Directive sur l’accès à l’information et protection des renseignements personnels

En vertu du règlement ADM-118 *Accès à l’information et protection des renseignements personnels*

Pour protéger les informations personnelles, afin de respecter les droits à la vie privée des personnes et des organisations liées à l'Université Saint-Paul (ci-après « l'Université »), la présente directive établit des lignes directrices concernant l'accès et le partage des données personnelles.

1. Définition

Le terme « données personnelles », tel qu'il est utilisé ici, désigne généralement toute information non publique. Les données personnelles comprennent, sans s'y limiter, les informations d'identification personnelle, les dossiers médicaux et toute donnée marquée comme personnelle par l'organisation.

Exemples de données personnelles :

- **Informations sur le personnel et les étudiants**, telles que les adresses personnelles, les numéros de téléphone, les adresses électroniques, les noms d'utilisateur, les mots de passe, les numéros de permis de conduire, les informations financières, les informations fiscales, les informations médicales et les numéros d'assurance sociale.
- **Informations relatives à la gestion**, telles des documents concernant des questions relatives aux relations privées entre employeurs et employés ou à des mesures disciplinaires, des licenciements ou des mises à pied prévus, des enquêtes sur le lieu de travail concernant des fautes professionnelles et d'autres informations liées à l'emploi.

2. Collecte d’informations personnelles

- L’Université limite la collecte d'informations personnelles à celles qui sont nécessaires aux fins identifiées.
- L'Université est généralement tenue d'obtenir un consentement valable pour la collecte d'informations personnelles, sauf si une exception au consentement s'applique.
- L'Université ne doit généralement utiliser ou divulguer les informations personnelles qu'aux fins pour lesquelles elles ont été initialement collectées et ne les conserver que pendant la durée nécessaire à ces fins, sauf si l'Université a obtenu le consentement de la personne concernée pour agir autrement ou si elle est légalement autorisée à les utiliser ou à les divulguer à d'autres fins.

3. Contrôle d’accès

- L'accès aux données personnelles doit être accordé strictement en fonction du besoin de les connaître, déterminé par les responsabilités inerrantes à chacun des postes.
- Seul le personnel autorisé ayant des raisons valables est autorisé à accéder aux informations personnelles.
- Les droits d'accès doivent être régulièrement revus et mis à jour afin de refléter les changements dans les rôles ou le statut du personnel.

4. Protocoles de partage des données

- Le partage de données personnelles à l’externe ou à l’interne doit être évalué, justifié et limité au strict nécessaire.
- Tout partage de données doit être effectué via des canaux sécurisés, tels que des courriels cryptés ou des protocoles de transfert de fichiers sécurisés.
- Les destinataires de données personnelles sont tenus au secret professionnel.

5. Traitement et stockage des données

- Les données personnelles doivent être stockées de manière sécurisée, à l'aide d'un cryptage et de contrôles d'accès afin d'empêcher tout accès non autorisé.
- Les copies physiques des données personnelles doivent être conservées dans des armoires verrouillées ou des zones sécurisées.
- Les données ne doivent être consultées ou traitées que dans des environnements sécurisés afin d'éviter toute violation.

6. Exigences

Tout le personnel doit :

- Limiter l'accès aux informations personnelles.
- Être vigilant face aux escroqueries, tant en ligne qu'en personne.
- Conserver les informations personnelles sous clé et en lieu sûr.
- Être prudent lors de l'utilisation du Wi-Fi public, en particulier lors du travail à distance.
- Se défaire des informations personnelles de manière sécurisée.
- Ne laisser aucune information personnelle sur son bureau à la fin de la journée.
- Sécuriser les données physiques et numériques.
- Mettre régulièrement à jour les logiciels de son ordinateur et ses mots de passe.
- Utiliser des plateformes de communication cryptées et approuvées, telles que Microsoft Teams ou des messageries électroniques sécurisées.
- Être prudent lors de l'envoi de courriels à plusieurs destinataires et éviter de partager inutilement des adresses avec d'autres personnes. Il est recommandé dans ces cas-ci d'insérer les adresses dans le champ « Cci » plutôt que dans le champ « À ».

7. Réponse aux incidents

Toute violation présumée ou avérée de données personnelles doit être immédiatement signalée au secrétaire général. Des mesures appropriées seront prises pour atténuer les risques et empêcher que cela ne se reproduise. Toute fuite d’information personnelle faisant atteinte à la vie privée doit être déclarée au Commissaire à l’information et à la protection de la vie privée. De plus, les personnes concernées doivent aussi être avisées de la situation dès que possible après avoir établi que l’atteinte à la vie privée s’est produite.

8. Conformité et audit

Des audits réguliers seront effectués afin de garantir le respect de la présente directive. Tout manquement présentant un risque réel de préjudice grave à la vie privée pourrait faire l'objet de mesures disciplinaires conformément aux politiques de l'Université.

La présente directive vise à promouvoir une culture de confidentialité et de sécurité, en garantissant la protection des données personnelles contre tout accès non autorisé, toute divulgation, altération ou destruction, afin de préserver la confiance et l'intégrité au sein de l'organisation.