copie pas de logiciel commercial sans autorisation.
- Je ne tente pas de contourner, forcer ou désactiver les protections informatiques.

Important	Si un contenu me semble choquant, illégal ou dangereux, je ferme la page et j'en parle à un formateur ou à un membre de l'équipe ADEA.
------------------	--

4. Internet, messagerie et réseaux sociaux

Internet et la messagerie doivent être utilisés dans le cadre de la formation et des activités autorisées par l'ADEA.

- Je vérifie les informations avant de les partager.
- Je ne clique pas sur un lien ou une pièce jointe si le message me semble suspect.
- Je ne réponds pas à une demande de mot de passe reçue par mail ou message.
- Je n'utilise pas les outils de l'ADEA pour harceler, insulter ou menacer quelqu'un.
- Je n'utilise pas les outils de l'ADEA pour des activités commerciales, militantes ou personnelles non autorisées.

Bon réflexe

Un doute sur un mail, un lien ou un fichier ? Je demande avant de cliquer. C'est simple et ça évite les galères numériques.

5. Mots de passe et sécurité

Mes identifiants sont personnels. Ils protègent mon travail, mes données et le réseau de l'ADEA.

- Je ne donne jamais mon mot de passe à une autre personne.
- Je ne note pas mon mot de passe sur un papier visible ou dans un fichier non protégé.
- Je verrouille ou ferme ma session quand je quitte mon poste.
- Je prévient l'ADEA si je pense que mon compte a été utilisé par quelqu'un d'autre.
- Je respecte les consignes données par l'équipe pédagogique ou informatique.

6. Fichiers et travail des autres

Je respecte le travail des autres stagiaires, des formateurs et de l'équipe ADEA.

- Je n'ouvre pas les fichiers qui ne me concernent pas.
- Je ne modifie pas et je ne supprime pas les fichiers d'une autre personne.
- Je ne déplace pas les dossiers ou fichiers partagés sans autorisation.
- Je nomme et range mes fichiers de manière claire.
- Je fais attention quand je partage un document contenant des données personnelles.

7. Données personnelles et confidentialité

Certaines informations sont personnelles : nom, prénom, adresse, téléphone, mail, photo, situation sociale, santé, parcours, notes, présence en formation.

- Je ne diffuse pas les informations personnelles d'une autre personne sans autorisation.
- Je ne prends pas et je ne publie pas la photo ou la vidéo d'une personne sans accord.
- Je ne copie pas de documents internes ou confidentiels sur un espace personnel sans autorisation.
- Je n'envoie pas de données personnelles vers un service en ligne ou une IA générative sans accord de l'ADEA.
- Je prévient un formateur si j'ai envoyé une information personnelle par erreur.

Exemple

Je ne colle pas une liste de stagiaires, des notes ou une situation personnelle dans un outil d'IA sans autorisation. Même si l'outil a l'air pratique.

8. Matériel et salles informatiques

Dans les salles équipées de matériel informatique, je prends soin du matériel mis à disposition.

- Je ne branche pas et je ne débranche pas de périphérique sans autorisation : casque, enceinte, souris, clavier, écran, câble, clé USB ou autre matériel.
- Je ne déplace pas le matériel sans accord du personnel de l'ADEA.
- Je ne modifie pas les réglages d'un ordinateur sans consigne.
- Je ne mange pas et je ne bois pas au-dessus du matériel informatique.
- Je signale rapidement une panne, un câble abîmé ou un comportement anormal de l'ordinateur.

9. Contrôle, assistance et prise en main à distance

L'ADEA peut mettre en place des moyens de contrôle et d'assistance pour protéger le réseau, le matériel, les données et le bon déroulement de la formation.

- Le personnel habilité peut vérifier l'utilisation des ressources informatiques dans un cadre pédagogique, technique ou de sécurité.
- Une visualisation ou une prise en main à distance peut être réalisée pour aider, dépanner ou sécuriser un poste.
- Quand c'est possible, je suis informé avant l'intervention.
- En cas d'urgence technique ou de risque de sécurité, l'ADEA peut intervenir rapidement pour protéger le réseau ou le matériel.
- Ces contrôles doivent rester proportionnés. Ils ne servent pas à surveiller les stagiaires en permanence.

Clarté

Les contrôles informatiques ont pour but la sécurité, l'assistance et le respect de la charte. Ils ne remplacent pas la confiance.

10. Vidéosurveillance des locaux

Je suis informé que certains espaces des locaux de l'ADEA sont placés sous vidéosurveillance.

- Le but est d'assurer la sécurité des personnes, des biens et des locaux.
- Les zones concernées sont signalées par un affichage visible dans l'établissement.
- Les images ne sont pas utilisées pour surveiller les stagiaires en permanence.
- Les images ne servent pas à contrôler l'assiduité ou le travail pédagogique des stagiaires.
- Seules les personnes habilitées par l'ADEA peuvent regarder les images, en cas d'incident ou de besoin justifié.
- Si nécessaire, les images peuvent être transmises aux autorités compétentes.
- Les images sont conservées pendant une durée limitée, adaptée à l'objectif de sécurité. En principe, cette durée ne dépasse pas un mois, sauf extraction nécessaire dans le cadre d'une procédure.
- Pour exercer mes droits sur les images qui me concernent, je peux contacter le DPO : dpo@adea-formation.com.

11. Si je ne respecte pas la charte

Si je ne respecte pas cette charte, l'ADEA peut prendre des mesures adaptées à la situation.

- Un rappel des règles peut être fait.
- Mon accès aux ressources informatiques peut être limité ou suspendu.
- Une mesure disciplinaire peut être prise selon le règlement intérieur de l'ADEA.
- En cas de fait grave ou illégal, l'ADEA peut effectuer les démarches nécessaires auprès des autorités compétentes.

Principe

La sanction n'est pas automatique. Elle dépend des faits, de leur gravité et du cadre prévu par le règlement intérieur.