Privacy Impact Assessment

Google Apps for Education

Memorial University of Newfoundland

Prepared by: Computing and Communications
Information Access and Privacy Protection

Creation Date: Version 1.0 October 2011

Contents

Executive Summary

This Privacy Impact Assessment supports the 'Privacy Compliance Checklist' completed for the ***Memorial University of Newfoundland Google Apps for Education Project*** and provides further information and analysis of the project's impact on privacy. Supporting documents are provided herein as enumerated appendices.

The Google Apps for Education project is aimed at improving the student email service and providing students with increased storage and tools such as real-time document collaboration, calendaring, and directory services that the University does not and cannot currently provide. By utilizing Google as a service provider, the risk related to security will be reduced, and greater protection will be provided to users through Google's threat-protection technology, effectively blocking viruses, filtering spam, and alerting users to phishing scams, and other threats.

A 4 month Google Apps for Education pilot to approximately 160 Faculty of Business Administration Commerce students was administered through the Spring 2011 academic semester and completed in August 2011. The pilot allowed for an assessment of the technical integration of Google Apps into Memorial's environment, the support model required, and the measurement of the student experience. Computing and Communications assessment was corroborated by the positive results of a survey to pilot participants, confirming that Google Apps for Education was perceived as a beneficial tool to the students of the University. Students will have access to a functionally rich suite of tools, greater mobile device configuration options, and greater than 60 times increase in storage space from the current Memorial email offering. Students will have the flexibility and functionality that they have come to expect from other available services.

Risks associated with privacy have been outlined in this document, some of which are mitigated through specific activities of Memorial and the contractual relationship with Google. Privacy risks include data intrusions and security, lawful access and questions of jurisdiction. Arguably, the most talked about risk associated with the use of Google services is information being disclosed to law enforcement or national security agencies under foreign legislation such as the USA Patriot Act. While the probability of such a request for information remains low, the risk to privacy it imposes - especially since Google may be forbidden from informing the University or the user of such a request - is significant, with little possibility of mitigation. We note that many institutions in Canada have assessed the risks associated with providing email through external cloud providers and they have determined that the benefits of adoption outweigh the risks. Examples of Canadian institutions that have implemented such a service include the University of Alberta (students, staff, and faculty - 2011), University of Toronto (students - 2011, alumni - 2008), University of PEI (students - 2011), Lakehead University (students, staff, and faculty - 2007), and Wilfred Laurier (students - 2010). Provinces such as Nova Scotia and British Columbia have legislation prohibiting, except in certain circumstances, the storage of personally identifiable information outside of Canada, but University of British Columbia and Dalhousie University have adopted Google Apps for Education services.

In March 2011, representatives from Computing and Communications and the University's Information Access and Privacy Protection Office met with the Office of the Information and Privacy Commissioner (OIPC). An overview of the project was presented to the designated OIPC official, together with a commitment to provide them with a copy of this privacy impact assessment. The OIPC is invited to provide feedback to the University on this project.

In September 2011, representatives from Computing and Communications presented an overview of the project to the University's Information Access and Privacy Protection Advisory Committee. The advisory

committee subsequently reviewed this privacy impact assessment and provided input and feedback on it at their October 2011 meeting and that input is incorporated.

It is the recommendation of Computing and Communications to expand the users of Google Apps for Education and proceed with a complete roll-out to all students of Memorial. The Information Management Committee approved this recommendation in October 2011 and a transition and communications strategy is currently being executed to replace the current student email service with a Memorial branded version of Google Apps for Education.

Definitions

Account – Establishes a user's identity and provides the authorization for a user to utilize Google Apps for Education.

Cloud Computing - A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST, 2011)

Data Mining - A technique for searching large-scale databases for patterns; used primarily to find previously unknown correlations between variables that may be commercially useful.

Email Alias - An alternative email address that points to an existing primary email address. For example, the user student@mun.ca might also want to receive email addressed to student_alias@mun.ca. If the user creates student_alias@mun.ca as an email alias for student@mun.ca, Google Apps will deliver email for both of these addresses to the same Gmail inbox. An email alias is optional.

Email Client - An application that runs on a personal computer and enables a user to send, receive and organize e-mail. Examples of email clients include Microsoft Outlook, Mozilla Thunderbird, and Apple Mail.

Function Creep - The gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy.

Google Apps for Education – The Google Apps for Education Services provided by Google and used by Memorial University. The Google Apps for Education Services are described here: http://www.google.com/a/help/intl/en/users/user_features.html.

Information Management Committee (IMC) - Serves as one element of the overall IT governance at Memorial University. The IMC's role is to provide a broad, campus-wide or "Enterprise" view of the Information Technology Applications Architecture and Technical Infrastructure to align these with Memorial's Strategic Plan.

Lightweight Directory Access Protocol (LDAP) - Provides a means of sharing address book type of information (e.g. name, address, email) across an intranet or the Internet.

Mobile Device - A generic term used to refer to a variety of devices that allow users to access data and information from wherever they are. This includes cell phones and portable devices.

Personal Information - Means recorded information about an identifiable individual, including (not an exhaustive list)

- the individual's name, address or telephone number
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations
- the individual's age, sex, sexual orientation, marital status or family status

- an identifying number, symbol or other particular assigned to the individual
- the individual's fingerprints, blood type or inheritable characteristics
- information about the individual's health care status or history, including a physical or mental disability
- information about the individual's educational, financial, criminal or employment status or history
- the opinions of a person about the individual, and
- the individual's personal views or opinions

Primary Email Address - The email address created and assigned when the user enrolls at, or is hired by, the University. Every user has a primary email address.

Records of the University – A record, in any media or form, under the control of the University and stored in any manner, created, received or maintained by the University in the routine course of its business and legal obligations and set aside for future reference.

Secure Sockets Layer (SSL) - A protocol that provides secure communications on the Internet for such things as web browsing, e-mail, instant messaging and other data transfers. SSL is available for Gmail, Chat, Calendar, Docs, and Sites.

Single Sign-On - An authentication model that enables users to access a variety of computing resources without being repeatedly prompted for their user IDs and passwords.

University - Memorial University of Newfoundland.

User - An individual permitted to make use of Memorial University's Google Apps for Education.

Project Description

The Google Apps for Education project is an initiative to improve the current student email service offered by Memorial University through implementation of Google's Gmail and associated suite of applications. In addition to email, Google Apps for Education will provide new document collaboration abilities, calendaring, and directory services that Memorial currently does not offer to students.

An assessment of external service providers of email and calendaring services, and the recent trends of other post-secondary institutions across Canada, led Computing and Communications (C&C) to consider Google's Apps for Education. Google Apps for Education meets the needs of the University and are offered free of charge to educational institutions. A preliminary assessment indicated that a contract for these services to Google Inc. would be of operational, and potentially economic, advantage to the University.

The initial phase of the project started with an investigation through the form of a pilot project, including approximately 160 Term 4 Commerce students from the Faculty of Business. The 16 week pilot helped C&C determine the impact that Google Apps would have on a number of our environments including technical, Service Desk and support, and allowed us to gather feedback on the experience from the participants. A comprehensive survey was delivered to the pilot group after 12 weeks of use.

Compiled results indicated that:

- 100% of respondents were "satisfied" or "very satisfied" with Google Apps for Education (76% indicated "very satisfied").
- Based on the pilot experience, 96% of respondents indicated that they would recommend Google Apps to other Memorial Students (89% indicated "Yes", 7% indicated "Yes, with reservations").
- A total of 81% of respondents indicated that Google Apps enhanced their ability to effectively communicate (44% - enhanced greatly, 37% enhanced somewhat)
- When asked if the collaboration tools offered by Google Apps have the potential to enrich the (or their?) learning experience, 67% of respondents indicated "agree" with an additional 20% indicating "somewhat agree"

Project Objectives

The objectives of Memorial's Google Apps for Education project are as follows:

- To improve email service to the University's students
- To provide new document collaboration, calendaring, and directory services
- To reduce the risk related to information technology security
- To provide other new services that the University cannot currently provide

Requirements for Personal Information

For students opting to avail of Google Apps for Education services, the following personal information will be disclosed to Google for account creation purposes:

- First Name
- Last Name
- Username / User ID
- Email Aliases (if applicable)
- Password (encrypted)

New students to the University will be automatically assigned an account but on first log-in will be given a detailed description of the services, terms and conditions, and risks and asked to give consent (as described under User Consent further in this document) or to choose the option of declining Google Apps for Education services and instead using the current email system for students. The draft consent which students will be asked to sign is attached as Appendix B.

Account creation information will not be collected directly from students; it already exists as data used to set them up on a variety of University accounts and to provide access to a number of University computing resources.

As part of the Google Apps communications and deployment strategy, current students will be presented with the choice of opting into the Google Apps for Education service. If a student does not wish to opt in, they will be able to maintain their existing email account without alteration and no personal information will be provided to Google for account creation purposes.

The user ID will be the same ID that students are assigned by Memorial to access other University provided services (e.g. MUN Portal, Memorial@Home, etc). To enable the support of mobile devices and email clients, a user's password will be stored at Google. This password will be synchronized with a user's Google account by University systems when a user updates their password.

The nature of email, calendaring, and applications allows for document creation, collaboration, and storage, meaning that many records containing personal information may be compiled by students through their use of email, Google Docs and associated applications. While the University will have access to student data in accordance with the terms of its contract with Google, the University will exercise access to data generated by students only if authorized by law.

This agreement is subject to the Google Apps for Education Terms of Service Agreement (specifically section 6.1, Intellectual Property Rights) which states "Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services."

Authority for Collection, Use and Disclosure of Personal Information

The University is a public body under the province's *Access to Information and Protection of Privacy Act*

(ATIPPA). Its authority to collect, use, disclose and its obligations to protect personal information are set out in that legislation.

The University is authorized under section 32 of the *ATIPPA* to collect personal information that relates directly to and is necessary for an operating program or activity of the University. The personal information collected and compiled by the university for the purpose of establishing student email accounts and access to university services is authorized under section 32(c).

> 32. *No personal information may be collected by or for a public body unless*
>
> *(a) the collection of that information is expressly authorized by or under an Act;*
>
> *(b) that information is collected for the purposes of law enforcement; or*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body.*

The *ATIPPA* imposes further restrictions around a public body's collection of personal information, namely that information must be collected directly from the individual concerned unless the legislation permits indirect collection under section 33. To establish student email accounts and to provide students with access to university services, the personal information needed is collected directly from students when they register as a student of the University.

A further constraint on a public body's collection of personal information is the requirement in 33(2) of the *ATIPPA* which requires the University as a public body to notify individuals from whom personal information is collected of the purpose for the collection, the legal authority for the collection and contact information of a person who can respond to questions about the collection. The privacy notice given to individual students who opt to use the Google Apps for Education service will contain the notice information required by 33(2).

> 33. *(2) A public body shall tell an individual from whom it collects personal information*
>
> *(a) the purpose for collecting it;*
>
> *(b) the legal authority for collecting it; and*
>
> *(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.*
>
> *(3) Subsection (2) does not apply where*
>
> *(a) the information is about law enforcement or anything referred to in section 22 (1) or (2); or*
>
> *(b) in the opinion of the head of the public body, complying with it would*
>
> *(i) result in the collection of inaccurate information, or*

(ii) defeat the purpose or prejudice the use for which the information is collected.

The University is authorized by the *ATIPPA* to use personal information for the purpose for which it was obtained or compiled, or a consistent use, or with the consent of the individual concerned or for a number of purposes set out in sections 39 to 42. The University's use of the personal information compiled to establish student email accounts and access to university services is authorized under 38(1)(a). As well, as set out below, the University's authority for this use comes from 38(1)(b).

The *ATIPPA* does not require the university to obtain an individual's consent to collect, use and disclose information since a public body's collection, use and disclosure of personal information is limited to only that information which is necessary for an operating program or activity. Use and disclosure are further constrained by other provisions in the legislation. However, because account information and information generated by Google Apps for Education users will be stored outside Canada, the university deems that informed consent is necessary and that for students who opt not to use the Google service, the current university email system will be available to them. Accordingly, the University's authority to use the personal information compiled to establish student email accounts and access to university services is authorized under 38(1)(a) and 38(1)(b)

Comment [A1]: Lionel suggested clarification in this paragraph. He quoted reference to several sections of ATIPPA (32, 39?). I know that you were clear on what he was talking about, so my notes are not much more detailed than that.

38. *(1) A public body may use personal information only*

(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 40 ;

(b) where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act; or

(c) for a purpose for which that information may be disclosed to that public body under sections 39 to 42 .

(2) The use of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.

The University's disclosure of personal information necessary to establish an account is authorized under section 39(1)(b) and 39(1)(c). The constraint imposed by 39(1)(2) is also met.

39. *(1) A public body may disclose personal information only*

(b) where the individual the information is about has identified the information and consented to the disclosure in the manner set by the minister responsible for this Act;

(c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in section 40 ;

(2) The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.

A necessary consideration about the University's obligations under the *ATIPPA* concerns the vast amount of data that student users of the Google Apps for Education project will generate. Some of the users will send email to the University and such information, on receipt by the University, may be deemed to be in the custody or control of the University for *ATIPPA* purposes, as that term is defined in the University's Information Request policy. However, the vast amount of emails and correspondence and other information created by students for their own purposes will not be considered to be in the custody or control of the University.

Comment [A2]: Lionel seemed to have issue with the "Custody and Control" piece, but I felt you were more than comfortable with the way things are currently written.

Two specific requirements of the Google Apps for Education service is that the university, as the customer, will have the ability to access, monitor, use, or disclose data in users' accounts and that the University must handle third party requests for access to information in an account. The Appropriate Use of Computing Resources Policy addresses access to users' accounts and the circumstances in which such access may be authorized.

The University will generate and maintain records necessary to document its business and legal obligations and will ensure the maintenance of these records in accordance with approved policies and procedures of the University.

The Single Email for Students and Employees policy at Memorial University of Newfoundland stipulates that Memorial will provide all students, staff, faculty, retirees, and alumni, with a single e-mail address that is to be the sole address used for official University e-mail communication. Every student and employee is provided with a single e-mail address as required and official e-mail correspondence from Memorial will be sent only to the Memorial address.

Any request for access to records under the province's *Access to Information and Protection of Privacy Act* will be handled in accordance with the University's Information Request policy.

Information Security Measures

Email is, by nature, an inherently insecure form of communication. There is a need to educate users of this fact. Gmail is at least as secure as the current campus email service and, arguably, more secure. While in transit, email is often unencrypted and could be intercepted. A user should always assume that email is not private, and this is true for all email services. However, the level of security provided to users of Google Apps for Education services includes a secure connection from the user's web browser and/or email client. This encrypts the data between the user and Google's servers during use, comparable to the methods that banks use to secure a user's connection for online banking.

Memorial University

User passwords for Google Apps will be managed through Memorial's systems, the process of which will remain unchanged from the current setup. By providing password management through Memorial's systems, all internal password policies will be enforced, including the requirements of password complexity and password expiration (a student must change their password every 122 days). As noted, to support mobile devices and email clients, a user's password will be stored at Google. A password will be stored using an industry standard level of encryption, sent over a secure connection, and synchronized only when a user changes their password at Memorial (Google's systems will never request an update of a

user password from Memorial). The level of encryption, in conjunction with Memorial's password complexity and expiration policies, make a compromised password in the encrypted format computationally prohibitive to break. Only passwords of Google Apps users will be synchronized with Google.

Memorial policies, such as the Privacy, Electronic Data Security and Appropriate Use of Computing Resources policies, exist to protect both users and the University. All members of the University have an obligation to comply with approved policies. The Electronic Data Security policy outlines the risks of transmitting sensitive electronic data through email and instant messaging and also provides a procedure for encrypting sensitive files that must be transmitted electronically. The Appropriate Use of Computing Resources policy provides guidance in a number of areas including access, accounts and identities, personal account responsibility, personal use, inspection, use and disclosure.

Administrative access to Memorial's Google Apps for Education is limited to authorized personnel for the purposes of account creation, maintenance, and security. Access may be exercised if authorized or required by law. Access privileges will be continuously assessed and will be rescinded in the event of a change in employee job duties.

Google

The security control will be managed through the contract for services with Google Inc. Details of security measures were provided to Memorial by Google in a document titled "Google Enterprise Products Security Standards". This document is included as an appendix in the contract between Google and Memorial. A review and analysis of the security practices employed by Google indicates that Google is able to provide both physical and technical security measures that will be commensurate with, exceed, or greatly exceed, the security that the University can provide. Google security measures include:

- Secure storage of data – user data will be stored in Google's network of data centers. Google maintains a number of geographically distributed data centers, the locations of which are kept discreet for security purposes. Google's computing clusters are designed with resiliency and redundancy in mind, eliminating any single point of failure and minimizing the impact of common equipment failures and environmental risks. Access to data centers is limited to only authorized select Google employees personnel.

- Data is safe from other institutions - Data is virtually protected as if it were on its own server. Unauthorized parties cannot access another's data. In fact, all user accounts are protected via this virtual lock and key that ensures that one user cannot see another user's data. This is similar to how customer data is segmented in other shared infrastructures such as online banking applications.

- Google Apps has received a satisfactory SAS 70 Type II audit - This means that an independent auditor has examined the controls protecting the data in Google Apps (including logical security, privacy, Data Center security, etc) and provided reasonable assurance that these controls are in place and operating effectively.

- Protection against attacks - Google runs its data centers using custom hardware running a custom OS and file system. Each of these systems has been optimized for security and performance. The Google Security Team continuously works with external parties to test and enhance security

infrastructure to ensure it is impervious to external attackers. And because Google controls all of the systems that run the Google Apps service, they are able to quickly respond to any threats or weaknesses that may emerge.

- Protection from hardware failure or natural disasters - Google maintains a number of geographically distributed data centers. Google's computing clusters are designed with resiliency and redundancy in mind, eliminating single points of failure and minimizing the impact of common equipment failures and environmental risks. Access to our data centers is restricted to authorized personnel.

- User protection from spam, viruses, and phishing attacks - All Google Apps services provide the ability to access all data using encryption and Memorial has chosen to require this option for all users. This helps ensure that no one except the user has access to his or her data. This is true for access to mail, calendar, video, and chat data via Google's web applications. The mobile email client also uses encrypted access to ensure the privacy of communications.

List of Personal Information Data Elements

To set up a Google Apps for Education account for a user, the following personal information data elements must be created and stored on Google's servers:

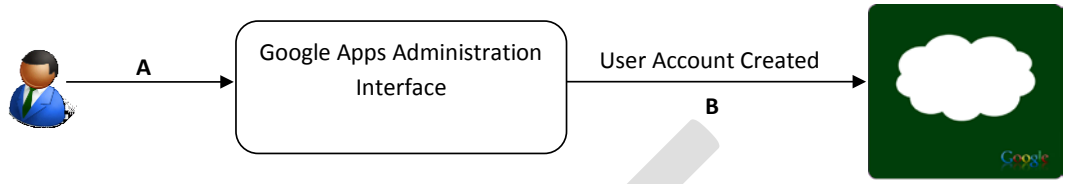
- First Name
- Last Name
- Username / User ID
- Email Aliases (if applicable)
- Password (Encrypted)

The above information is the only data disclosed to Google by Memorial, strictly for the purposes of account creation. All other data that will be stored on Google servers will be created by the users. The nature of email, calendaring, and applications that allow for document creation, collaboration, and storage, means that the vast volume of records generated through the use of the services will be records generated by student users and will not be considered to be in the University's custody and/or control in accordance with the *ATIPPA*

Personal Information Flows

1) Creation of a Google Apps User Account

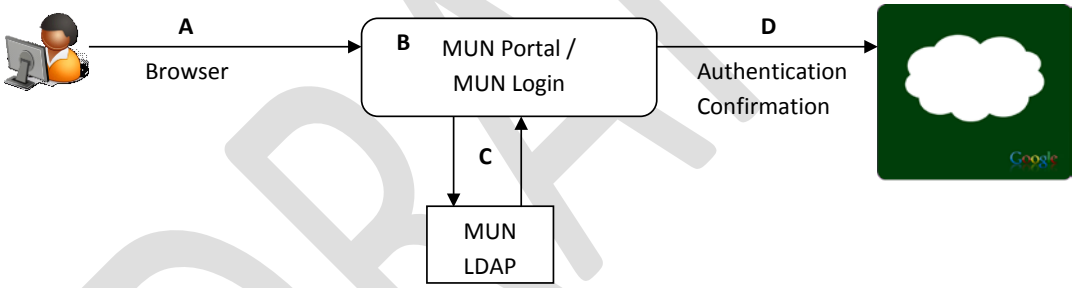
The creation of a Google Applications user account requires a one time (per user) flow of personal information from Memorial to Google. This information is provided to Google only once a student's consent is obtained.



1. A Memorial Google Apps administrator accesses the Google Apps Administration panel. (**A**)

2. A user account is created, which includes the following data elements: first name, last name, user ID, email aliases (if applicable), and password (encrypted). (**B**)

2) Google Apps Browser Based Access



1. A user enters Memorial's Google Apps web address (i.e. my.mun.ca) in a browser. (**A**)

2. The user authenticates through MUN Login, providing the necessary credentials (i.e. user id and password). This authentication is performed locally, using Memorial's Lightweight Directory Access Protocol (LDAP) server. (**B**)

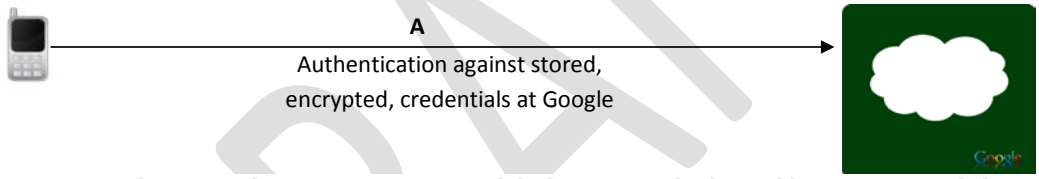
3. An industry standard Single Sign-On protocol has been adopted, to enable users to log into Google Apps using the same user id and password that is used for other University services. This setup also provides the ability to provide instant access upon logging into Memorial's Portal, or authenticating through MUN Login. Access to Google Apps for Education through a web browser, using Single Sign-On, functions as follows:

    - The user logs into Memorial's Portal (i.e. my.mun.ca), providing the necessary credentials (user id/password). These are the same credentials used for other Memorial services. (**B**)

- Upon successful login, a portal tab, visible only to individuals with a Google Apps account, will be displayed. A user selects his/her desired Google App (Gmail, Calendar, Docs, etc.) from the Google Apps portal tab. (**B**)
- When a user requests access to a Google app, Google sends a request to MUN's authentication server to confirm that the user has been successfully authenticated. (**C**)
- To this request, the authentication server sends a confirmation response. Because authentication has been performed through MUN Login (via the Portal), the user can now access Google Apps for Education. (**D**)
- To the user, after successful login to the Portal, the experience is a one-click entry into the desired Google App.

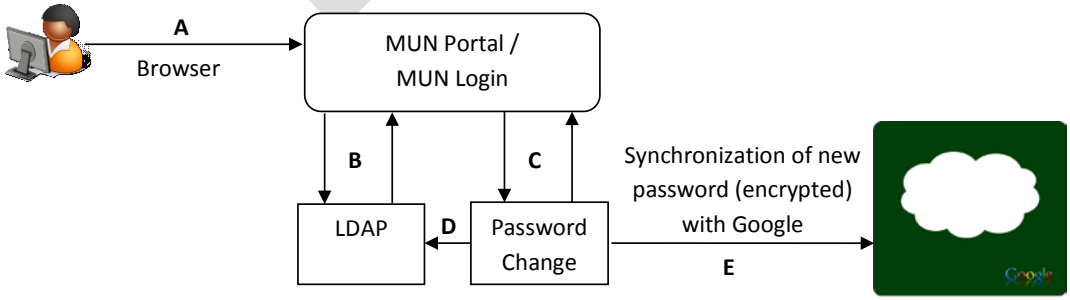
4. When a user accesses his/her account through a browser, all authentication is performed locally at Memorial.

3) Google Apps Mobile Device (and Email Client) Access



1. To utilize a Google Apps account on a mobile device or to check email by using an email client, a password must first be synchronized with the user's Google account (see Google Apps Account Password Change).
2. When accessing Google Apps through a mobile device or a desktop email client, authentication is performed directly with Google, using the user's Google account and synchronized Memorial password. (**A**)

4) Google Apps Account Password Change



1. A user enters the MUN Login or portal address (e.g. my.mun.ca) in a browser. (**A**)

2. The user authenticates through MUN Login, providing the necessary credentials (user id / password). This authentication is performed locally, using Memorial's LDAP server. (**B**)

3. A user initiates a password change using the MUN Login password change link. (**C**)

4. The password is updated on Memorial's LDAP server (**D**) and, in parallel, sent to the user's Google Account to ensure synchronization (**E**). The synchronization of a password is a one way process (e.g. it is sent to Google from Memorial, never requested from Memorial by Google) that takes place when a user changes his/her password through MUN Login. The password is synchronized with the user's Google account and stored, encrypted, by an industry standard.

User Consent

As discussed in the section entitled Authority for the Collection, Use and Disclosure of Personal Information, prior to the creation of a Google Apps account for a user, the informed consent of that user will be obtained through agreement with the terms and conditions that govern Google Apps for Education at Memorial (Appendix B). As well, Memorial will extensively communicate with stakeholders during the ongoing adoption of Google Apps for Education to ensure that they understand the issues and risks and also educate and communicate responsibilities to students (e.g., potential forwarding of messages, mobile device security, etc.).

In addition to the communicated issues and risks, the Consent and Notice to a user will address:

- the authority and purpose of the collection of personal information and the legal authority for it (required by s.33(2) of *ATIPPA*)
- contact information of a person who can respond to questions about the collection and use of personal information (required by s.33(2) of *ATIPPA*)
- consent required for the release of information to Google for the purposes of account creation
- consent to allow Google to give to the University administrators of the Google Apps for Education service the ability to access, monitor, use, or disclose data available to users within the users' accounts. Administrative access to Memorial's Google Apps for Education will be limited to authorized personnel for the purposes of account creation, maintenance, and security. Access may be exercised if authorized or required by law. Access privileges will be continuously assessed and will be rescinded in the event of a change in employee job duties.
- notification of other aspects of the service, including that the service will not serve ads, that non-Google apps products will not be enabled, and certain restrictions on use

Comment [A3]: The OIPC suggested restating the parameters of administrative access in this section.

As part of the Google Apps communications and deployment strategy, current students will be presented with the choice of opting into the Google Apps for Education service. If a student does not wish to opt in, they will be able to maintain their existing email account without modification. For those that opt-in, the information necessary for the purposes of account creation will be disclosed to Google. This required information is detailed in the section titled "List of Personal Information Data Elements" of this document.

Contractual Relationships

A contract between Memorial University and Google is currently being negotiated for the provision of Google Apps for Education to the University. This contract is anticipated to be in place by October 2011. The initial term of the contract will be for five years, effective as of the service commencement date which will be specified in the negotiated contract. During the term, there will be no charge for the University to use Google's services. Also, the contract stipulates that the University has no obligation to use the services of Google Apps for Education and may cease to do so at any time, for any reason (or no reason).

Privacy Risks

A number of the risks identified below have been adopted from risks identified by the Office of the Privacy Commissioner of Canada, in a publication titled "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing".

Jurisdiction - Subject to laws of other countries

Summary of Risk

- Access to University and/or user information held on Google servers as a consequence of foreign laws

Description of Risk

By utilizing Google Apps for Education, data will be stored and processed outside of Canada. Google is a wholly owned United States based company and personal information will be stored in the United States and possibly in multiple jurisdictions. As such, legislation of the United States, including laws like the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) may apply. The PATRIOT Act is one of a range of measures available to American authorities to access Canadians' information. Others include National Security Letters and grand jury subpoenas. The PATRIOT Act permits American law enforcement and national security agencies the ability to access information for law enforcement and foreign intelligence purposes. Its reach extends beyond U.S. borders, however. American companies doing business outside the U.S. and possibly organizations based in Canada or another jurisdiction with a presence in the U.S. may be "required to turn over customers' data to U.S. authorities on demand and, at the same time, be prohibited from acknowledging to anyone that their records have been accessed by a foreign government." [1] Memorial University information and information generated by student users of the Google Apps service may be provided by Google to American law enforcement or national security agencies without knowledge or notice to the student users or to the University.

[1] Lorna Stefanik (2007) "Outsourcing and transborder data flows: the challenge of protecting personal information under the shadow of the *USA Patriot Act*," *International Review of Administrative Sciences* 2007 73:532.

Two provinces in Canada (British Columbia and Nova Scotia) have enacted legislation which places certain restrictions on public and/or private bodies engaged in transborder data flows; however, no such legislation exists in Newfoundland and Labrador. We note that the University of British Columbia in British Columbia and Dalhousie University in Nova Scotia have both adopted Google Apps for Education services.

Using Google Apps for Education does not necessarily introduce a new or greater risk of University data being stored and processed outside of Canada. While the information of Google Apps may be physically located in the United States, which would allow the US Government to obtain direct access to that information, information located in Canada may still be accessible through sharing agreements between various law enforcement agencies. Also, information which is held in an email account has no guaranteed privacy. Any email exists not only in the account it has been sent to, but also in the account it was sent from, in any accounts to which it was forwarded, and likely on many servers which are situated in the United States. If an email user wanted to ensure that their account was not subject to US Government surveillance they would also need to ensure that those with whom they are corresponding have also ensured that their own accounts have no US exposure. A similar risk currently exists through the use of mobile devices on an external providers network, or on any device that transmits information outside of the University's environment. The use of many common devices today result in user information being stored in cloud environments.

Description of Mitigation Measures

- Contract provisions with Google state that the University, not Google, is responsible for responding to third party information requests and that, where legally permissible, Google will notify the University of any requests or demands it receives for personal information.
- Users of Google Apps for Education will be informed that their emails and all associated content that is created or stored, will reside in a foreign jurisdiction and will be subject to the laws of that jurisdiction, including the USA Patriot Act. Users can then make an informed decision about what kind of information they will transmit through email. The University will inform users that it will not be able to guarantee protection against the possible disclosure of data residing outside of Canada.

Estimation of Residual Risk after Mitigation

The contractual provisions assist in mitigating the risk that Google may provide information to a legal authority under American law but do not guarantee that Google will refuse to comply with an order under the Patriot Act or a national security letter. The risk remains that data stored by users of the Google Apps for Education service at Memorial University may be disclosed without notice to the university or users if required by law.

Lawful Access

Summary of Risk

- The issue of "collateral disclosure" (i.e., when a search warrant is served for one set of data on the service provider and it captures unrelated data by mistake.)
- User data accessed lawfully, but without notification

Description of Risk

Several Canadian laws authorize interception or seizure of personal information. The *Access to Information and Protection of Privacy Act* (under section 39) authorizes Memorial University to disclose personal information to comply with a subpoena, warrant or order or to comply with an Act or regulation of the province or of Canada. In Canada, the *Criminal Code, Anti-Terrorism Act, and CSIS Act* are among laws which permit production orders, search warrants, etc. to be issued. *ATIPPA* requires the university to ensure that such a disclosure is limited to the minimum amount of information necessary to fulfill the purpose for which it is disclosed. An order or warrant for data stored through the Google Apps for Education service may be presented to the University directly or to Google.

Beyond the generalized risk of government intrusion, outsourcing email services also raises particular concerns when it comes to lawful access. Lawful access itself is, of course, of concern whether the information is stored on a user's computer or with a service provider. However, use of cloud computing infrastructure, such as Google Apps for Education, raises the risk that an order or warrant will be presented to the service provider without the University's knowledge.

For instance, where many organizations are using Google's centralized infrastructure, a lawful access request to Google has the potential to garner information from data unrelated to the request, resulting in access to information above and beyond that intended by lawful access legislation. There are also instances that may prohibit Google from disclosing or notifying Memorial of the request for access, essentially leaving users unaware of the lawful access to their data.

The *Access to Information and Protection of Privacy Act* does not require the university to notify individuals if their information is disclosed except in cases where personal information is disclosed in the public interest in accordance with section 31 of the *Act.*

Description of Mitigation Measures

An order, warrant or other demand for information presented to the University would be reviewed with legal counsel. The Office of the General Counsel would oversee any such disclosure and, in accordance with *ATIPPA*'s requirement to minimize disclosure, the risk of "collateral disclosure" would accordingly be minimized.

- Memorial is required to comply with lawful requests for access
- The contract with Google requires due diligence and notification (where notification is not prohibited by law) of any disclosure of data

Estimation of Residual Risk after Mitigation

Contractual language specifies notification of access requests, where notification is not prohibited by law. It is very likely that if there was a lawful request to Google for access to data stored through the Google Apps for Education service, and that request prohibited Google from notifying the University, Memorial and/or Memorial users would probably not be informed.

Consumer lack of control / Function creep

Summary of Risk

- Changes in Google's business model may compromise the integrity or availability of University information
- Specific functionality of Google Apps for Education might expand over time without management rigor
- The cloud computing model may act as an incentive for Google to extend the features and scope of their product to take advantage of the information that is gathered through use of the services

Description of Risk

By allowing the control to reside in Google as the provider of the service, it may create unforeseen problems and risks for the University. Given the dynamic nature of Google, changes in business practices may affect the handling of University information and information generated by student users and the policy, procedures, and legislative requirements of the University. Another risk is that Memorial may adopt new features and services as implemented by Google without scrutiny, leading to the gradual widening of the use of Google Apps for Education beyond the purpose for which it was originally intended. Such adoption may lead to potential privacy concerns.

Description of Mitigation Measures

- Ongoing monitoring and risk assessment as to changes in the business practices of Google to ensure that the services provided are consistent with University policies.
- A formal process will be followed to seek approval from Memorial's Information Management Committee in the implementation or expansion of new functionality provided through Google Apps.
- Contract provisions clearly define that Google is not the owner of the data.
- Contractual language defines the process of notification in the event of material changes to the services that Google provides.
- The contract also states that Memorial has no obligation to use the Services and may cease using the Services at any time for any reason.
- Administrative functionality allows Memorial administrators to specify services users can utilize with Memorial Google Apps.

There is a concern of a potential service model change (e.g. pay vs. free) due to limitations of flexibility; however, the University's protection consists of a number of factors that can mitigate this risk:

- The negotiation of a contract between Memorial and Google. Typical contract terms for other universities have been for five year terms.
- The technical expertise will still exist at Memorial to bring e-mail back in-house if necessary.
- An option of exploring alternative approaches to providing a student email service exists (e.g. use a student's personal e-mail account(s) for official University correspondence).
- If services, or features, switch from a freely available to a pay service, Memorial can explore the option of paying for the service.

Estimation of Residual Risk after Mitigation

It is expected that over time, we will continue to use adopt cloud-based products for greater functionality, and also that Google will continue to provide greater functionality. While Memorial's email is tightly controlled today, Google allows considerable flexibility, and today's students are using other cloud services (e.g. Facebook, Twitter, personal Gmail accounts) for their own purposes.

Creation of New Data Streams, Advertising, and Data Mining

Summary of Risk

- Data mining, sale or transfer of data
- Targeted advertisements based on usage history

Description of Risk

A service like Google Apps for Education has the potential for users to create a huge collection of (new) data, and to expose it to Google. There is a risk that this data stream will be used, or sold, for purposes beyond those for which consent was originally given. This risk could involve any number of misuses of data, including the detailed analysis of user data for the purposes of serving users with targeted advertising.

Description of Mitigation Measures

- Contract provisions with Google
    - State that Google may use Confidential Information only to exercise rights and fulfill its obligations under the contractual agreement. The contract defines "Customer Data" as data generated through use of the Google Apps services. Customer Data is considered Confidential Information. In addition, Google states in their privacy policy (Appendix A), that if a user's data is used in a manner different from the purpose for which it was collected, then Google will ask for prior consent.
    - Clearly define data ownership does not rest with Google
- Google Advertising is a feature that Memorial can control – it can be turned on or off

Estimation of Residual Risk after Mitigation

The risk of data mining, sale or transfer of data is minimized by contract provisions. Memorial's Google Apps for Education service will not permit advertising and any decision to do so will not be made without extensive consultation and notice to users.

Data Intrusions & Security

Summary of Risk

- Authentication details stored at Google
- Personal identifiable information may be created, sent, and stored at Google by users
- Residual data may exist on systems after deletion/removal

Description of Risk

The risk of data intrusion and security relates to the possibility of unauthorized access, use or disclosure of personal information. There is a risk of email messages or documents containing personal information being inappropriately disclosed or intercepted in transmission. The nature of email, calendaring, and applications that allow for document creation, collaboration, and storage, means that any number of records containing personal information may be collected, used, and/or disclosed through the use of email and may exist in any of the user content that is generated using Google Docs and associated applications. A related risk through the use of email and content services includes the possible persistence of residual information or records on systems after that information was thought to be deleted and/or destroyed.

Description of Mitigation Measures

- There is a need to educate our users that e-mail is inherently insecure and that personally identifiable information should not be sent via e-mail
- There are no plans at this time to store any university information at Google other than the limited user data required for the purposes of account creation (described in this document)
- Passwords shared with Google for the support of mobile devices are stored using industry standard encryption methods. All password management is conducted at Memorial and all Memorial password policies are enforced. Upon a local password change, a user's new password is synchronized with the user's Google account using the encrypted format.

Estimation of Residual Risk after Mitigation

While data intrusions and the security of university information and information generated by users is an identified privacy risk, it is a risk that also exists in Memorial's current environment. A review and analysis of the security practices employed by Google indicates that:

- Google has a vastly larger resource base
    - People
    - Technology
    - Finances
- Security is "mission critical" for both Google's business and their reputation
- Google's physical security is much better
- Google's electronic security is much stronger
- Google will provide a greater level of security (both physical and electronic) than Memorial is able to provide

Mobile Device Security

Summary of Risk

- Unsecured mobile devices may place the personal information of users at risk, as many users typically do not take the basic steps necessary to protect their personal information.

Description of Risk

If a mobile device is lost or stolen, the personal information and privacy of a user could be threatened if the device is not protected by password and other user-level security measures. A recent survey by the Office of the Privacy Commissioner of Canada (2011 Canadians and Privacy Survey) found that only 39% of users of mobile devices configured a password lock on their device. It also found that only 40% of users adjusted the settings of their device or applications to limit the amount of personal information that they share with others.

Description of Mitigating Measures

- There is a need to educate our users of security and privacy issues, including those introduced by the use of mobile devices. For many mobile devices, security can be greatly enhanced by simply enabling password protection on a device, and to configure the lock screen to come on after a short period of inactivity. Memorial will extensively communicate with stakeholders during the ongoing adoption of Google Apps for Education. Communication will provide details on mobile security and will be provided through sessions with users, detailed documentation, and Service Desk staff.
- While Google provides greater connectivity options for accessing services through mobile devices, this risk is also present in our current environment

Estimation of Residual Risk after Mitigation

Even with communication and awareness, there will likely be a number of student users who will do little or nothing to protect their devices and, other than awareness, there is little that can be done by Memorial to ensure that devices are protected.

Summary of Risks and Mitigation Measures

As outlined, there are a number of privacy risks that may be associated with a move to a service like Google Apps for Education. Mitigating factors include:

- Memorial will avoid a “one size fits all” contract with Google and ensure that Memorial’s responsibilities are reflected in the contract. The contract will include provisions such that:
    - Data ownership is clear
    - There will be no data mining
    - There will be no advertising
    - Memorial policies are reflected and respected in the contract

- Memorial will manage the adoption of new functionality and function changes formally.

- There is a need to educate our users on security and privacy issues. Memorial will extensively communicate with stakeholders during the ongoing adoption of Google Apps for Education.

- Prior to the creation of a Google Apps account for a user, the informed consent of that user will be obtained through agreement with the terms and conditions that govern Google Apps for Education at Memorial (Appendix B).

Risk to privacy and security will be monitored and existing Memorial processes will be followed when risk events occur.

This Privacy Impact Assessment will be updated as necessary to reflect any applicable changes to Google Apps for Education, the University's policies and procedures, or legislative requirements of the University.

General Assessment of Project Compliance with Applicable Legislation

A review of Newfoundland and Labrador legislation, as performed by the project team, indicates that the adoption of Google Apps for Education is permitted by the *ATIPPA*, but only with the caveat that users not be compelled to use the service and may opt instead to use the existing University service. Memorial's Office of the General Counsel and the Information Access and Privacy Protection Office have been involved extensively in the privacy impact assessment and negotiation of a contract between the University and Google.

Appendices

Appendix A

Google Apps for Education Privacy Policy

Last modified: October 3, 2010 (view archived versions)

This Privacy Policy applies to all of the products, services and websites offered by Google Inc. or its subsidiaries or affiliated companies except Postini (Postini Privacy Policy). Sometimes, we may post product specific privacy notices or Help Center materials to explain our products in more detail.

If you have any questions about this Privacy Policy, please feel free to contact us through our website or write to us at

Privacy Matters
c/o Google Inc.
1600 Amphitheatre Parkway
Mountain View, California, 94043
USA

Information we collect and how we use it

We may collect the following types of information:

- **Information you provide** – When you sign up for a Google Account, we ask you for personal information. We may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services. For certain services, we may give you the opportunity to opt out of combining such information. You can use the Google Dashboard to learn more about the information associated with your Account. If you are using Google services in conjunction with your Google Apps Account, Google provides such services in conjunction with or on behalf of your domain administrator. Your administrator will have access to your account information including your email. Consult your domain administrator's privacy policy for more information.
- **Cookies** – When you visit Google, we send one or more cookies to your computer or other device. We use cookies to improve the quality of our service, including for storing user preferences, improving search results and ad selection, and tracking user trends, such as how people search. Google also uses cookies in its advertising services to help advertisers and publishers serve and manage ads across the web and on Google services.
- **Log information** – When you access Google services via a browser, application or other client our servers automatically record certain information. These server logs may include information

such as your web request, your interaction with a service, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser or your account.

- **User communications** – When you send email or other communications to Google, we may retain those communications in order to process your inquiries, respond to your requests and improve our services. When you send and receive SMS messages to or from one of our services that provides SMS functionality, we may collect and maintain information associated with those messages, such as the phone number, the wireless carrier associated with the phone number, the content of the message, and the date and time of the transaction. We may use your email address to communicate with you about our services.
- **Affiliated Google Services on other sites** – We offer some of our services on or through other web sites. Personal information that you provide to those sites may be sent to Google in order to deliver the service. We process such information under this Privacy Policy.
- **Third Party Applications** – Google may make available third party applications, such as gadgets or extensions, through its services. The information collected by Google when you enable a third party application is processed under this Privacy Policy. Information collected by the third party application provider is governed by their privacy policies.
- **Location data** – Google offers location-enabled services, such as Google Maps and Latitude. If you use those services, Google may receive information about your actual location (such as GPS signals sent by a mobile device) or information that can be used to approximate a location (such as a cell ID).
- **Unique application number** – Certain services, such as Google Toolbar, include a unique application number that is not associated with your account or you. This number and information about your installation (e.g., operating system type, version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers (for example, to request automatic updates to the software).
- **Other sites** – This Privacy Policy applies to Google services only. We do not exercise control over the sites displayed as search results, sites that include Google applications, products or services, or links from within our various services. These other sites may place their own cookies or other files on your computer, collect data or solicit personal information from you.

In addition to the above, we may use the information we collect to:

- Provide, maintain, protect, and improve our services (including advertising services) and develop new services; and
- Protect the rights or property of Google or our users.

If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use.

Google processes personal information on our servers in the United States of America and in other countries. In some cases, we process personal information outside your own country.

Choices

You can use the Google Dashboard to review and control the information stored in your Google Account.

Most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some Google features and services may not function properly if your cookies are disabled.

Google uses the DoubleClick advertising cookie on AdSense partner sites and certain Google services to help advertisers and publishers serve and manage ads across the web. You can view and manage your ads preferences associated with this cookie by accessing the Ads Preferences Manager. In addition, you may choose to opt out of the DoubleClick cookie at any time by using DoubleClick's opt-out cookie.

Information sharing

Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:

- We have your consent. We require opt-in consent for the sharing of any sensitive personal information.
- We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.
- We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.

If Google becomes involved in a merger, acquisition, or any form of sale of some or all of its assets, we will ensure the confidentiality of any personal information involved in such transactions and provide notice before personal information is transferred and becomes subject to a different privacy policy.

Information security

We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, including appropriate encryption and physical security measures to guard against unauthorized access to systems where we store personal data.

We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it on our behalf. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

Accessing and updating personal information

When you use Google services, we make good faith efforts to provide you with access to your personal information and either to correct this data if it is inaccurate or to delete such data at your request if it is not otherwise required to be retained by law or for legitimate business purposes. We ask individual users to identify themselves and the information requested to be accessed, corrected or removed before processing such requests, and we may decline to process requests that are unreasonably repetitive or systematic, require disproportionate technical effort, jeopardize the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes), or for which access is not otherwise required. In any case where we provide information access and correction, we perform this service free of charge, except if doing so would require a disproportionate effort. Because of the way we maintain certain services, after you delete your information, residual copies may take a period of time before they are deleted from our active servers and may remain in our backup systems. Please review the service Help Centers for more information.

Enforcement

Google adheres to the US Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement, and is registered with the U.S. Department of Commerce's Safe Harbor Program.

Google regularly reviews its compliance with this Privacy Policy. When we receive formal written complaints, it is Google's policy to contact the complaining user regarding his or her concerns. We will cooperate with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that cannot be resolved between Google and an individual.

Changes to this Privacy Policy

Please note that this Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any Privacy Policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

Appendix B: Student Consent Form

Memorial Google Apps for Education – User Consent

Memorial University is going Google – and you are invited. As a student at Memorial, you are entitled to a @mun.ca email address which is the sole address to be used for official university e-mail communication. This document describes a choice of moving from the existing student e-mail service to a Memorial branded version of Gmail and associated Google Apps for Education.

Option to stay with the current Memorial email system

You are not obliged to use Google Apps for Education. The University has evaluated Google Apps and does not believe that it raises a risk to users. However, we recognize that you may feel differently and we provide you with the option of maintaining your current Memorial University student e-mail account.

Privacy and confidentiality

By moving to Google Apps for Education, there are details related to your privacy and confidentiality which we would like to tell you about:

- Your data will be stored in Google's secure network of data centers.
- As with many Internet-based services (Facebook, Twitter, Hotmail, etc.), there is no certainty as to where data may be located and, therefore, your data may be subject to the laws of the hosting country.
- Google provides secure encrypted access to all services
- Our contract states that Google has no rights to student data
- The university will not enable offerings of non-Google apps products to the university or to you directly, since non-Google apps products may introduce security risks.
- For account setup purposes, it is necessary to store your Memorial username and password at Google; however it will only be stored in a highly encrypted manner which makes the possibility of loss remote.

By providing your consent and proceeding with a transfer of your Memorial email services to Google Apps for Education, you acknowledge that:

- Google has the ability to request the suspension of any user that is in violation of the Google Terms of Use. In the event of such a request, the University will defend a user's right to use Google Apps for Education in a manner that does not violate University policy, federal or provincial legislation, or relevant provisions of University Collective Agreements. Users should familiarize themselves with applicable policies, including Memorial's Appropriate Use of Computing Resources Policy.

- Memorial University and Google reserve the right under certain circumstances to terminate the Google Apps for Education agreement and services. In the event of a decision to terminate, or a decision by Memorial to provide an alternative email service, all user accounts and existing data will be preserved and transitioned to an alternate service.

- In the event of a material change to the Google Apps service, or in the implementation or expansion of new functionality, all users will be notified and provided with details of such change.

- The University cannot and does not guarantee protection against possible disclosure by Google including to a foreign authority as a consequence of foreign laws.

- The University will have the ability to access, monitor, use or disclose data available to users of Google Apps for Education. This ability is not different from what exists currently at Memorial with respect to email. The University may be required by law to provide access to information and, under certain circumstances, the University reserves the right to access user data to support the legitimate operations of the University. In such cases, University policies and procedures will be followed, specifically the Appropriate Use of Computing Resources Policy, the Procedure for Requesting Access by Non-Account Holder and the Information Request Policy. The privacy of all personal information not pertinent to the issue giving rise to the access will be protected to such an extent as reasonably possible.

- You will not (a) sell, resell, lease, or the functional equivalent, the services provided by Google to a third party; (b) attempt to reverse engineer the services or any component; (c) attempt to create a substitute or similar service through use of, or access to, the services provided by Google; (d) use the services for high risk activities; or (e) use the services to store or transfer information that is controlled for export under Export Control laws.

Comment [A4]: Before agreeing to the consent form (and starting the conversion process) it was suggested that a statement be added to the effect of "I recognize that my account would be subject to Google's policies outlined below" and also to move the related documents above the "I agree". I have made these changes, and am taking one last run through the form to refine it's content. When complete, I will send along for your review, and it can replace this version in the PIA.

If you have any questions, concerns, or would like further information before making a decision, please contact the Computing and Communications Service Desk by:

Phone: 864-4595
Email: help@mun.ca
In Person: By visiting the counter service at Henrietta Harvey, HH2012
Online request: You can submit an online request by using this form

By checking the "I Agree" box below, I certify that I have read the user terms above and that I consent to transfer my current Memorial e-mail account, including all current e-mail, to Google Apps for Education.

☐

I Agree

Submit

Related University Policies:

Appropriate Use of Computing Resources Policy

Electronic Data Security Policy

Information Request Policy

Privacy Policy

Single Email for Students and Employees Policy

Related Documents:

Google's Privacy Policy

Google Apps for Education Terms

Appendix C: Pilot Opt-out Form

Google Apps for Education Pilot

You are invited to join a Pilot Project, which Memorial's Computing and Communications is conducting, to determine how well Google Applications for Education (e-mail, calendaring, document collaboration etc.) will serve your needs. The pilot will operate from May 2011 to August 2011 and all Term 4 Commerce Students are invited to participate. We are excited about this pilot as you will experience:

- A much larger storage quota (7.5+ gigabytes of storage – greater than 35x what Memorial currently provides to students)
- The ability to create, and collaborate on, documents, presentations, and spreadsheets
- A full featured calendar
- Integrated chat and video conferencing
- No advertising
- No change to your current email address or password
- The transfer of all of your current email to your new account

You may be interested to know that many universities in Canada are either conducting similar pilots or have already moved their e-mail to Google or Microsoft. To date the results have been very positive, and we expect the same for our pilot.

During the pilot, we do not believe that there is risk to your data or confidentiality, however we want to inform you that:

- Memorial will own all of the data, not Google.
- Your data will be stored in Google's secure network of data centers.
- As with many internet-based services (Facebook, Twitter, Hotmail, etc.) there is no certainty as to where these data centers may be located, and therefore your data may be subject to the laws of the hosting country.
- Such laws are similar to those that exist in Canada, however, the University cannot and does not guarantee protection against possible disclosure including, without limitation, to a foreign authority as a consequence of foreign laws.
- When checking email, Google provides a secure connection from your web browser and/or email client. This encrypts the data between you and Google's servers while you view it or collect mail. This is the same system that banks use to secure your connection for online banking.
- It may be necessary (not yet determined) to store your Memorial username and password at Google. If that is the case this data will only be stored in a highly encrypted manner which makes the possibility of loss remote.

We do not think that this raises a risk for you, however, recognizing that you may feel differently, we would like to provide you with the opportunity to "Opt-out" of the pilot project and maintain your current Memorial University student e-mail account.

If you would like to opt out of this Pilot Project, please sign the form below and return it to the Computing and Communications Service Desk, Henrietta Harvey (HH) 2012, or fax it to 864-3514, by May 1, 2011.

If you have any questions, or you would like to discuss any aspect of the Pilot, please contact:

Albert Norman
Google Apps for Education, Project Lead
Computing and Communications
Phone: 864-3992
Email: anorman@mun.ca

By completing and signing the below form, I certify that I **do not** want to participate in the Google Apps for Education pilot project. Please print clearly.

Full Name: _____

MUN Email Address: _____

Signature: _____ Date: _____

Appendix D: Survey Questionnaire – Pilot Project

Note: The following survey questionnaire was delivered to students participating in the Google Apps pilot project as a web-based form.

Google Apps Pilot Survey

As you have been a Google Apps user since the beginning of the semester, an important aspect of the pilot project is to capture your feedback. This feedback will be used to measure the elements of Google Apps that have been successful, and those that may need further exploration. The following survey will provide the pilot team with valuable information that cannot be captured from any other source. Your feedback will be very important to future phases of the project, as the decision to offer Google Apps to other students on campus will be made based on your experience, and on your feedback. If you experience any issues with the survey, or have any questions, please contact the Computing and Communications Service Desk by phone (864-4595) or email (help@mun.ca).

1. Prior to participating in the pilot, which of the following Google Apps had you had any previous experience with? [check all that apply]

- ☐ Gmail
- ☐ Calendar
- ☐ Sites
- ☐ Docs
- ☐ Talk / Chat
- ☐ Other: _____

2. At the start of the pilot, how satisfied were you with the transition from your "old" Memorial email account to your Memorial Google Apps account?

- o Very Dissatisfied
- o Dissatisfied
- o Neutral
- o Satisfied
- o Very Satisfied

3. How often did you use the following Google Apps during the pilot?

	Never	Less than once/month	Monthly	Weekly	Daily
Gmail	O	O	O	O	O
Calendar	O	O	O	O	O
Docs	O	O	O	O	O
Sites	O	O	O	O	O
Talk / Chat	O	O	O	O	O
Video Chat	O	O	O	O	O

4. What support resources have you used for help or assistance with Google Apps during the pilot? Please rate your experience on those that apply.

	Very Dissatisfied	Dissatisfied	Satisfied	Very Satisfied	Did Not Use
Pilot provided documentation / resources (e.g., FAQs, Specific Mobile setup instructions)	○	○	○	○	○
Computing and Communications Service Desk (e.g., help@mun.ca, counter service, 864-4595)	○	○	○	○	○
Google's official help pages	○	○	○	○	○
Business Faculty Computing Staff / IT Support	○	○	○	○	○
Web search (e.g. Using Google, Yahoo!, Bing, etc.)	○	○	○	○	○

If you used other support resources not included above, please specify:

5. Throughout your use of Google Apps during the pilot, how would you describe your ability to learn the following apps:

	Very Difficult	Difficult	Neutral	Easy	Very Easy
Gmail	○	○	○	○	○
Calendar	○	○	○	○	○
Docs	○	○	○	○	○
Sites	○	○	○	○	○
Talk / Chat	○	○	○	○	○
Overall	○	○	○	○	○

6. To what level did Google Apps affect your ability to effectively communicate?

- o Impaired Greatly
- o Impaired Somewhat
- o Neutral
- o Enhanced Somewhat
- o Enhanced Greatly

7. The collaboration tools offered by Google Apps for Education have the potential to enrich my learning experience.

- o Disagree
- o Somewhat Disagree
- o Neither Agree nor Disagree
- o Somewhat Agree
- o Agree

8. Do you have any concerns with respect to privacy?

- o Yes
- o No

If "Yes", please explain:

_____
_____
_____
_____
_____

9. Prior to the pilot I checked my Memorial email by using [check all that apply]:

- ☐ Memorial webmail (webmail.mun.ca)
- ☐ Email Client (e.g., Microsoft Outlook, Mozilla Thunderbird)
- ☐ Mobile Device (e.g., iPhone, Blackberry, Android)
- ☐ Other: _____

10. During the Google Apps pilot I checked my Memorial email by using [check all that apply]:

- ☐ Memorial Gmail Web Interface (e.g. through my.mun.ca)
- ☐ Email Client (e.g., Microsoft Outlook, Mozilla Thunderbird)
- ☐ Mobile Device (e.g., iPhone, Blackberry, Android)
- ☐ Other: _____

11. During the pilot, if you configured a mobile device to access your Memorial Google Apps account, which of the following did you use? [check all that apply]
If you did not configure a mobile device, please skip this question.

- ☐ iPhone

- Blackberry
- Android
- Windows 7 Phone
- Other: _____

12. Would you have availed of training sessions for any of the Google Apps?

	Yes	No
Gmail	○	○
Calendar	○	○
Docs	○	○
Sites	○	○
Chat / Talk	○	○

13. How satisfied are you with Memorial's Google Apps for Education?

	Very Dissatisfied	Dissatisfied	Satisfied	Very Satisfied	Did Not Use
Gmail	○	○	○	○	○
Calendar	○	○	○	○	○
Docs	○	○	○	○	○
Sites	○	○	○	○	○
Talk / Chat	○	○	○	○	○
Overall	○	○	○	○	○

14. Based on my overall pilot experience, I would recommend Google Apps for Education to other Memorial students.

- No
- Neutral
- Yes, with reservations
- Yes

15. Is there anything else we should know about your experience using Memorial's Google Apps?

_____
_____
_____
_____
_____

Appendix E: Privacy Compliance Checklist