Addendum à l'offre *Enrollment for Education Solutions* (EES) Microsoft Online Services Agreement (Accord sur les services en ligne de Microsoft)

ID de la modification : EES17

N° EES *À remplir par Microsoft*		ID de la proposition

L'addendum à l'Accord sur les services en ligne de Microsoft (l'« addendum sur les services en ligne de Microsoft ») est conclu entre les parties désignées sur le formulaire de signature en vue de l'offre susmentionnée (l'« Offre EES »). Les parties conviennent que l'addendum sur les services en ligne de Microsoft complète l'Offre EES et ne s'applique qu'aux services en ligne de Microsoft, définis ci-dessous, que l'établissement achète aux termes de l'Offre EES.

1. Définitions

Les mots en lettres majuscules qui sont utilisés mais non définis dans le présent addendum sur les services en ligne de Microsoft ont le sens qui leur est donné dans l'Offre EES ainsi que dans l'accord *Campus and School*. Les définitions qui suivent sont utilisées dans le présent addendum sur les services en ligne de Microsoft :

« données sur les clients » Désigne toutes les données, y compris tous les fichiers textuels, sonores ou visuels qui sont fournis à Microsoft par l'Établissement, ou par l'entremise de ce dernier, dans le cadre de l'utilisation que fait l'Établissement des services en ligne de Microsoft.

« Office 365 Services » Désigne : a) Exchange Online, Exchange Online Archiving, SharePoint Online, Lync Online et les Office Web Apps inclus dans Office 365 Academic Plans A2, A3 et A4; et b) Exchange Online Plans 1, 2, Basic et Kiosk; SharePoint Online Plans 1, 2 et Kiosk; Office Web Apps Plans 1 et 2, et Lync Online Plans 1, 2 et 3. Les Office 365 Services n'incluent pas la suite Office 365 ProPlus ou tout autre service de marque distincte offert avec un plan ou une suite de marque Office 365.

« Services en ligne Dynamics CRM » Désigne les UGS de licences en volume concernant les services en ligne Dynamics CRM, comme DynCRMOnln ALNG SubsVL MVL PerUsr (DSD-00001). L'expression « services en ligne de Microsoft », dans le cas de la présente modification seulement, désigne Office 365 Services et/ou Dynamics CRM Online Services.

« utilisateur ultime » Désigne la personne qui a accès aux services en ligne de Microsoft.

2. Protection des renseignements personnels

a. **Pratiques en matière de protection des renseignements personnels.** Microsoft se conforme à toutes les lois en matière de protection des données et de protection de la vie privée qui s'appliquent de façon générale à la fourniture de ses services en ligne. Cependant, Microsoft n'est pas responsable du respect des lois en matière de protection des données ou de protection de la vie privée qui s'appliquent à l'Établissement ou à ses activités et qui ne visent pas de façon générale les fournisseurs de services infotechnologiques.

b. Données sur les clients. Microsoft traitera les données sur les clients d'une manière conforme aux dispositions du présent addendum sur les services en ligne de Microsoft et, à l'exception de ce qui est indiqué dans l'Offre EES et le présent addendum sur les services en ligne de Microsoft, Microsoft : 1) n'acquerra aucun droit à l'égard des données sur les clients et 2) n'utilisera ou ne communiquera des données sur les clients à aucune fin autre que celles énoncées ci-après. L'utilisation que fait Microsoft des données sur les clients est la suivante :

(i) Les données sur les clients ne serviront qu'à fournir à l'Établissement les services en ligne de Microsoft. Cela peut inclure les mesures de dépannage visant à prévenir, déceler et rectifier les problèmes touchant le fonctionnement des services en ligne de Microsoft ainsi qu'à améliorer les caractéristiques qui comprennent les mesures de détection et de protection concernant les menaces nouvelles auxquelles l'utilisateur est exposé (comme les logiciels malveillants ou les pourriels).

(ii) Microsoft ne divulguera les données sur les clients à un organisme d'exécution de la loi que si la loi l'exige. Si jamais un tel organisme entre en contact avec Microsoft et demande d'obtenir des données sur l'Établissement, Microsoft s'efforcera de faire en sorte que l'organisme d'exécution de la loi s'adresse directement à l'Établissement pour lui demander ses données. Dans le cadre de ces mesures, il est possible que Microsoft fournisse à l'organisme en question les coordonnées de base de l'Établissement. Si elle est obligée de communiquer des données sur les clients à un organisme d'exécution de la loi, Microsoft déploiera des efforts raisonnables sur le plan commercial pour aviser à l'avance l'Établissement d'une telle divulgation, sauf si la loi l'interdit.

c. Suppression ou retour des données sur les clients. À l'expiration ou à la résiliation de l'utilisation, par l'Établissement, des services en ligne de Microsoft, l'Établissement peut extraire les données sur les clients et Microsoft supprimera ces dernières, conformément, dans chaque cas, aux droits d'utilisation des produits.

d. Demandes de l'utilisateur ultime. Microsoft ne donnera pas suite de manière indépendante aux demandes émanant des utilisateurs ultimes de l'Établissement sans avoir obtenu au préalable le consentement écrit de l'Établissement, sauf dans les cas où la loi applicable l'exige.

e. Transfert des données sur les clients; désignation. Les données sur les clients que Microsoft traite pour le compte de l'Établissement peuvent être transférées, stockées et traitées aux États-Unis ou dans tout autre pays dans lequel Microsoft, ses filiales ou ses sous-traitants tiennent des installations. L'Établissement désigne Microsoft pour exécuter tout transfert de données sur les clients à ces pays ainsi que pour stocker et traiter les données sur les clients en vue de fournir les services en ligne de Microsoft. Microsoft : 1) se conforme aux cadres-refuge de l'UE et de la Suisse qui sont énoncés par le Département du commerce des Etats-Unis, relativement à la collecte, à l'utilisation et à la conservation des données émanant de l'Union européenne, de l'Espace économique européen et de la Suisse, et 2) pendant la durée désignée dans le cadre de l'Offre EES, demeurera certifiée dans le cadre des programmes-refuge de l'UE et de la Suisse, dans la mesure où ces derniers sont reconnus par le gouvernement des États-Unis.

f. Personnel de Microsoft. Le personnel de Microsoft ne traitera pas les données sur les clients sans l'accord de ces derniers. Le personnel de Microsoft est tenu de respecter la

confidentialité des données sur les clients, et cette obligation se poursuit même après la fin de son engagement.

g. **Sous-traitants/transferts**. Microsoft peut retenir les services d'autres entreprises pour fournir des services restreints en son nom, comme la prestation de services de soutien aux clients. Ces sous-traitants sont autorisés à obtenir des données sur les clients à seul fin de fournir les services pour lesquels Microsoft les a engagés, et il leur est interdit d'utiliser les données sur les clients à toute autre fin. Microsoft demeure chargée de la manière dont ces sous-traitants respectent les obligations du présent addendum sur les services en ligne de Microsoft. Les sous-traitants auxquels Microsoft transfère des données sur les clients auront conclu avec Microsoft des ententes écrites qui les obligeront à assurer au moins le même degré de protection de la vie privée que celui qui s'applique aux données personnelles que Microsoft reçoit et qu'exigent les principes-refuge applicables. L'Établissement consent à ce que Microsoft transfère des données sur les clients aux sous-traitants de la manière décrite dans le présent addendum sur les services en ligne de Microsoft. À l'exception de ce qui précède, ou si l'Établissement en décide autrement, Microsoft ne transférera à aucun tiers (même pas à des fins de stockage) les données personnelles que l'Établissement fournira à Microsoft par l'entremise des services en ligne de Microsoft.

3. Responsabilités de l'Établissement

L'Établissement est tenu de se conformer aux exigences légales applicables en matière de protection des renseignements personnels, de protection des données et de confidentialité des communications qui se rapportent à l'usage qu'il fait des services en ligne de Microsoft.

4. Autres conditions européennes

Si l'Établissement compte des utilisateurs ultimes dans l'Espace économique européen ou en Suisse, les conditions additionnelles qui suivent s'appliquent. Les termes utilisés dans la présente section qui ne sont pas définis de manière expresse ont le sens qui leur est donné dans la Directive 95/46/CE du Parlement européen et par le Conseil du 24 octobre 1995 sur la protection des individus en ce qui concerne le traitement des données personnelles et le libre mouvement de ces données (« Directive sur la protection des données de l'UE »).

a. **Intention des parties.** Pour ce qui est des services en ligne de Microsoft, l'Établissement est le contrôleur des données et Microsoft est un organisme de traitement de données qui agit pour le compte de l'Établissement. En tant qu'organisme de traitement de données, Microsoft ne donnera suite qu'aux instructions de l'Établissement. Le présent addendum sur les services en ligne de Microsoft et l'Offre EES (y compris les conditions qui y sont incorporées par renvoi) représentent les directives complètes et finales de l'Établissement à Microsoft en ce qui a trait au traitement des données sur les clients. Toutes les directives additionnelles ou de rechange doivent être approuvées, d'une manière conforme au processus de modification de l'Offre EES de l'Établissement.

b. **Durée et objet du traitement des données.** La durée du traitement des données correspond à celle qui est désignée dans l'Offre EES. L'objectif de ce traitement est la prestation des services en ligne de Microsoft.

c. **Portée et objet du traitement des données.** La portée et l'objet du traitement des données sur les clients, y compris toutes les données personnelles incluses dans ces données, sont décrites dans l'addendum sur les services en ligne de Microsoft ainsi que dans l'Offre EES.

d. Accès aux données sur les clients. Pendant la durée désignée dans l'Offre EES, Microsoft, à son gré et selon ce qu'impose la loi applicable mettant en œuvre l'alinéa 12b) de la Directive sur la protection des données de l'UE : 1) donnera à l'Établissement la possibilité de corriger, de supprimer ou de bloquer les données sur les clients, ou 2) procèdera aux corrections, aux suppressions ou aux blocages nécessaires pour le compte de l'Établissement.

e. Agent de protection des renseignements personnels. Il est possible de joindre le représentant de la protection des renseignements personnels de Microsoft pour l'Espace économique européen et la Suisse à l'adresse suivante :

Microsoft Ireland Operations Ltd.
À l'attention de l'agent de la protection des renseignements personnels
Carmenhall Road
Sandyford, Dublin 18 (Irlande)

5. Sécurité

a. Pratiques générales. Microsoft a mis en œuvre et tient à jour des mesures techniques et organisationnelles, des contrôles internes et des mesures de sécurité de l'information qui visent à protéger les données sur les clients contre la perte accidentelle, la destruction ou la modification, la divulgation ou l'accès non autorisés ou la destruction illicite, et ce, de la manière suivante :

(i) Domaine : Organisation de la sécurité de l'information

1) Responsabilité de la sécurité. Microsoft a désigné un ou plusieurs agents de sécurité chargés de coordonner et de surveiller les règles et les procédures de sécurité.

2) Rôles et responsabilités en matière de sécurité. Le personnel de Microsoft ayant accès aux données sur les clients est soumis à des obligations en matière de confidentialité.

3) Programme de gestion des risques. Microsoft a procédé à une évaluation de risques avant de traiter les données sur les clients ou de lancer ses Services en ligne.

4) Microsoft tient ses documents de sécurité d'une manière conforme à ses exigences en matière de conservation une fois que ces documents ne sont plus en vigueur.

(ii) Domaine : Gestion des biens

1) Liste des biens. Microsoft tient des listes de tous les supports dans lesquels sont stockées les données sur les clients. L'accès à ces listes est réservé au personnel de Microsoft qui est autorisé par écrit à le faire.

2) Manipulation des biens

A) Microsoft classe les données sur les biens de façon à aider à les identifier et à permettre à ce que l'accès à ces dernières soit limité de manière appropriée (p. ex., par chiffrement).

B) Microsoft impose des restrictions à l'impression des données sur les clients et a établi des procédures concernant l'élimination des documents imprimés qui contiennent des données sur les clients.

C) Le personnel de Microsoft doit obtenir l'autorisation de Microsoft avant de stocker des données sur les clients dans des dispositifs portables, d'accéder à distance à des données sur les clients ou de traiter des données sur les clients en dehors des installations de Microsoft. Cela inclut, notamment, le fait de retirer des installations de Microsoft des supports (p. ex., clés USB et CD-ROM) et des documents contenant des données sur les clients.

(iii) Domaine : Sécurité des ressources humaines

1) Formation en matière de sécurité

A) Microsoft informe son personnel des procédures de sécurité applicables ainsi que des rôles respectifs à jouer. Elle informe également son personnel des conséquences possibles d'un manquement aux règles et aux procédures de sécurité.

B) Microsoft ne se sert que de données anonymes dans le cadre de ses activités de formation.

(iv) Domaine : Sécurité physique et environnementale

1) Accès physique aux installations. Microsoft restreint l'accès aux installations dans lesquelles sont situées des systèmes d'information qui traitent les données sur les clients aux seules personnes autorisées à le faire.

2) Accès physique aux éléments. Microsoft tient un relevé des supports entrants et sortants qui contiennent des données sur les clients, dont le genre de support, l'expéditeur et les destinataires autorisés, la date et l'heure, le nombre de supports ainsi que les types de données sur les clients qu'ils contiennent.

3) Protection contre les perturbations. Microsoft se sert de divers systèmes standards de l'industrie pour se protéger contre la perte de données par suite d'une panne d'électricité ou d'interférences touchant les lignes de communication.

4) Élimination d'éléments. Microsoft se sert de processus standards de l'industrie pour supprimer les données sur les clients quand ces dernières ne sont plus nécessaires.

(v) Domaine : Communications et gestion des activités

1) Politique opérationnelle. Microsoft tient des documents sur la sécurité qui décrivent ses mesures de sécurité ainsi que les procédures applicables et les responsabilités des membres de son personnel qui ont accès aux données sur les clients.

2) Procédures de récupération des données

A) De façon permanente, mais en aucun cas à intervalles de moins d'une semaine (sauf si aucune donnée sur les clients n'a été mise à jour au cours de cette période), Microsoft tient de multiples copies des données sur les clients à partir desquelles il est possible de récupérer ces données.

B) Microsoft stocke les copies des données sur les clients et les procédures de récupération des données dans un endroit différent de celui où est situé le matériel informatique principal qui traite les données sur les clients.

C) Microsoft a établi des procédures précises pour régir l'accès aux copies des données sur les clients.

D) Microsoft passe en revue les procédures de récupération des données au moins tous les six mois.

E) Microsoft consigne les mesures de restauration des données, y compris la personne qui en est chargée, la description des données restaurées et les données (s'il y en a) qu'il a fallu intégrer manuellement dans le processus de récupération des données.

3) Logiciels malveillants. Microsoft est dotée de contrôles anti-logiciels malveillants qui aident à éviter que de tels logiciels obtiennent un accès non autorisé aux données sur les clients, et cela inclut les logiciels malveillants émanant de réseaux publics.

4) Données hors limites

A) Microsoft chiffre les données sur les clients qui sont transmises par des réseaux publics.

B) Microsoft restreint l'accès aux données sur les clients qui sont présentes dans les supports qui sortent de ses installations (p. ex., par chiffrement).

(vi) Domaine : Limitation de l'accès

1) Politique en matière d'accès. Microsoft tient un relevé des privilèges en matière de sécurité que détiennent les personnes ayant accès aux données sur les clients.

2) Autorisation de l'accès

A) Microsoft tient à jour un relevé des membres du personnel qui sont autorisés à accéder aux systèmes de Microsoft qui contiennent des données sur les clients.

B) Microsoft désactive les légitimations d'authentification qui n'ont pas été utilisées depuis au moins six mois.

C) Microsoft identifie les membres du personnel qui peuvent accorder, modifier ou annuler l'accès autorisé aux données et aux ressources.

3) Droit d'accès minimal

A) Les membres du personnel de soutien technique n'ont le droit d'accéder aux données sur les clients qu'en cas de besoin.

B) Microsoft limite l'accès aux données sur les clients aux personnes qui en ont besoin pour exécuter leurs tâches professionnelles.

4) Intégrité et confidentialité. Microsoft donne instruction aux membres de son personnel de désactiver les séances administratives lorsqu'ils quittent les installations que Microsoft contrôle ou lorsque des ordinateurs sont par ailleurs laissés sans surveillance.

5) Authentification

A) Microsoft utilise des pratiques standards de l'industrie pour identifier et authentifier les utilisateurs qui tentent d'avoir accès aux systèmes d'information.

B) Lorsque les mécanismes d'authentification sont fondés sur des mots de passe, Microsoft exige que ces derniers soient renouvelés à intervalles réguliers.

C) Lorsque les mécanismes d'authentification sont fondés sur des mots de passe, Microsoft exige que ces derniers comportent au moins huit caractères.

D) Microsoft s'assure que les identificateurs désactivés ou expirés ne sont pas attribués à d'autres personnes.

E) Microsoft surveille les tentatives répétées d'accès aux systèmes d'information au moyen d'un mot de passe non valide.

F) Microsoft tient des procédures standards de l'industrie pour désactiver les mots de passe corrompus ou divulgués par inadvertance.

G) Microsoft utilise des pratiques standards de l'industrie pour protéger les mots de passe, y compris celles qui sont conçues pour préserver la confidentialité et l'intégrité des mots de passe quand ces derniers sont attribués et distribués ainsi qu'au cours de leur stockage.

6) Conception de réseaux. Microsoft dispose de contrôles permettant d'éviter qu'une personne assumant des droits d'accès qui ne lui ont pas été assignés parvienne malgré tout à accéder à des données sur les clients.

(vii) Domaine : Gestion des incidents relatifs à la sécurité des informations

1) Processus d'intervention en cas d'incident. Microsoft tient un relevé des atteintes à la sécurité qui comportent : une description de l'atteinte, le moment de l'atteinte et ses conséquences, le nom de la personne qui l'a signalée et la personne à laquelle elle a été signalée, de même que la procédure suivie pour récupérer les données.

2) Surveillance des services. Les membres du personnel de sécurité de Microsoft vérifient les relevés à intervalles d'au moins six mois en vue de proposer, au besoin, des mesures correctives.

(viii) Domaine : Gestion de la continuité des activités

1) Microsoft tient des plans d'urgence et de contingence pour les installations où sont situés ses systèmes d'information qui traitent les données sur les clients.

2) Les procédures de stockage redondant et de récupération des données de Microsoft sont conçues pour tenter de ramener les données sur les clients à l'état dans lequel elles se trouvaient avant leur perte ou leur destruction.

(ix) Les mesures de sécurité décrites dans la présente section 5 sont les seules responsabilités qui incombent à Microsoft en rapport avec les données sur les clients. Pour ce qui est de ces données, ces mesures remplacent toutes les obligations de confidentialité contenues dans l'Offre EES ou dans toute autre entente de non-divulgation conclue entre Microsoft et l'Établissement.

b. Certifications et vérifications

(i) Microsoft a établi et convient de tenir à jour une politique en matière de sécurité des données qui est conforme aux normes ISO 27001 qui s'appliquent à l'établissement, à la mise en œuvre, au contrôle et à l'amélioration du Système de gestion de la sécurité de l'information ainsi qu'au code ISO/IEC 27002 des pratiques exemplaires en matière de gestion de la sécurité de l'information (la « Politique régissant la sécurité des informations en ligne de Microsoft ».) Selon le principe de l'accès sélectif et confidentiel, et sous réserve de l'accord de l'Établissement à l'égard des obligations de non-divulgation que Microsoft spécifie, Microsoft mettra la Politique régissant la sécurité des informations en ligne de Microsoft à la disposition de l'Établissement, de pair avec les autres informations que l'Établissement demandera de manière raisonnable au sujet des pratiques et des politiques de Microsoft en matière de sécurité. L'Établissement est seul chargé de passer en revue la Politique régissant la sécurité des informations en ligne de Microsoft, de décider par lui-même si cette politique répond à ses exigences et de veiller à ce que les membres de son personnel et ses consultants suivent les lignes directrices qu'on leur fournit au sujet de la sécurité des données.

(ii) Microsoft vérifiera la sécurité des ordinateurs et de l'environnement informatique dont elle se sert pour traiter les données sur les clients (ce qui inclut les données personnelles) dans le cadre des services en ligne de Microsoft, ainsi que celle des centres de données physiques à partir desquels Microsoft fournit ses services en ligne. Cette vérification : 1) aura lieu au moins une fois par année, 2) sera exécutée d'une manière conforme aux normes ISO 27001, 3) sera accomplie par des professionnels de la sécurité tiers que Microsoft aura choisis et qu'elle paiera, 4) donnera lieu à la production d'un rapport de vérification (le « rapport de vérification de Microsoft »), lequel fera partie des informations confidentielles de Microsoft, et 5) pourra être menée à des fins autres que le fait de répondre aux exigences de la présente section (p. ex. dans le cadre des procédures de sécurité interne régulières de Microsoft ou en vue de s'acquitter d'autres obligations de nature contractuelle).

(iii) Si l'Établissement en fait la demande par écrit, Microsoft fournira à ce dernier un sommaire confidentiel de son rapport de vérification (le « rapport sommaire ») de façon à ce que l'établissement puisse vérifier de manière raisonnable si Microsoft se conforme aux obligations en matière de sécurité qu'impose le présent addendum sur les services en ligne de Microsoft. Le rapport sommaire fait partie des informations confidentielles de Microsoft.

(iv) Microsoft s'efforcera, de bonne foi et d'une manière raisonnable sur le plan commercial, de corriger : 1) toute erreur relevée dans un de ses rapports de vérification et qui, peut-on raisonnablement s'y attendre, aura un effet néfaste sur l'utilisation que fait l'établissement des services en ligne de Microsoft, et 2) les lacunes de contrôle importantes qui sont relevées dans ce rapport de vérification.

6. Notification d'incident de sécurité

a. Si Microsoft prend connaissance d'un accès illicite aux données sur les clients qui sont stockées dans son matériel ou ses installations, ou d'un accès non autorisé à ce matériel ou à ces installations qui entraîne une perte, une divulgation ou une modification des données sur les clients (dans chaque cas, un « incident de sécurité »), Microsoft s'engage à , sans

délai : a) notifier le client de l'incident de sécurité, b) faire enquête sur cet incident et fournir ensuite au client des renseignements détaillés, et c) prendre des mesures raisonnables pour atténuer les effets de l'incident et réduire les dommages susceptibles d'en découler.

b. Le client convient que :

(i) tout incident de sécurité infructueux ne sera pas assujetti à la présente section. Un incident de sécurité infructueux est un incident qui ne donne pas lieu à un accès non autorisé aux données sur les clients ou au matériel ou aux installations de Microsoft dans lesquels sont stockés ces données sur les clients, et il inclut, notamment, les sondeurs PING et autres attaques lancées contre les pare-feux ou serveurs frontières, balayages de port, tentatives de connexion infructueuses, attaques entraînant un refus de service, reniflages de paquets (ou autres accès non autorisés à des données liées au trafic qui ne permettent pas d'aller au-delà des adresses IP ou des en-têtes) ou des incidents semblables;

(ii) l'obligation qu'a Microsoft de signaler un incident de sécurité ou d'y répondre en vertu de la présente section ne saurait être interprétée comme une reconnaissance de sa part de toute faute ou responsabilité à l'égard de cet incident de sécurité.

c. Les incidents de sécurité, s'il y en a, seront notifiés à un ou plusieurs des administrateurs du client par tout moyen que Microsoft choisit, y compris par courriel. Il incombe exclusivement au client de veiller à ce que ses administrateurs tiennent en tout temps des coordonnées exactes dans le portail des Services en ligne.

7. Divers

a. Confidentialité. L'Établissement est tenu de considérer comme confidentiels les modalités du présent addendum sur les services en ligne de Microsoft, le contenu de la Politique régissant la sécurité des informations en ligne de Microsoft, le rapport de vérification de Microsoft et le rapport sommaire, et il lui est interdit de les divulguer à des tiers, à l'exception de ses vérificateurs ou de ses consultants qui ont besoin d'avoir accès à ces renseignements pour les besoins de la relation d'affaires exposée dans le présent addendum sur les services en ligne de Microsoft et l'Offre EES.

b. Durée et résiliation. Le présent addendum sur les services en ligne de Microsoft sera automatiquement résilié à l'expiration ou à la résiliation de l'Offre EES.

c. Ordre de préséance. S'il survient un conflit entre une disposition quelconque du présent addendum sur les services en ligne de Microsoft et tout autre disposition de l'Offre EES ou de l'accord *Campus and School*, ce sont les dispositions du présent addendum qui ont préséance.

d. Totalité de l'entente. À l'exception des changements qu'apporte le présent addendum sur les services en ligne de Microsoft, l'Offre EES demeure inchangée et s'applique intégralement.

Pour être valide, le présent addendum doit être joint à un formulaire de signature.