



---

DIRECTIVE SUR L'UTILISATION ACCEPTABLE DES ACTIFS INFORMATIONNELS

## Table des matières

Préambule .....	3
Définitions .....	3
1. Champ d'application.....	6
1.1 Personnes concernées.....	6
1.2 Actifs et services visés .....	6
1.3 Activités visées.....	6
2. Objectifs.....	6
3. Obligation des membres .....	6
3.1 Utilisation sécuritaire, légale et éthique des actifs informationnels.....	6
3.2 Protéger l'information et les renseignements personnels.....	7
3.3 Prévenir les accès non autorisés et les abus .....	8
3.4 Utilisation strictement interdite .....	8
4. Surveillance .....	10
5. Manquements à la Directive .....	10

## Préambule

La Directive sur l'utilisation acceptable des actifs informationnels (« **Directive** ») découle de la Politique de sécurité de l'information, du Cadre de gestion de la sécurité de l'information et du Cadre de gouvernance à l'égard de la protection des renseignements personnels. Elle établit les lignes directrices encadrant l'utilisation des actifs informationnels du Cégep de Sainte-Foy (« **Cégep** »). Cette utilisation est principalement destinée à des fins d'enseignement, d'apprentissage, de recherche, de gestion ou d'administration, en lien avec la mission éducative du Cégep et les services offerts à la collectivité.

Toutefois, une utilisation personnelle des actifs informationnels du Cégep, notamment du poste de travail ou du téléphone intelligent mis à la disposition d'un membre, est permise, à condition qu'elle demeure **raisonnable** et **responsable**, et conforme aux bonnes pratiques d'utilisation. Cette utilisation ne doit en aucun cas compromettre le fonctionnement, la sécurité ou l'intégrité des actifs informationnels, ni la confidentialité, ni la disponibilité ou l'intégrité des informations qui y sont conservées.

Ces actifs incluent, sans s'y limiter :

- L'information, les renseignements personnels et les données sensibles ;
- Les équipements informatiques, tels que les ordinateurs, réseaux, logiciels, systèmes, tablettes et téléphones intelligents ;
- Les services infonuagiques, tels que diverses solutions accessibles via Internet, tels que les plateformes, les applications, les environnements de virtualisation et bien d'autres ressources informatiques.

L'accès aux actifs informationnels du Cégep est réservé uniquement aux personnes autorisées dans le cadre de leurs prérogatives. L'utilisation des actifs informationnels ne constitue pas une autorisation automatique, mais doit respecter les limites des accès accordés.

Le Cégep est responsable de la protection des informations collectées dans le cadre de ses activités pédagogiques et administratives. Une utilisation inappropriée des actifs informationnels peut entraîner des interruptions de service, des atteintes à la vie privée et d'éventuelles conséquences juridiques.

## Définitions

**Actif informationnel** : Une information, une banque d'information, un système ou un support d'information, un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par le Cégep habituellement accessible ou utilisable avec un dispositif technologique (notamment : logiciel, progiciel, didacticiel, base de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale). Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

**Authentification** : Est une procédure permettant pour un système informatique de vérifier l'identité d'une personne ou d'un ordinateur et d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications).

**Base de données** : est une collection organisée d'informations structurées, généralement stockées électroniquement dans un système informatique.

**Cégep** : Collège d'enseignement général et professionnel de Sainte-Foy.

**Confidentialité** : Propriété que possède une information ou une donnée de n'être accessible qu'aux personnes ou entités désignées et autorisées.

**CSIO** : Chef de la sécurité de l'information organisationnelle.

**Disponibilité** : Propriété que possède une information ou une donnée d'être accessible en temps voulu et de la manière requise par une personne autorisée.

**Équipement informatique** : Les composants et les équipements réseaux, les serveurs informatiques, les postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information ; tout équipement de télécommunication (cellulaire, lecteur MP3, téléphone intelligent, etc.) ; les logiciels, les progiciels, les didacticiels, les documents ou les bases de données et de renseignements (textuelles, sonores ou visuelles) placées dans un équipement ou sur un média informatique ; le système de courrier électronique et le système de messagerie. Les équipements informatiques sont ceux qui appartiennent au Cégep et qui sont mis à la disposition du membre en fonction du besoin identifié.

**Équipement informatique personnel** : Les équipements informatiques qui appartiennent au membre, qu'ils soient ou non mis en lien avec les équipements informatiques du Cégep.

**Étudiant et étudiante** : Toute personne dûment inscrite au Cégep au secteur régulier ou à la formation continue à des cours crédités ou non crédités.

**Fraude** : Acte déloyal et intentionnel pour obtenir un avantage indu, matériel ou moral, souvent par des moyens illégaux ou déguisés.

**Intégrité** : Propriété des données ou informations qui ne subissent aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.

**L'infonuagique** : est un modèle d'accès au réseau habilitant, pratique et sur demande comprenant un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peut rapidement être activé et désactivé en réduisant au minimum les efforts de gestion ou les contacts avec le fournisseur de services.

**Membre**: Tous les utilisatrices et les utilisateurs d'actifs informationnels au Cégep, y compris les étudiants et les étudiantes, le personnel enseignant, le personnel administratif, les partenaires, les contractuels, les stagiaires, les bénévoles, ainsi que les collaboratrices et collaborateurs externes qui sont autorisés, dans l'exercice de leurs fonctions, à utiliser les actifs informationnels mis à leur disposition par le Cégep dans tout lieu où se déroule une activité du cégep, qu'elle soit en présence ou à distance.

**Méthode à double facteur (2FA) ou authentification multifacteur (AMF) :** Méthode de sécurité qui nécessite plusieurs formes de vérification pour accéder à un compte ou un système.

Elle combine généralement :

- Quelque chose que vous **connaissez** (Par exemple : mot de passe, code PIN).
- Quelque chose que vous **possédez** (clé de sécurité, application d'authentification).
- Quelque chose que vous **êtes** (empreinte digitale, reconnaissance faciale).

**Renseignement personnel:** Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent directement ou indirectement de l'identifier, tels que : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, la date de naissance, la photographie et les coordonnées bancaires. Les renseignements personnels sont confidentiels sauf dans les cas prévus à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Les renseignements personnels doivent être protégés, peu importe la nature de leur support, et quelle qu'en soit leur forme : écrite, graphique, sonore, visuelle, informatisée ou autre.

**RPV ou VPN en anglais:** Un RPV (réseau privé virtuel) ou VPN est une technologie qui permet d'établir une connexion sécurisée et chiffrée entre un appareil et un réseau distant via Internet, donnant accès aux ressources internes comme si l'utilisateur était physiquement sur place, tout en protégeant les données échangées contre l'interception, notamment sur des réseaux publics.

**Sécurité de l'information :** Ensemble de mesures mises en place pour assurer la protection des informations selon le niveau de confidentialité, d'intégrité et de disponibilité jugé nécessaire.

**Système informatique :** un système automatisé de stockage, de traitement et de récupération de données qui tire parti des outils informatiques et électroniques pour effectuer une série complexe de processus et d'opérations.

**Utilisation acceptable :** Actions que le membre peut effectuer avec les actifs informationnels du Cégep.

**Utilisation interdite :** Actions que le membre ne doit pas effectuer avec les actifs informationnels du Cégep.

**Utilisation personnelle :** Utilisation des actifs informationnels du Cégep à des fins autres que des fins d'enseignement, d'apprentissage, de recherche, de gestion ou d'administration, en lien avec la mission éducative du Cégep et les services offerts à la collectivité.

## 1. Champ d'application

### 1.1 Personnes concernées

La Directive s'applique aux (« **membres** ») autorisés à utiliser les actifs informationnels du Cégep dans le cadre de leurs fonctions, tels que définis, soient la communauté étudiante, le personnel enseignant et administratif, les partenaires, les contractuels, les stagiaires, les bénévoles ainsi que les collaboratrices et collaborateurs externes.

### 1.2 Actifs et services visés

Tous les actifs informationnels et services technologiques qui sont mis à la disposition des membres sont visés par la Directive.

### 1.3 Activités visées

Toutes les activités impliquant l'utilisation sous toute forme d'actifs informationnels mis à la disposition des membres par le Cégep sont visées par la Directive, que ces activités soient conduites dans tout lieu où se déroule une activité du cégep, qu'elle soit en présence ou à distance.

## 2. Objectifs

La Directive vise à :

- Assurer une utilisation sécuritaire, légale et éthique des actifs informationnels.
- Protéger l'information et les renseignements personnels du Cégep.
- Maintenir la disponibilité, l'intégrité et la confidentialité des actifs informationnels.
- Prévenir les accès non autorisés et les abus.

## 3. Obligation des membres

Les membres sont tenus d'utiliser les ressources informationnelles de manière responsable et raisonnable. Ils doivent respecter les règles de sécurité et de confidentialité, utiliser les outils technologiques conformément aux objectifs du Cégep et éviter toute action pouvant nuire aux systèmes, aux données ou à la réputation de l'établissement. Le respect de cette directive contribue à maintenir un environnement numérique sécuritaire, fiable et efficace pour tous.

Tous les actifs informationnels fournis et mis à la disposition des membres dans le cadre de leurs fonctions au Cégep demeurent la propriété exclusive du Cégep.

### 3.1 Utilisation sécuritaire, légale et éthique des actifs informationnels

Afin d'assurer une utilisation sécuritaire, légale et éthique des actifs informationnels, le membre doit, en tout temps :

- Connaître et se conformer à la Politique de sécurité de l'information, au Cadre de gestion de la sécurité de l'information, au Cadre de gouvernance à l'égard de la protection des

renseignements personnels, au Cadre d'utilisation des médias sociaux du Cégep et aux directives du Cégep, notamment celles relatives à la sécurité.

<https://www.csfoyc.ca/notre-cegep/politiques-et-reglements/>

- Utiliser les équipements informatiques du Cégep principalement à des fins d'enseignement, d'apprentissage, de recherche, de gestion ou d'administration, en lien avec la mission éducative du Cégep et les services offerts à la collectivité.
- Utiliser les services infonuagiques approuvés par le Cégep, tels que proposés dans l'offre de services de la DSTI, afin de partager, d'enregistrer et d'organiser l'information liée à l'ensemble des activités pédagogiques et administratives du Cégep.<sup>1</sup>
- Utiliser les actifs informationnels de manière éthique et professionnelle, en respectant autrui et en s'abstenant de tout comportement nuisible, discriminatoire, intimidant ou offensant.
- Obtenir l'autorisation de la DSTI pour tout usage d'équipements informatiques appartenant au Cégep (ordinateur portable, tablette, cellulaire ou autre) à l'extérieur du Canada.
- Accéder uniquement aux informations et aux données nécessaires à l'exercice de ses fonctions.
- Respecter les lois sur le droit d'auteur et s'abstenir d'utiliser, de reproduire ou de distribuer du contenu protégé sans autorisation (Documents, logiciels, etc.).
- Participer activement aux activités de formation et de sensibilisation obligatoires ou non concernant l'adoption d'un comportement numérique responsable et sécuritaire.
- Informer immédiatement la DSTI de tout courriel suspect ou tentative d'hameçonnage.
- Signaler par le portail de services ou en se présentant au comptoir (C-135) toute situation susceptible d'affecter la sécurité des actifs informationnels, ou la protection des renseignements personnels, dont il est victime ou témoin.

### **3.2 Protéger l'information et les renseignements personnels**

Afin de protéger l'information, la confidentialité des données et des renseignements personnels et de maintenir la disponibilité et l'intégrité des données, le membre doit :

- Lire, comprendre et signer un « engagement de confidentialité, de protection des renseignements personnels et d'utilisation acceptable des actifs informationnels » à l'embauche et à toute autre étape qui le requiert au cours de son emploi au Cégep. Ces obligations et la discrétion attendue perdurent au-delà du lien d'emploi.
- Respecter la confidentialité et l'intégrité des informations auxquelles il a accès en tout temps et en toute circonstance.

---

<sup>1</sup> Voir également à cet effet la Directive sur les évaluations des facteurs relatifs à la vie privée.

- S'assurer qu'un logiciel antivirus est installé sur ses équipements informatiques personnels lorsqu'ils sont utilisés au Cégep.
- Assurer une surveillance constante de ses équipements informatiques (personnels et professionnels) surtout dans les espaces publics ou partagés.
- Signaler sans délai à la Personne responsable de l'accès à l'information et de la protection des renseignements personnels ou au CSIO, toute perte, égarement ou disparition d'équipement informatique contenant des informations confidentielles du Cégep ou des renseignements personnels qu'il détient ou de tout événement qui menace la disponibilité, l'intégrité ou la confidentialité des données du Cégep.

### 3.3 Prévenir les accès non autorisés et les abus

En plus des obligations énumérées dans les précédentes sections, le membre doit agir afin de prévenir les accès non autorisés aux données du Cégep, ainsi que les abus. Pour ce faire, le membre doit :

- Utiliser des mots de passe sécurisés conformément à la Directive sur la gestion des mots de passe du Cégep et ne jamais les partager, que ce soit avec des collègues, des tiers ou même des membres de sa famille. De plus, il est recommandé de ne pas réutiliser le même mot de passe, ou une variante, pour plusieurs comptes professionnels ou personnels.
- S'assurer que la création, la collecte, le stockage, le traitement, la transmission et la destruction des données personnelles sont effectués conformément aux lois et aux normes institutionnelles en vigueur.
- Modifier son mot de passe lorsque requis ou lorsqu'il juge que la confidentialité du mot de passe est ou pourrait avoir été compromise, le modifier sans délai et en aviser la DSTI.
- Lorsque requis, s'identifier en utilisant des méthodes à double facteur (2FA) ou d'authentification multifacteur (AMF).
- Verrouiller sa session lorsqu'il s'absente de son poste pour éviter tout accès non autorisé à son environnement de travail.

### 3.4 Utilisation strictement interdite

Il est strictement interdit à tout membre du Cégep de :

- D'utiliser les réseaux **Wi-Fi publics et non sécurisés** pour accéder à des informations **sensibles** du Cégep, en raison des risques élevés d'interception des données, d'usurpation d'identité et d'accès non autorisé aux systèmes. L'utilisation d'un réseau Wi-Fi public est acceptable pour des données **non sensibles**. Toutefois, assurez-vous d'utiliser un navigateur (Edge, Chrome, Safari, etc) à jour et de consulter uniquement des sites sécurisés (HTTPS).

- Utiliser les adresses courriel professionnelles (notamment : **@csfoy.ca** et **@cegep-ste-foy.qc.ca**) pour créer des **comptes personnels** sur des plateformes web, réseaux sociaux ou pour toute autre activité non liée aux fonctions exercées au Cégep.
- Partager ou divulguer avec quiconque ses mots de passe, ses questions et réponses secrètes si applicables ou tout autre moyen rendu disponible pour accéder aux actifs informationnels du Cégep.
- D'utiliser ou de tenter d'utiliser de façon malveillante des équipements informatiques, notamment pour la réalisation ou la tentative de réalisation: d'un plagiat, d'une tricherie, d'une fraude ou d'une cyberattaque. La participation à de tels actes est illégale.
- D'utiliser les espaces de sauvegarde infonuagique fournis par le Cégep (tels que OneDrive ou SharePoint) à des fins personnelles, notamment pour la sauvegarde de photos ou de documents personnels.
- Copier, enregistrer, télécharger ou reproduire sur des équipements non gérés (incluant les équipements personnels) par le Cégep des informations sensibles, incluant des renseignements personnels.
- Partager les données ou des informations sensibles du Cégep à des tiers, incluant des renseignements personnels sans les consentements requis ou l'autorisation de la Personne responsable de l'accès à l'information et de la protection des renseignements personnels.
- Tenter d'accéder à des informations, fichiers, bases de données, systèmes ou réseaux internes ou externes sans détenir les autorisations requises ou lorsque cet accès dépasse son rôle ou ses responsabilités.
- Modifier ou détruire sciemment des mesures de sécurité mise en place par le Cégep, un logiciel, une base de données ou un fichier numérique.
- Modifier ou remplacer le système d'exploitation des équipements informatiques appartenant au Cégep sans l'autorisation préalable de la DSTI.
- Entraver le fonctionnement des outils de sécurité tels que les antivirus, les sauvegardes de données, les écrans de veille, les outils de contrôle d'accès ou autre.
- Tenter de déchiffrer ou de découvrir un code d'accès ou un mot de passe, sans les autorisations appropriées de la DSTI.
- Installer des logiciels non autorisés ou piratés sur les équipements informatiques appartenant au Cégep sans l'autorisation de la DSTI.
- Utiliser les actifs informationnels ou les technologies de l'information du Cégep pour réaliser, notamment, les actions suivantes, **sauf autorisation préalable**:
  - o participer à une chaîne de lettres;
  - o effectuer de la publicité à des fins non autorisées;
  - o participer à des activités commerciales;
  - o faire de la vente pyramidale;

- le minage de monnaie électronique;
  - faire des envois massifs non autorisés;
- Utiliser les actifs informationnels du Cégep pour des activités illégales, commerciales ou personnelles non autorisées, telles que :
- Capturer, stocker, reproduire ou transmettre au moyen des équipements informatiques du Cégep un document ou un message à caractère obscène ou pornographique;
  - Transmettre des messages ou de réaliser des actions d'harcèlement, à caractères haineux, de violence ou de menaces.

#### **4. Surveillance**

Le Cégep applique des mesures de sécurité d'accès basées sur le principe du moindre privilège et selon le niveau de sensibilité des informations. Il limite ainsi l'accès uniquement aux personnes dont les fonctions l'exigent.

Eu égard à la vie privée des personnes, le Cégep se réserve le droit de faire des vérifications sur les actifs informationnels qu'elle administre et sur leur utilisation afin d'en assurer leur protection et leur bon fonctionnement tout au long de leur cycle de vie et de façon à ne pas compromettre ses activités. Le Cégep peut ainsi retirer à toute personne le droit d'utilisation d'actifs informationnels du Cégep ou l'utilisation d'équipements informatiques personnels pour accéder à des actifs informationnels du Cégep.

En présence d'un incident de sécurité ou de confidentialité, le Cégep prend en charge la restauration du poste de travail à sa configuration d'origine afin de le remettre en état de fonctionnement normal.

#### **5. Manquements à la Directive**

Toute personne qui contrevient à la *Directive*, ainsi qu'aux mesures de sécurité de l'information et de protection des renseignements personnels qui en découlent ou au cadre légal sur laquelle elle s'appuie, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi et des règles disciplinaires internes applicables.

La directive est approuvée par la régie de direction du 6 janvier 2026.