

Code de conduite pour l'utilisation des ressources informatiques

Principe directeur

Les ressources informatiques de l'Université d'Ottawa servent à appuyer ses activités d'enseignement et de recherche.

Infractions au Code et mesures disciplinaires

Les infractions au Code de conduite, les plaintes concernant des infractions et les mesures disciplinaires envers les contrevenants sont régies par les lois et règlements applicables, par les règlements et méthodes de l'Université ainsi que par les contrats de travail et les conventions collectives.

Définitions

1. **Compte** : Tout numéro de compte, code d'accès, code d'utilisateur ou autre code d'autorisation attribué à l'égard d'une ressource informatique.
2. **Ressource informatique** : Entre autres, les ordinateurs, périphériques, logiciels, données, réseaux et autre matériel que l'Université d'Ottawa possède ou gère.
3. **Usager** : Toute personne à qui l'Université a attribué un compte ou des ressources informatiques.

Engagement et responsabilité de l'utilisateur

L'utilisateur accepte l'entière responsabilité de l'usage de son compte et des ressources informatiques qui lui sont attribuées et s'engage à respecter le Code de conduite ci-après.

Droits de l'Université d'Ottawa

Si l'Université soupçonne une infraction au Code de conduite, elle se réserve le droit d'enlever tout matériel placé dans un compte ou une ressource informatique et de suspendre l'accès à un compte ou à une ressource informatique en attendant la tenue d'une enquête, s'il y a lieu.

L'Université n'entérine et n'approuve le contenu ou les données que les utilisateurs ont dans leurs comptes ni ce qui apparaît sur leur site Web personnel.

Responsabilités des utilisateurs

Selon le Code de conduite, les utilisateurs doivent :

1. Utiliser uniquement le compte que leur attribue l'Université et respecter toutes les restrictions s'y rapportant.

2. Prévenir l'accès illicite à tous les comptes et aux ressources informatiques mis à leur disposition en utilisant des mots de passe et d'autres méthodes de contrôle, et préserver en tout temps la confidentialité de leurs mots de passe et de leurs codes d'accès.
3. Ne jamais se faire passer pour d'autres usagers ou pour toute autre personne.
4. Utiliser leurs comptes et les ressources informatiques uniquement pour les fins autorisées.
5. Ne jamais utiliser leurs comptes et les ressources informatiques à des fins commerciales personnelles ou pour en tirer un gain financier.
6. Empêcher l'utilisation de leurs comptes et des ressources informatiques par d'autres personnes, y compris les membres de leur famille, leurs amis, leurs connaissances, etc..
7. Ne jamais transmettre, afficher ou stocker du matériel à caractère obscène ou pornographique ni d'autre matériel assujetti aux lois ou règlements applicables.
8. Ne jamais envoyer des communications harcelantes ou envoyer en vrac des messages électroniques non autorisés et non sollicités.
9. Ne jamais intercepter ni tenter d'intercepter une communication réseau (entre autres, un courriel, une conversation privée) qui ne leur est pas destinée.
10. Ne jamais perturber ni tenter de perturber l'utilisation d'un compte ou des ressources informatiques ce qui pourrait nuire au bon fonctionnement des opérations normales.
11. Ne jamais utiliser les comptes ou les ressources informatiques pour accéder illicitement à des ressources non universitaires.
12. Préserver les comptes et les ressources informatiques en utilisant des méthodes et des dispositifs de protection efficaces tels que la modification régulière du mot de passe, un logiciel anti-virus et la sauvegarde périodique des données.
13. Respecter les droits d'auteur, les marques de commerce et les noms commerciaux ainsi que les licences rattachés aux logiciels ou à d'autre matériel.

Cabinet du secrétaire, 562-5950

Approuvé par le Comité d'administration le 4 octobre 2000