



POLITIQUE SUR L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DES COMMUNICATIONS 2025-2026

1. Objectifs

La présente politique établit un cadre d'utilisation des TIC pour tous les utilisateurs. Elle vise :

1. à promouvoir les objectifs pédagogiques dans l'utilisation des TIC;
2. à promouvoir une utilisation responsable des TIC, dans le respect de la légalité;
3. à assurer la protection des renseignements confidentiels ou à caractère personnel;
4. à prévenir les risques de destruction ou de modification des systèmes et des données;
5. à protéger le parc informatique du Collège et les appareils de ses utilisateurs.

2. Champs d'application de la politique

La présente politique s'applique à tous les élèves du Collège Reine-Marie.

Cette politique s'applique à l'utilisation de l'ensemble des TIC appartenant au Collège Reine-Marie, peu importe leur localisation, ou ne lui appartenant pas, mais utilisées dans ses locaux, ou reliées de quelque façon à son réseau informatique.

3. Principes d'utilisation des TIC

Les TIC sont mises à la disposition des utilisateurs pour la réalisation d'activités d'enseignement, d'apprentissage et de services à la collectivité reliés à la réalisation de la mission du Collège durant leurs heures de travail.

Dans un contexte de partage équitable des ressources, l'utilisateur doit faire un usage raisonnable des TIC du Collège Reine-Marie et éviter de les monopoliser ou d'en abuser.

L'utilisateur élève doit se soumettre aux limites d'usage imposées par son enseignant(e), et ce, même si son appareil n'est pas contrôlé par un logiciel de surveillance.

3.1 Utilisation

Le Collège Reine-Marie rend disponible un *espace disque sur Google Disque* pour chaque élève ainsi qu'une adresse courriel lié au domaine @educrm.ca et un compte sur le Pluriportail.

L'utilisateur doit notamment :

1. éviter le téléchargement et le stockage de données personnelles de façon abusive;

2. utiliser l'équipement de manière à ne pas nuire à la performance **ou** au travail des autres élèves ou du personnel du collège;
3. utiliser l'équipement aux moments permis;
4. utiliser l'équipement de façon responsable;
5. utiliser l'équipement de manière à ne pas nuire au fonctionnement optimal des TIC, ni générer de coûts supplémentaires.

3.2 Comportements interdits

Les comportements interdits énumérés dans cette politique précisent les gestes qui contreviennent à l'éthique exigée par le Collège Reine-Marie dans l'utilisation des TIC. L'énumération qui suit ne doit pas être considérée comme exhaustive.

Il est interdit à l'utilisateur :

1. de partager ses identifiants ou de connecter un appareil ne lui appartenant pas, au réseau du collège (ex. connecter le cellulaire d'un ami, avec ses propres identifiants, au réseau sans-fil);
2. d'utiliser des logiciels autres que ceux fournis et installés par le Collège Reine-Marie. Tout nouveau logiciel qu'on souhaite installer devra être préalablement approuvé par un membre du département des technologies de l'information du Collège;
3. de publier des photos, vidéos ou enregistrements sonores de d'autres élèves ou de membres du personnel d'une quelconque façon (ex. Internet, YouTube, Facebook, Instagram, TikTok, Twitter, Snapchat, messages textes, journaux, médias, etc .) sans l'autorisation de toutes les personnes concernées;
4. d'accéder, de télécharger, de stocker, d'imprimer et des propos ou des images de nature haineuse, diffamatoire, violente, offensante, désobligeante, perturbante, harcelante, illégale, à caractère sexuelle, pornographique, raciste, sexiste ou incompatible avec la Charte des droits ou la mission éducative ou les normes administratives établies par le Collège Reine-Marie;
5. de faire circuler d'une quelconque façon (ex. Internet, YouTube, Facebook, Instagram, Twitter, Snapchat, messages textes, journaux, médias, etc .) des propos, images, photos, vidéos, informations malicieuses concernant la vie privée des personnes ou des propos de nature à compromettre leur réputation;
6. d'utiliser les TIC à des fins politiques, de propagande, de harcèlement ou de menace sous quelque forme que ce soit, ou pour jouer un tour à des tiers;
7. de participer à des jeux d'argent et de paris, de quelque nature que ce soit;
8. d'associer des propos personnels avec ou au nom du Collège Reine-Marie dans des groupes de discussions, des séances de clavardage, ou d'utiliser tout autre mode d'échange d'opinions de manière à laisser croire que les opinions qui y sont exprimées sont endossées par le Collège Reine-Marie;
9. de créer des liens de communication, d'installer des serveurs ou des services, ou de modifier le réseau du Collège Reine-Marie;
10. d'accéder ou de tenter d'accéder à des systèmes informatiques ou de communication autres que ceux autorisés;

11. d'introduire des virus, contourner les règles de filtrage et de sécurité mises en place ou de tenter de pénétrer les systèmes du Collège Reine-Marie;
12. d'utiliser un logiciel/application de type VPN (Virtual Private Network) sur le réseau du collège, ou lors de l'enseignement à distance durant les heures de cours (8h à 17h);
13. de télécharger, de transmettre ou de distribuer toute information et tout document confidentiel;
14. d'utiliser un ou des subterfuges ou d'autres moyens pour transmettre un message électronique de façon anonyme ou en utilisant le nom d'une autre personne;
15. de télécharger, de transmettre ou de distribuer, sans autorisation, à tout le personnel ou à des groupes de membres du personnel des chaînes de lettres;
16. d'envoyer du courrier non ciblé.

3.3 Droit d'un utilisateur à la confidentialité

Les utilisateurs doivent savoir que le Collège Reine-Marie peut avoir accès aux communications ou transactions faites au moyen de ses TIC et que, par conséquent, toute utilisation à des fins personnelles ne peut être considérée comme entièrement privée.

Puisque les TIC sont mis à la disposition des utilisateurs pour contribuer à la réalisation de la mission du Collège Reine-Marie, les utilisateurs doivent présumer que toute utilisation, qu'elle soit personnelle ou non, est enregistrée et conservée sous forme de copie de sécurité.

De plus, le Collège Reine-Marie se réserve le droit de faire enquête lorsqu'il constate que l'équipement est utilisé en contravention du présent code. Les membres du département des services informatiques pourront accéder aux données de tout utilisateur dans le cadre de cette enquête. Les membres du département des services informatiques, la direction de niveau associé, le/la technicien.ne en éducation spécialisé, la direction pédagogique et la direction générale, auront accès à l'information recueillie lors de cette enquête et les recherches seront faites avec respect et de la façon la moins intrusive possible.

3.4 Droit d'auteur et de propriété intellectuelle

En tout temps, l'utilisateur doit respecter le droit d'auteur et les autres droits de propriété intellectuelle des tiers. Les documents électroniques et les logiciels sont couverts par la *Loi sur le droit d'auteur* (L.R.C., c. C-42).

Il existe une grande variété de types de droits d'utilisation et de reproduction de documents et de logiciels. Dans tous les cas, il faut se référer à la licence d'utilisation correspondante.

4. Rôles et responsabilités

4.1. Responsabilités des membres du personnel du collège

Tous les membres du personnel du collège doivent s'assurer du respect de la présente politique dans les différents services ainsi que son application. Ils doivent en informer le département d'informatique et la direction de niveau associé à l'élève de tout manquement à cette politique

4.2. Rôles du département de l'informatique

Le département de l'informatique doit informer le coordonnateur dans les plus brefs délais, de toute dérogation au code d'éthique en identifiant le ou les fautifs ainsi que la nature de l'infraction.

4.3 Responsabilités des utilisateurs

L'utilisateur est responsable d'utiliser avec soin et discernement les appareils qui lui sont prêtés.

Les utilisateurs des TIC doivent assumer la responsabilité de la sécurité, de l'intégrité et de l'intégralité de l'information et des traitements effectués sur les équipements qu'ils utilisent.

Ils doivent protéger la confidentialité des renseignements qu'ils peuvent détenir et en protéger l'accès par un mot de passe.

Ils doivent protéger la confidentialité de leurs mots de passe et s'assurer de fermer/verrouiller la session durant leur absence. Un utilisateur peut être tenu responsable des actes commis par une autre personne qui utilise son code utilisateur et son mot de passe.

Toute anomalie, qu'elle provienne du réseau, des logiciels ou de l'équipement, doit être déclarée au département des technologies de l'information.

5. Infraction au code d'éthique sur l'utilisation des TIC

Tout contrevenant à la présente politique et aux modalités d'application s'expose à la révocation de ses privilèges et à l'imposition de mesures disciplinaires.

Annexe A. Procédure relative aux mots de passe

1. Avantages d'une procédure relative aux mots de passe

- Accès approprié pour tous les usager;
- Gestion de l'identité et vérification de l'accès efficace;
- Conservation et protection des informations personnelles qui sont partagées;

2. Paramètres du choix du mots de passe

Application : sur toutes les plateformes

Il doit contenir :

- Entre 10 et 25 caractères
- Au moins une (1) majuscule
- Au moins un (1) chiffre
- Au moins un (1) caractère spécial (@ # \$! % etc.)

Il ne doit pas doit contenir en tout ou en partie les éléments suivants :

- Votre numéro de fiche (ex. 2909999)
- Votre nom ou prénom
- Votre date de naissance

Les points suivants offrent des conseils sur les meilleures pratiques pour la création d'un mot de passe :

- Les mots de passe ne doivent pas contenir des informations personnelles, telles que le nom ou le numéro de la rue, le nom du collège, la date de naissance, etc;
- Les mots de passe ne doivent jamais contenir de noms des membres de la famille, des animaux de compagnie, des amies et amis;
- Les mots de passe ne doivent pas être une phrase commune suivie d'un chiffre qui change lorsque le mot de passe expire.

3. Changement de mot de passe

Le mot de passe d'un étudiant doit être changé au moins 1 fois par année à la rentrée scolaire.

Le mot de passe peut être changé qu'au collège via l'adresse suivante :

4. Principes d'une utilisation sécuritaire d'un mot de passe

1. Ne partage pas ton mot de passe avec quiconque.
2. N'utilise jamais le même mot de passe que celui que tu utilises pour d'autres comptes personnels (courriel, site de jeux, comptes bancaires, etc.)
3. N'écris pas les mots de passe et ne les envoie pas dans un courriel ou un texto (SMS).
4. Ne sauvegarde pas les mots de passe électroniquement, à moins qu'ils ne soient cryptés par un logiciel gestionnaire de mots de passe.