

AVIS SUR LA POLITIQUE CONCERNANT LE CODE DE DÉONTOLOGIE ET D'ÉTHIQUE RELATIF À L'UTILISATION DES TECHNOLOGIES À LA CSDM

Avis présenté à la
Commission scolaire de Montréal

par l'Alliance des professeures et professeurs de Montréal

20 janvier 2014



Lors de la rencontre du Comité des relations de travail du 1^{er} novembre 2013, la Commission scolaire de Montréal a déposé, pour consultation, le projet de Politique concernant le code de déontologie et d'éthique relatif à l'utilisation des technologies à la CSDM (la Politique) ainsi que les Modalités d'application qui s'y rattachent.

Tel que mentionné dans le préambule du projet de la Politique, celle-ci « remplace et complète le *Code d'éthique sur l'utilisation des technologies de l'information et des communications et des équipements informatiques de la CSDM* » en vigueur depuis septembre 2001.

L'Alliance reconnaît la nécessité pour la CSDM d'avoir une Politique relative à l'utilisation des outils technologiques mis à la disposition des enseignantes et des enseignants.

Cependant, des éléments de ce projet de Politique nous questionnent et nous interpellent. Nous avons choisi de les regrouper par sujets afin de faciliter notre présentation.

1- Adhésion à la politique

La lecture des modalités d'application de la Politique mentionne que « tout gestionnaire est responsable de faire en sorte que, pour tous les utilisateurs sous sa responsabilité, la Politique soit connue et bien comprise ». L'Alliance se questionne sur les moyens qui seront mis en œuvre pour qu'un gestionnaire puisse s'assurer de la connaissance et de la compréhension de la Politique. Il est vrai qu'en début d'année, il est possible, lors d'une réunion du personnel enseignant, de rappeler l'existence de la Politique. Mais qu'en est-il de l'enseignante ou de l'enseignant qui intègre l'école en cours d'année ou encore de la suppléante ou du suppléant qui ne sera présent à l'école que pour une courte durée – un remplacement de quelques semaines par exemple?

Dans un deuxième temps, le même document nous apprend que le Service de la gestion des personnes et du développement des compétences devra intégrer à son processus d'embauche et de recrutement « une communication claire qui concerne la Politique et les responsabilités qui en découlent pour l'employé ». Que signifie « une communication claire »? Est-ce que cela se limitera à l'insertion du texte de la Politique dans la pochette remise lors de la rencontre d'embauche – pochette qui contient déjà plusieurs documents? L'Alliance estime qu'une présentation explicite devrait être faite lors de ces rencontres.

De plus, l'Alliance ne peut être en accord avec le fait que « l'identification sur un outil technologique de la CSDM comporte implicitement l'adhésion de l'utilisateur à la Politique et l'engagement de ce dernier à en respecter l'esprit et la lettre (paragraphe 5.2 de la Politique). Il est mentionné dans cette même section que « la Commission scolaire pourra notamment demander à tout utilisateur de confirmer qu'il a pris connaissance de la Politique et qu'il s'engage à la respecter. » L'adhésion de l'utilisateur se doit d'être explicite et la Commission scolaire a l'obligation de s'en assurer.

2- Imputabilité

La Politique indique que « l'utilisateur est imputable de son utilisation des outils technologiques » (paragraphe 4.4).

L'Alliance considère que cette imputabilité va trop loin particulièrement en ce qui a trait aux responsabilités relatives à la sécurité informatique, aux communications par messagerie numérique et à l'utilisation des réseaux sociaux.

Il n'est pas du ressort de l'enseignante ou l'enseignant de s'assurer que l'outil technologique dont elle ou il dispose en classe soit prémuni contre les logiciels malveillants (5-7.2). De plus, une enseignante ou un enseignant ne peut être tenu responsable de la réception, par messagerie, d'un fichier non exempt de virus (5.9.4) ou dont le contenu est illicite ou inapproprié (5-3.6).

Certaines responsabilités auraient intérêt à être mieux définies. Qu'est-ce qu'une utilisation abusive des envois en copie conforme et en copie conforme invisible (5-9.5)? Qui détermine où commence l'abus?

Il en est de même quant aux responsabilités relatives à l'utilisation des réseaux sociaux (5.10). Tel que présenté, les responsabilités des utilisateurs ne sont pas clairement définies contrairement aux autres éléments. Le texte se contente de mentionner « que les attentes exprimées par la CSDM par voie de sa *Déclaration de principe sur le civisme et l'éthique* s'appliquent aux comportements des utilisateurs au sein de ces réseaux virtuels ». L'Alliance considère que la Politique devrait indiquer clairement la nature de ces attentes plutôt que de faire référence à un autre document qui n'est probablement pas remis aux enseignantes et enseignants.

L'Alliance se questionne également sur le niveau de responsabilité des enseignantes et enseignants en lien avec les élèves qui sont aussi des utilisateurs et en conséquence assujettis à la Politique. Qui aura la responsabilité de faire connaître la Politique aux élèves jeunes et adultes? Une des responsabilités du gestionnaire est de « s'assurer qu'une surveillance adéquate est exercée par l'ensemble du personnel [...] à l'endroit des élèves qui utilisent un outil technologique [...] » Les directions d'école devront préciser ce qu'est une surveillance adéquate. Les enseignantes et enseignants seront-ils tenus responsables des manquements à la politique des élèves mineurs placés sous leur responsabilité? Est-ce que les parents des élèves mineurs devraient être informés de cette politique puisque leurs enfants sont des utilisateurs? En ce qui concerne les élèves adultes, l'Alliance considère qu'ils ne pourront se soustraire à leur propre responsabilité.

3- Supervision

L'Alliance est en accord avec le fait que le gestionnaire soit responsable de la supervision des utilisateurs sous sa responsabilité – la direction d'établissement dans le cas des enseignantes et enseignants.

L'Alliance s'interroge cependant sur les activités de vérification et de surveillance active du comportement des utilisateurs et tient à rappeler que la littérature à cet effet mentionne qu'il faut un motif raisonnable avant de procéder à une surveillance.

De plus, les modalités d'application du projet de politique indiquent que le Service de la gestion des personnes et des compétences (SGPDC) a la responsabilité d'autoriser une demande de contrôle, de vérification ou de surveillance active des activités faite par un gestionnaire à l'égard d'un utilisateur mais que la décision d'aviser un utilisateur qu'une telle demande a été faite est à la discrétion du gestionnaire de qui relève l'utilisateur. L'Alliance est d'avis que la personne concernée par une telle demande doit en être avisée systématiquement. Il en est de même lorsque l'autorisation de contrôle et de surveillance est accordée.

Le Service des technologies de l'information peut, quant à lui, amorcer une enquête sans autorisation préalable. L'Alliance comprend la nécessité de vérifier de façon générale l'utilisation qui est faite du matériel de la CSDM mais est d'avis que la vérification ou la surveillance du comportement d'un utilisateur doit toujours être autorisée par le SGPDC.

Une inquiétude est également soulevée par la lecture du texte portant sur l'adhésion à la politique (5.2). Il y est écrit que « Tout manquement à la présente politique et à ses modalités d'application doit être rapporté au directeur de l'unité administrative concernée [...] ». Est-ce à dire que tout le monde espionne et est espionné? Est-ce un encouragement à la délation? L'Alliance estime qu'il est de la responsabilité du supérieur immédiat de veiller à l'application de la politique et de ses modalités d'application.

Il est aussi écrit que « l'utilisation de tout outil technologique doit être réservée en priorité aux besoins liés à sa fonction (paragraphe 5.3) ou compatibles avec la fonction exercée (5.3.6). Il s'agit ici d'une expression très large. Qui sera responsable d'évaluer s'il y a compatibilité ou non d'une recherche, faite sur Internet par exemple, avec les besoins liés à la fonction?

Finalement, l'Alliance tient à rappeler que la convention collective locale prévoit à la clause 3-2.07 que la déléguée ou le délégué syndical peut avoir accès à un ordinateur de l'école pour acheminer ou recevoir des informations de nature syndicale. La Politique et ses modalités d'application devraient exclure nommément ses échanges de toute possibilité de contrôle, de vérification ou de surveillance active.

4- Perte des droits d'utilisation

La Politique prévoit que l'utilisateur qui quitte la CSDM perdra les droits d'utilisation de son adresse @csdm au plus tard 90 jours après son départ (5.9.8). L'Alliance croit qu'il faudrait spécifier que la perte des droits d'utilisation pourra se faire après un départ « définitif » et ce afin de s'assurer qu'une enseignante ou un enseignant conserve son accès aux séances d'affectation par Internet (SAI) étant donné que la convention locale prévoit que le nom d'une suppléante ou d'un suppléant ne peut être retiré du bassin que dans le cas où elle ou il n'a dispensé aucun service à la Commission pendant deux (2) ans (Annexe V).

L'Alliance conçoit qu'un utilisateur pourrait perdre les droits d'utilisation de son adresse @csdm dans certains cas de mesures disciplinaires. Cependant, cette perte de droit ne devrait en aucun temps restreindre son droit à l'obtention d'une affectation via les séances d'affectation par Internet (SAI).

5- Omission

La Politique fait état des droits, responsabilités et obligations de l'utilisateur. L'Alliance constate cependant l'absence d'un élément important que devrait contenir une politique d'utilisation des technologies à savoir l'identification claire et précise des comportements qui constituent une violation de la politique et l'énumération des conséquences dans le cas du non-respect de celle-ci.