Addendum No. 1

to Google Apps for Education Agreement

This Addendum (Addendum) is incorporated by reference into the Google Apps for Education Agreement ("Agreement") entered into by and between Google Inc. ("**Google**"), and the customer identified in the Order Form ("**Customer**") effective as of the date Customer clicked the "I Accept" button or, if applicable, the date the Agreement is countersigned (the "**Effective Date**"). The provisions of this Addendum amend or supplement the Agreement. Where the provisions of this Addendum conflict with the Agreement, the Addendum prevails.

1. The definition of "Customer Data" in the Agreement will be deleted in its entirety and replaced with the following:

   "Customer Data" means data, including email, provided, generated, transmitted, displayed, or stored via the Services by Customer or End Users."

2. The definition of "Confidential Information" in the Agreement will be deleted in its entirety and replaced with the following:

   "Confidential Information" means information disclosed by a party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is considered Customer's Confidential Information. Customer or End Users, as applicable, own all Customer Data."

3. The following section will be added to the Agreement:

   "a. Acknowledgement Regarding MFIPPA. "MFIPPA" means the Municipal Freedom of Information and Protection of Privacy Act, Revised Statutes of Ontario 1990, chapter M.56, as amended or otherwise modified from time to time. Customer advises Google that Customer is subject to MFIPPA. Google covenants and agrees to utilize commercially reasonable efforts to provide Customer with timely access to End User Accounts and Customer Data as limited by section 2.7 (or the equivalent section entitled Third Party Requests). Customer is responsible for evaluating whether use of the Services is consistent with its legal obligations under MFIPPA.

   b. Indemnification By Customer. Customer agrees to indemnify Google from and against any fines relating to MFIPPA violations."

4. The following section will be added to the Agreement:

> "Use of Customer Data. Google will use Customer Data for the following purposes: (a) to provide the Services; (b) to operate, maintain, enhance and support the infrastructure used to provide the Services; and (c) to comply with Customer's or End Users' instructions in the use, management and administration of the Services; (d) to respond to customer support requests. Google will only use Customer Data in accordance with this Agreement."

5. The following sentence will be added to the end of Section 12.3 (or the equivalent section titled Effects of Termination) of the Agreement:

> "Upon Customer deleting data, Google will delete the data and pointers to the data from active servers and replication servers."

6. Section 10.1 (or the equivalent section entitled Representations and Warranties) in the Agreement will be deleted in its entirety and replace with the following:

> "Each party represents that it has full authority to enter into the Agreement. Each party warrants that it will comply with all laws and regulations applicable to its provision or use of the Services. Google warrants that it will provide the Services in accordance with the applicable SLA. Customer represents that it is an Educational Institution. "Educational Institution" means any publicly funded elementary or secondary school or school board or educational program operated by school boards throughout the Province of Ontario, and further includes First Nation and native schools in Ontario, operating under the Ontario educational curriculum as such curriculum may exist from time to time, publicly funded Faculties of Education and Ontario teacher training institutes; For greater certainty the term "Educational Institution" does not include private schools. Customer acknowledges and agrees that it is solely responsible for compliance with the Children's Online Privacy Protection Act of 1998 (USA), and in particular with obtaining parental consent for collection of students' Confidential Information used in connection with the Services by the Customer and End Users."

7. The following section will be added to the Agreement:

> "As of the Effective Date, Google abides by the security standards in Attachment A ("Security Standards"). During the term of the Agreement, the Security Standards may change but Google agrees that any such change shall not cause a material degradation in the security of the Services."

Attachment A

Google Apps Security Standards

In these Security Standards below, unless specified herein, "Services" means the following: Google Apps for Business, Google Apps for Education, Google Apps for Government and Google Apps – Postini Services:

1. Data Center & Network Security.

   a. Data Centers

      i. Infrastructure. Google maintains a vast number of geographically distributed Google-owned or Google-managed data centers. Google stores all production data in physically secure data centers.

      ii. Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

      iii. Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

      iv. Server Operating Systems. Google servers use a Linux based implementation customized for the Google application environment. Customer Data is stored using Google proprietary algorithms to augment data security and redundancy. Google

employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

v. Businesses Continuity. Google has designed and regularly engages in actively planning and testing its business continuity planning/disaster recovery programs.

b. Networks & Transmission.

i. Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. Google transfers all Customer Data via Internet standard protocols.

ii. External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect Google's external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

iii. Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's approach to this involves:

1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;

2. Employing intelligent detection controls at data entry points; and

3. Employing technologies that automatically remedy certain dangerous situations.

iv. Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

2. Access and Site Controls.

a. Site Controls.

i. On-site Data Center Security Operation. Each Google data center maintains an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

ii. Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site

security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized Google employees, contractors and visitors are allowed entry to the data centers. Only Google employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

iii. On-site Data Center Security Devices. Google data centers employ an electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

b. Access Control.

i. Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for Google personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and for responding to security incidents.

ii. Access Control and Privilege Management. Administrators and End Users must authenticate themselves via a central authentication system or via a Customer's single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

iii. Internal Data Access Processes and Policies – Access Policy. Google employs a centralized access management system to control personnel access to Google production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a Google proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, Customer Data and configuration information. Google requires the use of unique user IDs, strong passwords; two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication at Google (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., Credit Card data), Google uses hardware tokens.

c. Audits and Certifications. During the Term, Google will maintain its Standard for Attestation Engagement No. 16 audit report or a comparable report ("Audit Report") and its ISO/IEC 27001:2005 Certification or a comparable certification ("ISO Certification") for Google Apps Core Services. Google will update the Audit Report, at least every eighteen (18) months.

d. Security Breach. To the extent a state or federal security breach law applies to a Security Breach, Google will comply with the applicable law. To the extent no such law applies to a Security Breach, Google will notify Customer of a Security Breach, following the discovery or notification of such Security Breach, in the most expedient time possible under the circumstances, without unreasonable delay, consistent with the legitimate needs of applicable law enforcement, and after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Google will send any applicable notifications regarding a Security Breach to the Notification Email Address or via direct communication with the Customer (e.g. phone call, in person meeting, etc). For purposes of this Section, "Security Breach" means an actual disclosure, or reasonable belief that there has been a disclosure, by Google of Customer Data to any unauthorized person or entity.

3. Data.

a. Data Storage, Isolation & Authentication. Google stores Customer Data in a multi-tenant environment on Google-owned servers. Customer Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Google logically isolates data on a per End User basis at the application layer. Google also logically isolates data on a per Customer account basis, and each Customer account will be given control over specific data sharing policies. Google logically separates data from different End Users from each other, and data for an authenticated End User will not be displayed to another End User (unless the former End User or Administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data.

b. Decommissioned Disks and Disk Erase Policy. Certain disks containing Customer Data may experience performance issues, errors or hardware failure that lead them to be decommissioned by Google ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.