MUNICIPALITÉ DE
Saint-Ferréol
les-Neiges

POLITIQUE DE GESTION INTÉGRÉE DES DOCUMENTS ET DE SÉCURITÉ DE L'INFORMATION

Adopté le 11 août 2025

Résolution numéro 25-247

Table des matières

1. Préambule

Dans un monde organisé autour de l'information et dans lequel le numérique a pris une place prépondérante, la gestion, la conservation et l'élimination des documents – et de l'information qu'ils contiennent – constituent des enjeux majeurs. La gestion intégrée des documents et la gestion de la sécurité des systèmes d'informations sont des activités quotidiennes essentielles pour tous les organismes publics, incluant les municipalités, les centres de services scolaires et les centres de santé, soumis à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « **Loi sur l'accès** » ou « **LAI** »), car elle leur assure la capacité de remplir leurs mandats, d'atteindre leurs objectifs et d'offrir des produits et services à leur clientèle et à leur personnel.

À la lumière des normes gouvernementales établies dans le secteur public, les documents et les données d'un organisme doivent être gérés de manière à pouvoir être utilisés pour rencontrer les exigences en matière de protection des renseignements personnels et de preuve. Leur gestion doit assurer que leur confidentialité, leur authenticité, leur fiabilité, leur intégrité, leur utilité et leur disponibilité soient protégés tout au long de leur cycle de vie. Lorsqu'il est question de documents et d'information, il est essentiel de comprendre que ce concept englobe aussi les banques de données.

Par la présente politique, la Municipalité de Saint-Ferréol-les-Neiges (ci-après la « **Municipalité** ») établit ses orientations en matière de gestion intégrée des documents et de gestion de la sécurité des systèmes d'informations. Elle y énonce ses objectifs, y définit les champs d'application et le cadre normatif, ainsi que les rôles et les obligations des divers intervenants en plus d'y réaffirmer que les documents produits et reçus par ses unités représentent un actif informationnel riche et essentiel à la réalisation de sa mission ainsi qu'à la constitution de sa mémoire institutionnelle. Elle convient que ces derniers doivent absolument être sécurisés afin d'assurer la continuité des affaires de la Municipalité au fil du temps et le respect de ses obligations légales, financières et fiscales.

2. Objectifs et champ d'application

Ce document s'applique à tous les types d'informations, quelle qu'en soit la forme – documents sur papier ou support électronique, applications et bases de données, etc., que les documents et les enregistrements aient été créés à l'intérieur de la Municipalité ou qu'ils soient d'origine externe.
Les procédures décrites au sein de la présente politique permettront de contrôler l'information utilisée dans le système de gestion documentaire et de sécurité de l'information, depuis sa création en passant par toute approbation, communication, utilisation et mises à jour de celle-ci, jusqu'à sa destruction.

Les documents et les enregistrements sont réputés appartenir à la Municipalité. C'est pourquoi toute personne quittant une fonction dans un service de la Municipalité doit remettre l'entièreté de ceux qui sont encore sous son contrôle à son supérieur immédiat ou au responsable de la gestion intégré des documents.

Les utilisateurs de ce document sont tous les employés de la Municipalité ainsi que les élus municipaux.

3. Définitions

Archives
Ensemble des documents, quelle que soit leur date ou leur nature, qui ne se qualifie plus de document actif ou semi-actif.

Calendrier de conservation
Outil de gestion qui détermine les périodes d'utilisation et les supports de conservation des documents actifs et semi-actifs d'un organisme ainsi que leurs supports de conservation. Le calendrier indique également quels documents inactifs sont conservés de manière permanente et lesquels sont détruits.

Cycle de vie
Ensemble des étapes que franchit un document depuis sa création ou son obtention, en passant par sa collecte ou sa création, son utilisation, sa consultation, sa communication jusqu'à sa conservation en archivage et sa destruction ou son anonymisation.

Document
Toute information consignée sur quelque support que ce soit est assimilée à un document. Toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite est également assimilée à un document.

Document actif
Document essentiel au soutien ou au maintien des activités quotidiennes d'un organisme qui peut contenir des renseignements personnels, ou non.

Document semi-actif
Document qui doit être conservé pour des raisons administratives, légales, financières ou probatoires, mais qui n'a pas à être utilisé fréquemment pour soutenir ou maintenir les activités quotidiennes d'une administration.

Document institutionnel
Document relatif à l'organisme qui peut contenir des informations confidentielles et/ou des renseignements personnels.

Document essentiel
Document indispensable au fonctionnement de l'organisme et qui assure la continuité de celui-ci à la suite d'un désastre et qui peut contenir des renseignements personnels. Il s'agit notamment de vos politiques et procédures en matière de reprise d'activités à la suite d'un incident de confidentialité.

Gestion intégrée des documents (GID)
Gestion intégrée de l'ensemble des documents et des dossiers, peu importe leur support et leur format, durant tout leur cycle de vie ; utilisation des mêmes méthodes et outils pour effectuer la gestion des documents sur support papier et des documents numériques.

Plan de classification
Document qui permet le classement et le repérage de tous les dossiers (et/ou renseignements) produits ou obtenus par les unités d'affaire et le repérage de ces derniers ainsi que l'identification des finalités associées au traitement de renseignements personnels.

4. Principes généraux

Pour assurer une gestion efficace, économique et sécuritaire des documents durant tout leur cycle de vie, la Municipalité a établi un système de gestion intégrée des documents et de sécurité de l'information. Ce système se compose principalement :

- de la présente politique, qui précise, entre autres, les responsabilités des intervenants ;
- d'un Plan de classification qui permet le classement et le repérage de tous les dossiers produits par les unités et le repérage des finalités associées au traitement de renseignements personnels ;
- d'un Calendrier de conservation qui établit la durée de conservation de l'ensemble des dossiers, des documents et des renseignements personnels, permettant ainsi de diminuer la masse de documents et de renseignements personnels à conserver grâce à la destruction à la fin de la période de rétention tout en préservant ceux qui ont une valeur administrative, légale ou fiscale;
- d'un ensemble de procédures et de processus qui spécifient les façons de faire et les actions à poser en matière de GID, notamment en ce qui concerne la numérisation des documents.

5. Règles et responsabilités relatives au contrôle des documents

Pour assurer l'application et le respect de la présente politique, la Municipalité met en place une structure et des mécanismes opérationnels, relatifs aux documents internes créés au sein de la Municipalité ou collectés de l'externe.

6. Approbation des documents

Tous les documents officiels, qu'il s'agisse de nouveaux documents ou de nouvelles versions de documents existants, doivent être approuvés par le supérieur immédiat de l'auteur du document.

7. Classement et archivage de documents

a. Classement et accès aux documents

L'accès aux documents, et plus précisément les documents qui contiennent des renseignements personnels, doit être limité aux employés pour qui il est nécessaire d'y accéder. Les droits d'accès sont accordés en fonction du poste occupé par l'employé selon son profil d'utilisateur. Tout droit d'accès supplémentaire peut être accordé par le supérieur immédiat de l'employé.

Il est fortement recommandé de conserver uniquement les versions les plus récentes des divers documents de la Municipalité. Le fait de conserver de multiples versions, certaines étant désuètes, augmente le risque d'envoi ou d'utilisation d'un document qui ne devrait plus servir les fins de la Municipalité.

b. Classement et accès aux courriels

L'accès aux courriels doit être limité aux employés qui sont les destinataires de ce courriel. Lorsqu'un membre du personnel doit avoir accès à de l'information transmise par un ou des courriels, une copie peut être envoyée à ce destinataire. Il revient à l'expéditeur de s'assurer que le destinataire a le droit de recevoir et d'accéder aux informations et renseignements personnels contenus dans ce courriel.

La classification des courriels doit être effectuée selon le dossier auquel il est lié et les renseignements personnels qui pourraient s'y trouver. Le partage d'un courriel dans un dossier public accessible à tous les membres de la Municipalité est déconseillé, puisque seules les personnes qui ont nécessairement besoin d'accès à ces courriels devraient pouvoir y accéder.

Il est cependant possible pour une équipe opérationnelle partageant des tâches communes ou complémentaires de placer ces courriels dans un dossier, répertoire ou plateforme dont l'accès est réservé à l'équipe.

c. Archivage des documents

Dès qu'un document ne rencontre plus les attributs de statut de **document actif ou semi-actif,** il doit être envoyé à l'archivage selon la procédure d'archivage des documents.

d. Mises à jour des documents

Toutes les modifications apportées aux documents doivent être effectuées à l'aide de « Suivre les modifications », en rendant visibles uniquement les révisions apportées à la version précédente.

Toute version d'un document officiel devrait avoir une description brève de la nature des modifications apportées au document. Cette description se trouve généralement à la première page ou au début du document.

e. Gestion des droits d'accès par profil d'usager

Les droits d'accès aux informations détenues par la Municipalité sont attribués conformément au profil d'usager détaillé dans une demande effectuée par le gestionnaire de l'employé tel que démontré à l'article 3 de la Politique de contrôle d'accès.

8. Règles et responsabilités relatives aux périodes de rétention et à la destruction des documents

La présente section de la politique décrit la façon d'établir les périodes de conservation requises pour des catégories spécifiées de documents et de renseignements personnels et précise les normes minimales à appliquer lors de la destruction de certaines informations détenues par la Municipalité.

Ces règles et responsabilités s'appliquent à tous les services ou directions, processus et systèmes d'information dans toutes les provinces, états ou pays dans lesquels la Municipalité exerce des activités ou a des relations d'affaires avec des tiers.

Ces règles et responsabilités s'appliquent à tous les dirigeants, administrateurs, employés, agents, sociétés affiliées, sous-traitants, consultants, conseillers ou fournisseurs de services de la Municipalité qui peuvent collecter, utiliser, traiter, communiquer ou avoir accès à des données (y compris des renseignements personnels et/ou des renseignements personnels sensibles). **Il est de la responsabilité de tous de se familiariser avec la présente Politique et d'assurer un respect adéquat de celle-ci.**

Cette politique s'applique à toutes les informations détenues par la Municipalité. Voici des exemples de supports documentaires de ces informations :

- Courriels ;
- Documents papier ;
- Documents électroniques ;
- Documents vidéo et audio ;
- Données générées par les systèmes de contrôle d'accès physique.

9. Principe général de conservation

Pour toute catégorie de documents non spécifiquement définis dans la Calendrier de conservation et sauf disposition contraire d'une loi ou d'un règlement applicable, la période de conservation de tout document sera réputée être de 7 ans à compter de la date de fin d'utilisation du document.

10. Délai de rétention au calendrier de conservation

Le responsable de la protection des renseignements personnels et de l'accès aux documents (« **Responsable de la PRP et de l'accès** »), en collaboration avec la personne responsable de la GID, définit la période pendant laquelle les documents, incluant les enregistrements électroniques, doivent être conservés en mode semi-actifs ou inactifs. Ce délai est inscrit au Calendrier de conservation.

Exceptionnellement, les périodes de rétention peuvent être prolongées pour des situations particulières telles que :

- Enquêtes en cours par une autorité d'une province, d'un état ou d'un pays autre que le Québec et/ou le Canada dont une loi sur la protection des renseignements personnels s'applique à la Municipalité, s'il semble nécessaire de conserver des renseignements personnels pour démontrer la conformité de la Municipalité à toute exigence légale ; ou
- Lors de l'exercice de droits légaux dans des procédures judiciaires intentées en vertu de la législation provinciale ou fédérale.

11. Protection des données pendant la période de conservation

La possibilité que les supports de données utilisés pour l'archivage s'usent ou deviennent désuets doit être envisagée. Si des supports de stockage électroniques sont choisis, toutes les procédures et tous les systèmes garantissant l'accès aux informations pendant la période de conservation (tant en ce qui concerne le support d'information que la lisibilité des formats) doivent également être stockés afin de protéger les informations contre la perte résultant de changements technologiques futurs. La responsabilité de l'entreposage incombe à la personne responsable du comité de gestion de risques de la Municipalité en collaboration avec le Responsable de la PRP et de l'accès et la personne responsable de la GID, le cas échéant.

12. Destruction des données

La Municipalité doit donc, sur une base annuelle, examiner toutes les données et documents, qu'ils soient conservés électroniquement ou sur papier, pour décider de les transférer aux archives lorsque les documents ou les données ne se qualifient plus de documents actifs ou semi-actifs. La responsabilité globale de la destruction des données et des documents transmis aux archives incombe au responsable de la gestion intégrée documentaire ou au Responsable de la PRP et de l'accès, le cas échéant.

La destruction des données et des documents, doit être assurée par tout mode garantissant leur suppression définitive, déchiquetés ou autrement détruits de façon appropriée et sécuritaire. La méthode de destruction peut varier et dépend de la nature et de la confidentialité du document. (Par exemple, tous les renseignements personnels sensibles doivent être détruits en tant que déchets confidentiels et faire l'objet d'une suppression électronique définitive et sécurisée ; certains documents désuets, expirés ou remplacés peuvent ne justifier qu'un déchiquetage interne. La section « Procédure de destruction de routine » des documents ci-dessous définit le mode de destruction.)

Dans ce contexte, l'employé doit exécuter les tâches et assumer les responsabilités pertinentes pour la destruction de l'information. Le processus spécifique de destruction peut être effectué soit par un employé, soit par un prestataire de services interne ou externe que le responsable de la gestion documentaire ou le Responsable de la PRP et de l'accès, le cas échéant, sous-traite à cette fin. Toutes les dispositions générales applicables en vertu des lois pertinentes sur la vie privée et de la politique de protection des renseignements personnels de la Municipalité doivent être respectées.

Des contrôles appropriés doivent être en place pour prévenir la perte permanente d'informations essentielles de la Municipalité à la suite de la destruction malveillante ou involontaire d'informations.

La personne responsable de la GID ou le Responsable de la PRP et de l'accès, le cas échéant, doit documenter et approuver intégralement le processus de destruction. Les exigences légales applicables en matière de destruction d'informations, en particulier les exigences des lois applicables en matière de protection des données, doivent être pleinement respectées.

13. Procédure de destruction de routine

Les documents qui peuvent être systématiquement détruits à moins de faire l'objet d'une enquête judiciaire ou réglementaire en cours ou qui se qualifient de documents actifs ou semi-actifs sont notamment les suivants :

- Annonces et avis de réunions quotidiennes et d'autres événements, y compris les acceptations et les discours ;
- Réservations pour des réunions internes sans frais et coûts externes;
- Documents de transmission tels que lettres, feuilles de couverture de fax, courriels qui ne nécessitent aucun classement conformément à la présente politique, bordereaux d'acheminement et articles similaires qui accompagnent les documents mais n'ajoutent aucune valeur;
- Bordereaux de message;
- Liste d'adresses remplacée, listes de distribution, etc.;
- Documents dupliqués tels que des copies CC et FYI, des brouillons non modifiés, des impressions instantanées ou des extraits de bases de données et de fichiers journaliers;
- Publications internes qui sont obsolètes ou remplacées;
- Magazines spécialisés, catalogues de fournisseurs, dépliants et bulletins d'information de fournisseurs ou d'autres organisations externes.

14. Méthode de destruction

Les documents de **niveau I** sont ceux qui contiennent des informations ayant le plus haut niveau de sécurité et de confidentialité et ceux qui contiennent des renseignements personnels. Ces documents sont détruits en tant que déchets confidentiels (déchiquetés) et font l'objet d'une suppression électronique définitive et sécurisée. On peut également choisir de procéder à l'anonymisation mais il faudra alors que la Municipalité s'assure qu'elle équivaut bien à la destruction de façon irréversible et que l'information ne peut en aucun cas et à tout jamais être recréée. Une preuve de destruction doit être fournie.

Les documents de **niveau II** sont des documents exclusifs qui contiennent des informations confidentielles telles que les noms, signatures et adresses des parties, ou qui pourraient être utilisées par des tiers pour commettre une fraude, mais qui ne contiennent aucun renseignement personnel sensible. Les documents doivent être déchiquetés, puis placés dans des poubelles verrouillées pour être collectés par une entreprise de destruction agréée, et les documents électroniques feront l'objet d'une suppression électronique définitive et sécurisée. Une preuve de destruction doit être fournie.

Les documents de **niveau III** sont ceux qui ne contiennent aucune information confidentielle ou renseignement personnel et qui sont des documents publiés par la Municipalité. Ceux-ci doivent être recyclés par une entreprise de recyclage ou être recyclés par la Municipalité et comprennent, entre autres, des publicités, des catalogues, des dépliants et des bulletins d'information. Ceux-ci peuvent être détruits sans piste d'audit.

15. Violation, application et conformité

Le Responsable de la PRP et de l'accès à la responsabilité de s'assurer que chacun des bureaux de la Municipalité se conforme à la présente politique. Il est également de sa responsabilité d'aider tout bureau local à répondre aux demandes de renseignements des autorités gouvernementales de protection des informations quant aux politiques et procédures en place.

Tout soupçon de violation de la présente politique doit être signalé immédiatement au Responsable de la PRP et de l'accès. Tous les cas de violation présumée de la politique doivent faire l'objet d'une enquête et le Responsable de la PRP et de l'accès doit prendre les mesures appropriées pour y remédier.

Le non-respect de la présente Politique peut entraîner des conséquences négatives, y compris, mais sans s'y limiter, la perte de confiance des citoyens ou des clients, des litiges, la perte d'avantage concurrentiel, des pertes financières et des dommages à la réputation de la Municipalité, les préjudices ou les pertes.

Le non-respect de la présente politique par des employés permanents, temporaires ou contractuels ou par des tiers tenus de la respecter, qui ont obtenu l'accès aux locaux ou aux informations de la Municipalité, peut entraîner des procédures disciplinaires ou la résiliation de leur emploi ou de leur contrat. Des poursuites judiciaires peuvent également être intentées contre les parties impliquées dans de telles activités.

16. Validité et gestion des documents

Ce document est valide à partir du 12 août 2025.

Le propriétaire de ce document est la municipalité de Saint-Ferréol-les-Neiges, et son Responsable de la protection des renseignements confidentiels doit vérifier et, si nécessaire, mettre à jour le document au moins une fois par an à moins qu'une situation particulière justifie la révision de façon plus rapide.

_____

Mélanie Royer-Couture, mairesse

_____

Eric Ennis, directeur général et trésorier