

Numéro du document normatif	
Instance d'approbation	Conseil de gouvernance
Responsabilité administrative	Vice-rectorat à l'administration
Date d'approbation	15 septembre 2021
Date d'entrée en vigueur	15 septembre 2021
Date de dernière révision	

POLITIQUE SUR L'UTILISATION DES INSTALLATIONS NUMÉRIQUES

1. Objectif

En tant que propriétaire et gestionnaire des installations numériques, l'Université de l'Ontario français (ci-après « Université ») assure avec vigilance et rigueur l'encadrement pour en assurer une utilisation adéquate. L'Université fait preuve de diligence en se dotant de moyens d'interventions lui permettant notamment de retirer les informations portées à son attention comme étant préjudiciables ou contraires aux lois en vigueur. De plus, l'Université tient à sensibiliser tous les utilisatrices et utilisateurs à l'importance de recourir aux équipements numériques aux fins pour lesquelles ils ont été conçus et non à des fins autres qui pourraient être préjudiciables pour l'Université ou contraires aux lois applicables en la matière.

2. Champ d'application et portée

La présente politique s'applique à tous les membres du corps professoral, du personnel, des étudiantes et des étudiants, des diplômées et des diplômés, des locataires et des visiteurs ainsi qu'à toute personne autorisée à utiliser les installations numériques de l'Université.

3. Valeurs et principes d'application

Les installations numériques de l'Université sont mises à la disposition de la population étudiante, des membres du corps professoral, du personnel, des diplômées et des diplômés, des visiteurs et des locataires et autres utilisatrices et utilisateurs pour faciliter l'apprentissage, l'enseignement, la recherche ainsi que l'administration qui soutient ces buts. Il incombe à tout utilisatrices et utilisateurs de s'abstenir de gaspiller les ressources, de nuire au travail d'autrui et d'enfreindre les politiques et lois applicables.

4. Définitions

Aux fins de la présente politique, les expressions ou termes suivants sont définis comme suit :

- a) Administratrices et administrateurs de systèmes : les responsables de solutions et logiciels qui assurent la gestion de l'environnement numérique de l'Université.

- b) Installations numériques de l'Université : tout ordinateur, périphérique, téléphone, Internet, Intranet, logiciel ou toute combinaison de ces éléments appartenant à l'Université, sous sa garde ou sous sa responsabilité. Le matériel et les logiciels achetés au moyen des fonds de recherche administrés par l'Université appartiennent à l'Université sauf indications contraires clairement stipulées dans la subvention ou le contrat de recherche en question.

5. Rôles et responsabilités

- 5.1. L'Université, dans la mesure de ses moyens, est responsable de fournir les ressources nécessaires aux usagers afin qu'ils assument leurs responsabilités quant à l'utilisation sécuritaire des installations et ce, dans le cadre d'une saine gestion des risques pour l'Université. Cependant, l'Université ne pourra être tenue responsable des pertes, dommages, manques à gagner ou inconvéniens qui pourraient être causés à un usager à l'occasion ou en conséquence de l'utilisation d'un équipement ou advenant le cas où l'Université devrait, pour quelque cause que ce soit, diminuer ses services, ou les interrompre, quelle que soit la durée de telles diminution ou interruption. De plus, l'Université ne pourra être tenue responsable de tout défaut ou retard d'exécution causé par des circonstances de force majeure.
- 5.2. Le vice-rectorat à l'administration, par le biais de la direction des stratégies numériques, est responsable de l'application, l'interprétation et la révision de la présente politique.
- 5.3. Les administratrices et administrateurs de systèmes dûment autorisés ont l'obligation de prendre des mesures raisonnables appropriées pour assurer l'intégrité des systèmes et le respect de la présente politique.

6. Principes généraux

- 6.1. L'utilisation des installations numériques à des fins personnelles doit respecter la présente politique et ne doit en aucun temps causer un préjudice à l'Université.
- 6.2. Afin de protéger les installations contre les incidents, les pannes ou les actes de malveillance, l'Université se réserve le droit de limiter, de restreindre ou de supprimer l'accès de tout utilisateur à ses installations ou de tout hôte ou appareil au réseau et d'inspecter, de copier, ou de retirer les données, les fichiers ou les ressources du système.
- 6.3. L'Université n'offre aucune garantie expresse ou implicite en ce qui concerne les ressources et les installations numériques offertes ou leur convenance à un but particulier. La fonction des administratrices et administrateurs de systèmes est de servir le bassin d'utilisateurs dans la communauté universitaire, mais on ne peut s'attendre à ce qu'ils répondent à chacun des besoins spécialisés.

7. Gestion de l'accès aux installations numériques

- 7.1. L'accès aux installations numériques de l'Université a pour but la poursuite de la mission pédagogique et l'exécution des fonctions administratives de l'Université, et non la poursuite des gains commerciaux ou de publicité gratuite sauf dans le cas des services universitaires ou de sous-traitants qui respectent les paramètres définis dans le cadre de leur mission. De même, la publicité indirecte n'est autorisée que dans les limites de ces paramètres. Ainsi, il est interdit de vendre de l'espace publicitaire sur les plateformes Web de l'Université (incluant les médias sociaux), sauf si une politique interne l'autorise.

- 7.2. L'accès aux installations numériques de l'Université ne peut être utilisé pour les envois de masse non sollicités, notamment les lettres et publicités en chaîne, sauf par les services de l'Université et les sous-traitants qui agissent dans le cadre de leurs missions définies par l'Université. Les courriels de masse non sollicités doivent être utilisés avec modération et seulement par les canaux de distribution approuvés par le service des communications et le service de l'information pour l'enseignement.
- 7.3. L'identifiant et le mot de passe sont réservés à l'usage exclusif de la personne à qui ils sont destinés. Le partage des identifiants et mots de passe parmi les personnes autorisées (par ex., utilisation d'un compte collectif) est déconseillé et interdit dans toutes autres circonstances. Toute responsabilité incombe uniquement à la personne officiellement porteuse de l'identifiant.
- 7.4. L'Université doit s'assurer qu'elle peut repérer toute utilisation du réseau à partir de son organisation interne afin de retrouver l'autrice ou l'auteur. Par conséquent, la provenance de tout courriel ou message d'un groupe de diffusion (ou toute autre communication électronique) doit être exacte et clairement indiquée. Par exemple, la rubrique de l'expéditrice ou de l'expéditeur doit contenir une adresse valide correspondant au compte numérique de la personne.
- 7.5. Il est interdit d'utiliser une partie des installations numériques de l'Université sans l'autorisation de l'administratrice et de l'administrateur du système concerné.
- 7.6. Les utilisatrices et utilisateurs ne doivent pas se servir des installations numériques pour obtenir ou échanger des logiciels, des informations ou autre matériel numérique protégés par des droits d'auteur quand une telle action porte atteinte aux droits d'auteur.
- 7.7. Les utilisatrices et utilisateurs ne doivent pas se servir des installations numériques dans un but non autorisé ou illicite tel que, entre autres : la destruction ou l'altération de données appartenant à autrui, l'entrave à un accès légitime, la rupture des communications au sein des installations numériques, la tentative de piratage des systèmes de sécurité des installations numériques ou de toutes autres installations numériques.

Si une administratrice ou un administrateur de réseau soupçonne qu'une utilisatrice ou un utilisateur abuse du privilège d'accès aux installations numériques décrit dans la présente politique, cette personne peut se voir temporairement retirer ce privilège, dans l'attente d'une enquête.

- 7.8. Les utilisatrices et utilisateurs ne doivent pas profiter des installations numériques pour envoyer des messages obscènes, vulgaires ou de harcèlement par courrier électronique ou par tout autre moyen. L'Université a prévu des politiques pour sanctionner ces actes de malveillance et elles seront appliquées, s'il y a lieu.

Les cas de malveillance numérique peuvent aussi constituer un motif de recours en vertu du Code des droits et des obligations, du Code de conduite (pédagogique), d'autres politiques de l'Université, ou des lois fédérales ou provinciales.

8. Gestion de l'accès des utilisatrices et utilisateurs

- 8.1. Les administratrices et administrateurs de systèmes accordent un accès libre, mais limité à certains éléments particuliers des installations numériques de l'Université par les systèmes met à leur disposition, aux groupes d'utilisatrices et utilisateurs suivants :

- a. les étudiantes et étudiants à temps plein et à temps partiel ;
 - b. les membres du corps professoral à temps plein et à temps partiel et chercheuses et chercheurs;
 - c. le personnel administratif et de soutien à temps plein ; le personnel administratif et de soutien à temps partiel détenant des postes à contrat.
- 8.2. En plus des groupes d'utilisatrices et utilisateurs énumérés à l'article 8.1., des arrangements spéciaux sont possibles et ce, à la discrétion du Vice-rectorat à l'administration.
- 8.3. Les utilisatrices et utilisateurs suivants n'ont pas accès aux installations numériques de l'Université, mais peuvent en faire la demande en vertu du paragraphe 8.2 ci-haut :
- a. les employées et employés occasionnels ;
 - b. les sous-traitantes et sous-traitants.
- 8.4. En raison des limitations de ressources, les différents groupes d'utilisatrices et utilisateurs reçoivent des services différents mais en général, l'accessibilité au réseau est équivalente. Les utilisatrices et utilisateurs ont le droit de se servir du matériel d'accès public, d'exploiter des programmes sur des ordinateurs désignés, d'utiliser les services de réseau et d'emmagasiner des fichiers.
- 8.5. Sur les systèmes, les étudiantes et les étudiants conservent leur identifiant tant qu'elles sont inscrites et ils sont inscrits et que le compte lui-même est actif.
- 8.6. L'identifiant attribué aux étudiantes et étudiants des cycles supérieurs demeure actif tant qu'elles sont inscrites et qu'ils sont inscrits ou que leur professeure superviseuse ou professeur superviseur autorise leurs activités.
- 8.7. Les membres du corps professoral et le personnel administratif et de soutien peuvent conserver leur identifiant tant qu'elles ou qu'ils sont à l'emploi de l'Université. Tous les ans, elles et ils seront avisés de l'identifiant dont elles et ils sont responsables. Si elles ou ils n'ont plus besoin d'avoir accès aux installations numériques, elles et ils doivent en informer le Service TIE ou leur administratrice ou administrateur de réseau.
- 9. Confidentialité de l'information**
- 9.1. Toute utilisatrice et utilisateur est en droit de s'attendre raisonnablement au respect de la confidentialité de la part de tout autre utilisatrice et utilisateur.
- 9.2. L'information détenue par une utilisatrice ou un utilisateur lui appartient, sauf si celle-ci ou celui-ci prend des mesures spécifiques pour mettre l'information à la disposition des autres utilisatrices et utilisateurs.
- 9.3. La confidentialité des informations dépend en grande partie du degré de protection dont les utilisatrices elles-mêmes ou utilisateurs eux-mêmes entourent leur identifiant et mot de passe. Elle et il leur appartient de veiller à la sécurité numérique et aux risques d'intrusion frauduleuse (comme les dommages causés par les programmes du Cheval de Troie ou par des virus). Conformément à l'article 7.3 de la présente politique, il incombe à l'utilisatrice ou utilisateur de ne jamais révéler son mot de passe.

- 9.4. Il est interdit de parcourir les écrans des autres, de récupérer les fichiers que d'autres utilisatrices ou utilisateurs ont jetés à la poubelle, de voler de l'information sur support papier, ou d'accomplir tout autre acte de ce genre.
- 9.5. Toute violation de la confidentialité, réelle ou soupçonnée, doit être signalée à la direction de stratégie numérique ou à l'administratrice ou administrateur du système concerné, à défaut de quoi cette omission pourra être interprétée comme un consentement tacite.
- 9.6. La confidentialité doit être respectée même après l'expiration de l'identifiant.
- 9.7. Les utilisatrices et utilisateurs doivent être informés que divers systèmes numériques rendent certaines informations accessibles à d'autres. Le contenu des fichiers individuels n'est jamais du domaine public par défaut, mais certains éléments comme la dernière commande exécutée, l'heure d'entrée dans le système et le nom de l'utilisatrice et de l'utilisateur sont souvent disponibles à d'autres utilisatrices et utilisateurs.
- 9.8. Le contenu du message électronique est protégé par le principe de la confidentialité de l'information, mais les utilisatrices doivent être conscientes et les utilisateurs doivent être conscients qu'en cours de livraison, elle et il passe souvent par des systèmes numériques qui ne sont pas forcément liés par la présente politique. Il ne faut alors pas transmettre de documents de nature confidentielle par courriel sans prendre des précautions nécessaires pour protéger leur confidentialité.
- 9.9. Afin de préserver l'intégrité des systèmes numériques contre les incidents, les pannes ou les fraudes, l'Université se réserve le droit d'inspecter, de copier, de retirer ou de modifier des données, des fichiers ou des ressources des systèmes relevant des installations numériques. En particulier, les représentantes désignées et les représentants désignés du Service de la stratégie numérique ou les responsables désignées et désignés par leurs départements ou services, ont l'autorité de retirer tout matériel des installations qu'ils dirigent si elles ou ils jugent que ce matériel enfreint les politiques de l'Université ou les lois en vigueur ou est inapproprié par rapport à la vocation de l'installation. Elles et ils pourraient par exemple mettre en œuvre des méthodes automatiques de détection et de retrait de ce matériel, comme configurer les logiciels de messagerie électronique pour rejeter les polluriels (spam).

Toutefois, l'Université n'entreprend pas de vérifier systématiquement son parc numérique pour déceler ce genre de matériel, sachant qu'il a pu être placé par des gens de l'extérieur. Ainsi, elle décline toute responsabilité pour le matériel reçu par l'intermédiaire de listes d'envoi électronique, groupes de diffusions ou autres forums. Des transmissions valides risquent parfois d'être retirées par erreur à cause des mesures correctives automatiques. Dans ce cas, l'Université n'en sera pas tenue responsable.

10. Diffusion sur l'Internet

- 10.1. Les pages de médias sociaux de la page Web officielle sont celles qui représentent l'identité institutionnelle de l'Université. Elles donnent les renseignements généraux sur les volets politique, pédagogique et administratif de l'établissement, ainsi que sur le recrutement et la fidélisation de la population étudiante et du personnel.
- 10.2. Tous sites Web ou pages de médias sociaux lancées par un membre du personnel de l'Université en lien avec l'établissement doivent se conformer aux lignes de conduite édictées

par l'Université, par le biais de son Service des communications et du marketing, et s'assurer des mises à jour régulières des informations qui s'y retrouvent.

- 10.3. Les éditrices et éditeurs des pages officielles doivent veiller à leur révision et mise à jour régulières.
- 10.4. Au besoin, l'éditrice ou l'éditeur d'une page publiée à partir des systèmes numériques doit obtenir la permission voulue avant d'afficher des textes, des graphiques, des sons ou des films qui ne sont pas de sa création.

11. MODIFICATION ET RÉVISION

La présente politique doit faire l'objet d'une révision un (1) an après son entrée en vigueur, puis à tous les trois (3) ans. Toute modification à la présente politique nécessite l'approbation du Conseil de gouvernance de l'Université.