Deloitte.

University of Ottawa

Cloud Computing Initiative Privacy Impact Assessment (PIA)

FINAL Report – Technical Implementation
June 2013

Document Change Control

Version	Date	Description	Author
FINAL Report – Conceptual Solution	September 2012	Initial PIA completed on the conceptual solution of the Cloud Computing Initiative	Deloitte
FINAL Report – Technical Implementation	June 2013	Final PIA Report of the technical implementation of the Cloud Computing Initiative	Deloitte

Executive Summary

The University of Ottawa (uOttawa) is the largest bilingual university in North America and a top 10 research university in Canada. The university has over 40,000 registered students; 5,000 professors and support staff; and 160,000 alumni. In the fall of 2009, the Chief Technology Officer (CTO) office began a review of using 'Software as a Service' (SaaS) for its email, calendaring and office productivity tools for all students. This project was re-assigned to the Student Services team in the fall of 2011. The goal of the 'Cloud Computing Initiative' is primarily to enhance student experience, but has the added benefit of achieving cost optimizations in operating and capital expenses, improving efficiencies, and enabling business continuity for those services. The Initiative replaces uOttawa's Squirrel Mail by a new 'cloud' e-mail service provided by Google (i.e., Google Apps for Education). uOttawa signed an agreement with Google (*Google Apps for Education Agreement* and a related *Addendum*) on October 4, 2012.

The objective of the Privacy Impact Assessment (PIA) was to perform a privacy risk assessment and recommend any remediation measures required to help ensure the protection of personal information in accordance with uOttawa privacy requirements and leading practices in relation to the Cloud Computing Initiative. The scope of the PIA was limited to the collection, use, disclosure, and retention of personal information by uOttawa in relation to the Cloud Computing Initiative, specifically the use of Google Apps for Education email for uOttawa students, as well as calendar, contacts and GoogleTalk. An initial PIA completed on the conceptual solution was completed in September 2012. This is an update to the initial PIA, in order to determine if additional privacy risks have been introduced, or if previously identified risks have been mitigated now that the technical solution has been completed.

uOttawa is subject to Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA), and must ensure personal information is managed in accordance with the requirements of FIPPA. As FIPPA does not apply to private sector service providers such as Google, the most effective means to require that an outside service provider respects the statutory requirements of FIPPA is to ensure there are relevant privacy clauses in any contractual agreement between uOttawa and Google. However, Google is subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) in its dealings with uOttawa. A noted privacy concern in recent years related to a Canadian organization's utilization of service providers with operations outside of Canada is that an organization's personal information may be subject to the laws of the country where such information is stored. For example, some groups have expressed concern over the ability of American law enforcement officials to potentially access personal information on Canadians without a search warrant under the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USA PATRIOT Act). Although some of the actual risks may be overstated[1], alleviating these concerns will be a key communications challenge that uOttawa will need to address throughout the Cloud Computing Initiative.

The PIA included a detailed review of the standard *Google Apps for Education Agreement* and its related *Addendum* and has noted areas of potential risk related to the current agreement clauses. It is important to recognize the identified risks described in the table below relate to the potential implementation of the Cloud Computing Initiative and, as such, do not necessarily reflect current risks related to the privacy and

[1] It should be noted that given that Canadian search and seizure laws are fairly similar to United States law (to the extent of the powers provided to government), the close collaboration and ongoing sharing of information between Canadian and US agencies, and the ability of Canadian authorities to obtain warrants for US authorities through mechanisms such as mutual legal assistance treaties, it is possible that data managed in Canada by a Canadian company could in theory end up in the hands of US authorities, which highlights that an agreement with any service provider, regardless of location, should consider the privacy risks/implications of the relationship, and that a transfer of data across borders should not necessarily cause grave concern in and of itself.

personal information management practices of uOttawa. The overall risk rating was determined based on two factors: 1) the probability that an adverse event could occur; and 2) the impact on uOttawa should an adverse event occur (e.g., a data breach). Refer to **Appendix A** for more information on the risk rating methodology. The goal of privacy risk management is to maintain privacy risks within acceptable bounds. The higher ratings provide an indication of priority areas for implementing suggested risk mitigation mechanisms.

uOttawa has been proactive in its consideration of privacy and ensured privacy was embedded into the implementation of the initiative. To this extent, one moderate risk related to the initiative has been identified.

#	Risk	Risk Level	Recommendation
1	Based on the information gathering done as part of this PIA, there appears to be a risk that uOttawa staff and faculty are sending emails to students that contain personal information, and given the potential sensitivities related to the use of Google as a service provider, uOttawa should ensure faculties and administrative units review their email practices. *Refer to Section 3.7*	**Moderate**	uOttawa should ensure faculties and administrative units review their email practices. As uOttawa works toward developing a formal email policy, consider items such as: - For personal information that is not particularly sensitive, uOttawa may want administration and faculty to ensure that consent has been obtained from the student for its communication through email. - For more sensitive personal information, uOttawa may want administration and faculty to ensure these data elements are not communicated through email unless they have been appropriately encrypted.

Although not identified as a specific risk, there is always an element of risk in managing a service provider, and uOttawa should ensure there remain designated contact individuals at uOttawa and Google to actively manage the relationship around such matters as:

- Breach identification and response;
- Review and discussion on the audits conducted by Google related to security and privacy[2]; and,
- Changes to Google Acceptable Use Policy, Privacy Notice, and other related Terms of Service.

Once the final PIA report has been prepared, uOttawa should consider these next steps:

- Develop an action plan to address the risk outlined in the PIA (including the responsible party, the action to be taken, and the timeframe for the action). The PIA is intended to be an evolving risk management tool, to be revisited and updated as required based on changes to the organization;
- Consult with the Office of the Information and Privacy Commissioner of Ontario as required.

[2] Section 2c of the addendum to the agreement includes the following clause on audits: "*During the Term, Google will maintain its Standard for Attestation Engagement No. 16 audit report or a comparable report ("Audit Report") and will update the Audit Report at least every eighteen (18) months. On Customer's written request during the Term, Google will provide Customer a copy of such Audit Report in accordance with Google's policy as to the distribution thereof (including that such Audit Report must be returned or destroyed within 10 days of receipt and no copies of the report may be made).*" The Standard for Attestation Engagements No. 16, is an attestation standard issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and is an attestation standard intended for service organizations for purposes of reporting on the design of controls and their operating effectiveness.

The PIA is intended to be a 'living document' that should be updated throughout the project as the solution evolves.

1 Introduction

1.1 Background

The University of Ottawa (uOttawa) is the largest bilingual university in North America and a top 10 research university in Canada. The university has over 40,000 registered students; 5,000 professors and support staff; and 160,000 alumni. In the fall of 2009, the Chief Technology Officer (CTO) office began a review of using 'Software as a Service' (SaaS) for its email, calendaring and office productivity tools for all students. This project was re-assigned to the Student Services team in the fall of 2011.

The goal of the 'Cloud Computing Initiative' is primarily to enhance student experience, but has the added benefit of achieving cost optimizations in operating and capital expenses, improving efficiencies, and enabling business continuity for those services. The Initiative replaces uOttawa's Squirrel Mail by a new 'cloud' e-mail service provided by Google (i.e., Google Apps for Education). uOttawa signed an agreement with Google (Google Apps for Education Agreement and a related Addendum) on October 4, 2012.

A small group of early adopters has already begun utilizing the Google Apps solution. Starting mid-May, all new students (those enrolled for September 2013) will receive a uOttawa email address that utilizes Google Apps.

1.2 Objective and Scope

The objective of the Privacy Impact Assessment (PIA) was to perform a privacy risk assessment and recommend any remediation measures required to help ensure the protection of personal information in accordance with uOttawa privacy requirements and leading practices in relation to the Cloud Computing Initiative. The scope of the PIA was limited to the collection, use, disclosure, and retention of personal information by uOttawa in relation to the Cloud Computing Initiative, specifically the use of Google Apps for Education email for uOttawa students, as well as calendar, contacts and GoogleTalk. An initial PIA completed on the conceptual solution was completed in September 2012. This is an update to the initial PIA, in order to determine if additional privacy risks have been introduced, or if previously identified risks have been mitigated now that the technical implementation was completed.

The PIA identified privacy risks associated with the above services being offered. The assessment identified the risks based on probability and impact to the organization (rated as high, moderate or low). The PIA references the clauses within the *Google Apps for Education Agreement* and its related *Addendum* signed on October 4, 2012.

1.3 Approach

The PIA approach and methodology used for this report builds from, and is consistent, with the PIA guidelines articulated at the federal and Ontario public sector level. The analysis of privacy risks was based both on the University's requirements under Ontario's Freedom of Information and Protection of Privacy Act (FIPPA), as well as the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information* (*the Model Code*), which has become a *de facto* standard for the consideration of privacy issues centered around ten privacy principles. The analysis was also consistent with the principles outlined in the Privacy by Design (PbD) approach, as promoted by the Information and Privacy Commissioner (IPC)/Ontario.

The PIA relies on information gathering from uOttawa stakeholders, through interviews and document review (refer to **Appendix C** and **D**) and does not constitute legal opinion. The PIA is intended for uOttawa management in helping management in their privacy compliance responsibilities.

1.4 Privacy Requirements

For Ontario public sector institutions such as uOttawa, **personal information** is very broadly defined as, " information about an identifiable individual", for example, an individual's name and contact information, or more sensitive information such as financial and medical history. uOttawa is subject to the requirements of FIPPA related to privacy and the management of personal information. The IPC/Ontario describes **privacy** as "... *having the ability to control or influence the way in which information about you is collected, used and disclosed*". Leading privacy practices frameworks have also been consulted as part of the privacy analysis of this PIA (e.g. the Privacy by Design (PbD) foundational principles and the Generally Accepted Privacy Principles (GAPP) published by the Canadian Institute of Chartered Accountants (CICA)).

A list of all relevant legislation, other requirements, guidance documents, and leading practice frameworks is provided in **Appendix C**.

2 Business Model and Data Flow Analysis

2.1 Overview of Previous Email System

University policy requires that email from university administration and faculty must be sent to an official uOttawa email address (@uottawa.ca). Students are able to redirect their uOttawa email to another email address; currently 38% of students do this.

Information on students is originally provided to uOttawa from the Ontario Universities' Application Centre (OUAC), and is entered in the uOttawa Student Information System (SIS), the university's principal tool for the support of academic administration, and a digital identity (user ID and password) is created for him/her based on the information in SIS. When a student becomes a registrant (has registered for his/her first class), a uOttawa email account is created. The creation of the digital identity is controlled by CAMS, uOttawa's in house developed identity management system. Although there is an expiry field associated with the digital identity within CAMS, there is currently no automated account management process that updates the field for students. The student is informed of the user ID and password via an email to the email address that was associated with the student prior to being registered (the student's personal email obtained from OUAC). This student's email address is stored in the SIS and is sent to Talisma, uOttawa's CRM system.

Email users are required to adhere to the uOttawa *User Code of Conduct*, which is provided in **Appendix E**[3].

Students log in to their email through a login webpage[4], refer to Figure 1, or connect through the authenticated student portal, uoZone[5].

---

[3] The User Code of Conduct is also available at: www.ccs.uottawa.ca/about/policies/code.html

[4] Webmail access is available at: https://web.uottawa.ca/email/.

[5] uoZone is available at: www.uozone.uottawa.ca.

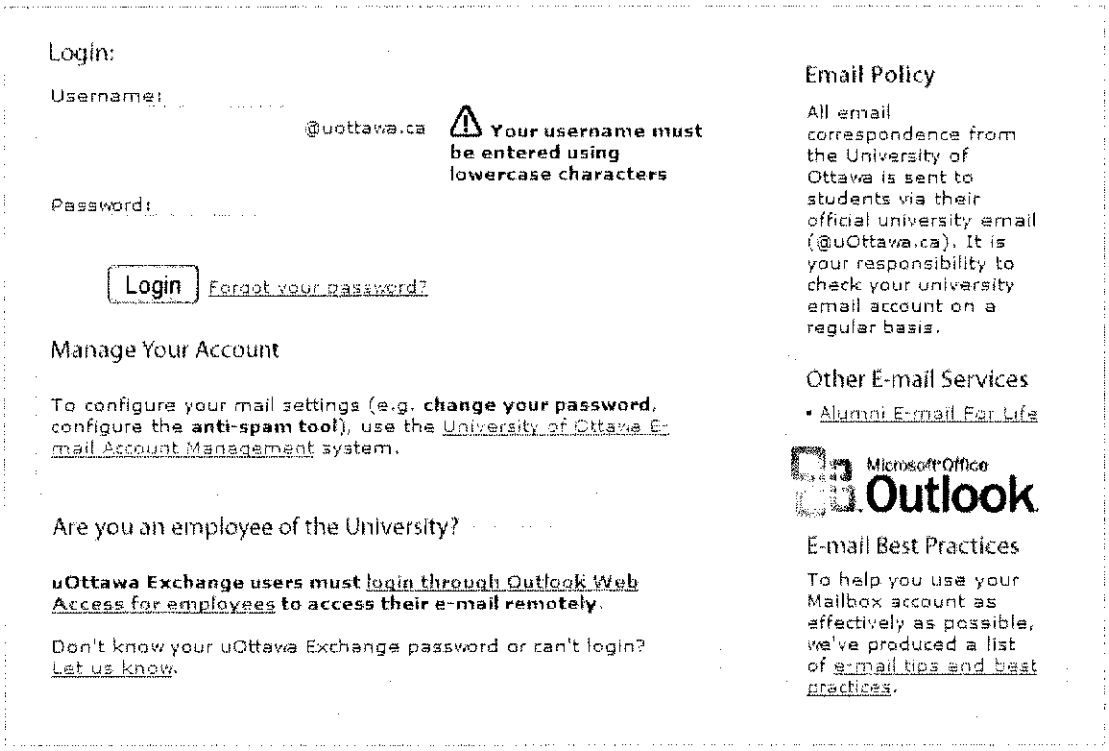

Figure 1: Email Login Page

The login webpage includes a link to *Email tips and best practices*[6], which includes guidance such as "*Don't put confidential, personal or emotional content when replying to an email*", and below the section on email tips and best practices is a *Netiquette* section, which states, "*Don't rely on the privacy of email, especially from work, but respect the privacy of others.*"

From the login webpage there is also a link to uOttawa's Privacy Policy[7].

The link to the account management webpage (refer to Figure 2) allows users to do a variety of actions with their email account as outlined in Figure 3.

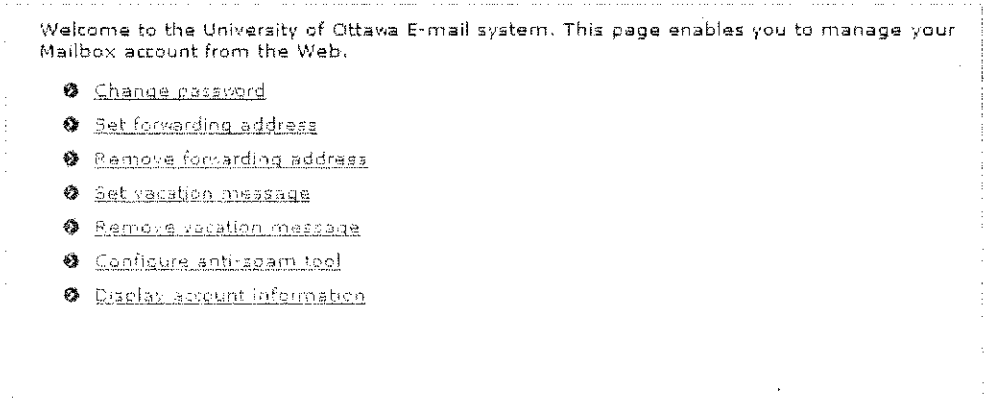

Figure 2: Account Management Webpage

[6] uOttawa's email tips and best practices is available at: www.ccs.uottawa.ca/email/overview.html#tips

[7] uOttawa's Privacy Policy is available at: http://web5.uottawa.ca/admingov/policy_90.html

Change password	Allows users to change their password, and includes tips for selecting a good password..
Set forwarding address	Allows users to set a forwarding address, and all email sent to the student's uOttawa email account will be redirected to this account..
Remove Forwarding address	Allows users to remove the forwarding address they had set for their uOttawa email account.
Set vacation message	Allows users to set an auto-response message which will be sent out in response to every message that is received.
Remove vacation message	Allows users to remove their auto-response message.
Configure anti-spam tool	Allows users to direct any junk mail that is sent to their Mailbox account away from their Inbox to be erased or stored in a Spam folder. An extra folder will appear where all the spam will be sent.
Display account information	Allows the user to display their account information.

Figure 3: Users Email Account Management

2.2 Proposed Email Solution

uOttawa has moved towards a single sign on solution, and students sign in to the new email service through the authenticated student portal (uoZone).

For existing students, the Google Apps solution will be available when their name is added to the appropriate active directory (AD) group by CCS (currently this is a small number of early adopters). For these students the introduction to Google Apps link will be visible when they sign in through the student portal (uoZone).

Students may choose to opt-in or opt-out of the service (refer to Figure 4).

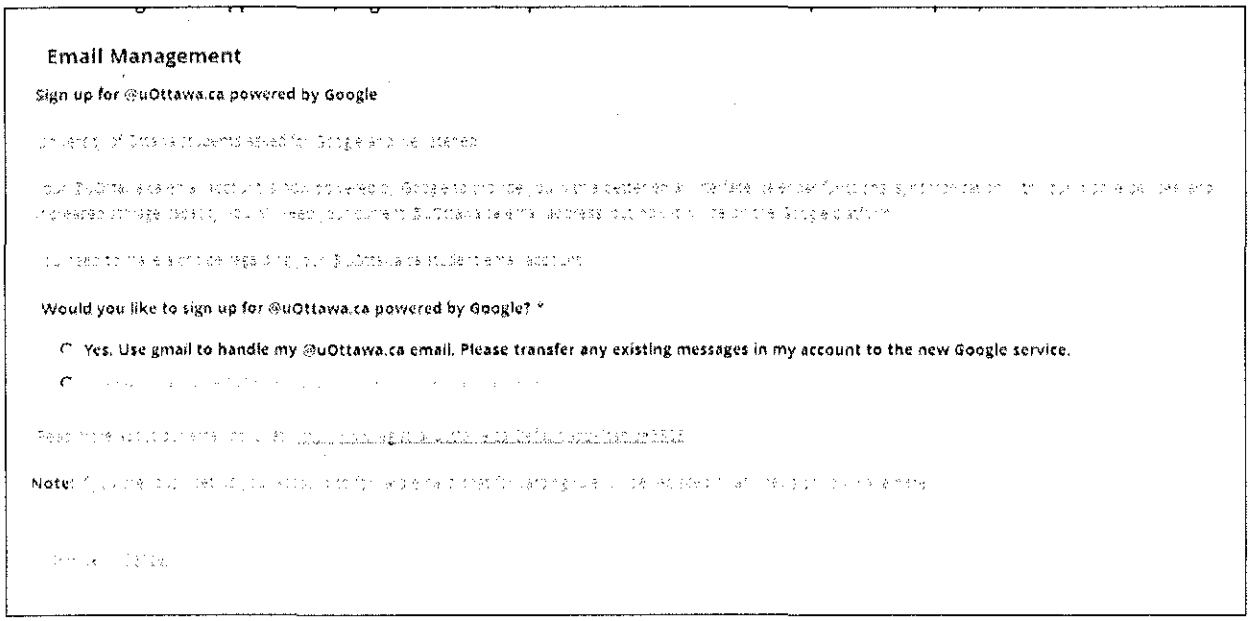

Figure 4: Opt-in / Out-out Screen

For students that opt-in (refer to Figure 5), they must agree to the Terms of Service (refer to **Appendix E**) and set their password. The new strong password requirements set by uOttawa are:

- Minimum of eight characters;
- One special character (&,%,$, etc); and,
- One capital and one lowercase letter.

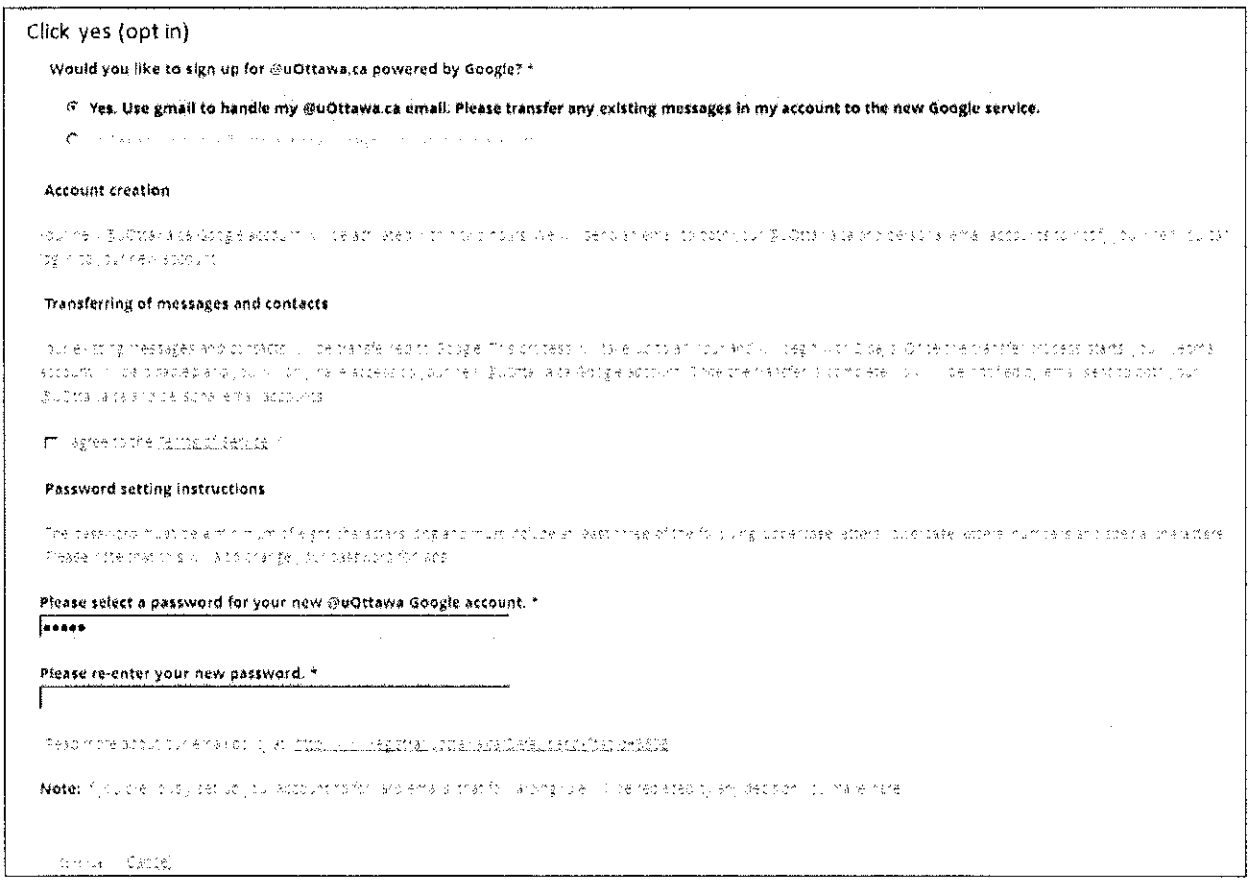

Figure 5: Opt In Screen

A Google account is then created for the student. Through the utilization of the Google Apps Directory Sync (GADS), the information uOttawa provides to Google for the provisioning of email accounts is limited to username, first name, and last name. GADS performs a one-way synchronization of the uOttawa Google Apps user accounts to match the user data in the uOttawa LDAP server.

Activation of the students account may take up to 24 hours. Once activation is complete, the student will receive an email in their personal email inbox and in their @uOttawa.ca Google account inbox with instructions on how to access their @uOttawa.ca Google account. From this point on, all emails sent to the students @uOttawa.ca address will appear in the new @uOttawa.ca Google account Inbox.

Once the student's Google account is activated, they will enter the queue to have their old Webmail account email and contacts transferred to their new @uOttawa.ca Google account. Once the transfer is complete, an email will be sent to the student's @uOttawa.ca Google account and to their personal email account to confirm that the transfer has been successful.

If a student opts out (refer to Figure 6), they will still have an @uottawa.ca email address but email sent to this address will be forwarded to a separate email address provided by the student through the opt out process. Emails sent to students that opt out will not go through the Google infrastructure but stay within the uOttawa email infrastructure. The uOttawa e-mail servers will send email directed to the university

email address of a student who as opted out to that student's personal email account. For students who initially opt in, they can still opt out at a later time by contacting CCS. If a student opts out, a uOttawa email administrator will need to either disable or delete the student's account. Functionality exists to allow students to first migrate their personal information from their Google email account to another solution before the account is disabled/deleted.

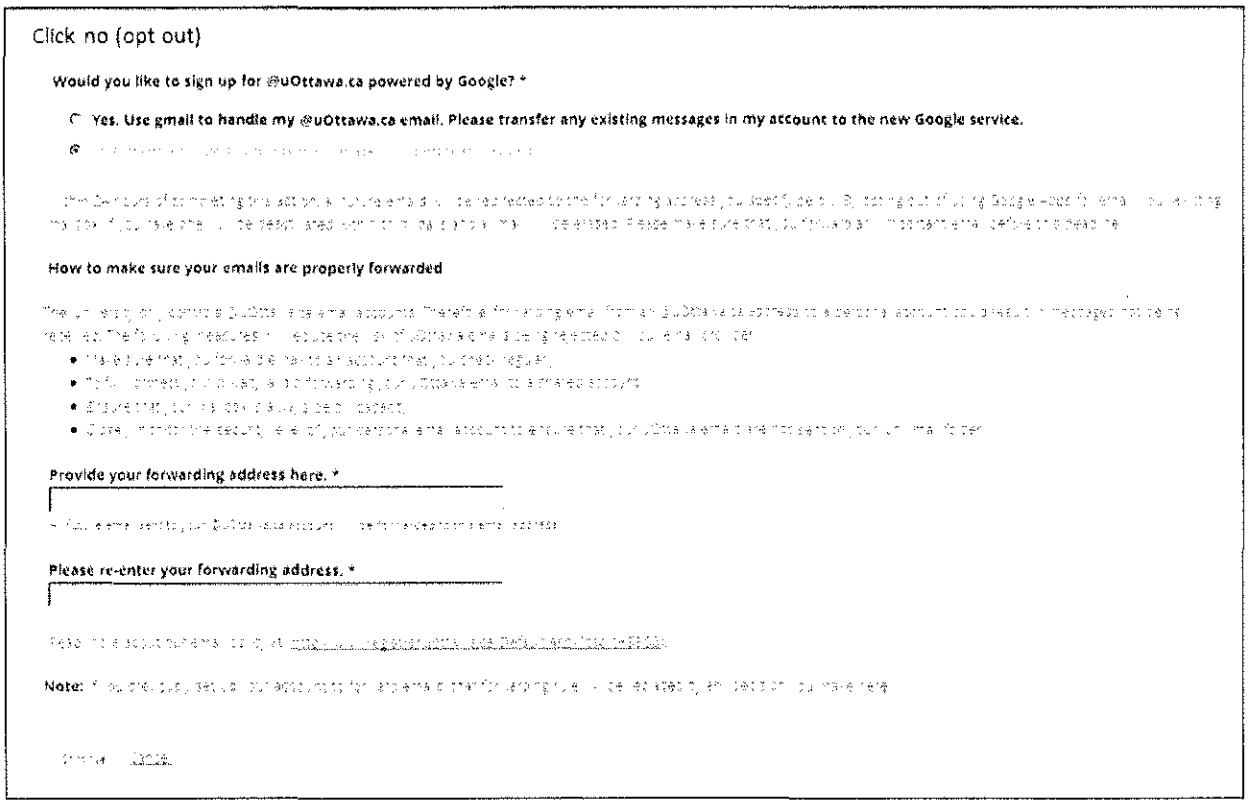

Figure 6: Opt Out Screen

For new students, a student account is created within uOttawa's active directory (AD) when the student registers. The new student will be taken to the same opt in/out screens when they sign in through the student portal.

For either new or existing students, once their email account is activated, students can access their email account through a mobile device by generating a 'Google Token', which students can do through the uoZone student portal. The token is a 16-character string of letters and numbers. The token is not stored by uOttawa.

Students will not be able to use their uOttawa email account to sign into Google's non-core services (e.g., YouTube, Google Plus, etc.) in the initial implementation. Google does not have an automated process in place to deactivate a user's account after they graduate, nor do they have a mechanism to track when someone graduates.

2.2.1 Collection and Use of Personal Information

The information uOttawa will need to provide to Google for the provisioning of email accounts is limited to username, first name, and last name. uOttawa will not be collecting additional personal information from students as part of the proposed new email solution. Students that opt out will need to provide a personal email address to which their university email will be forwarded. Note that 38% of students under the current email system already have their university email forwarded to a personal mail account.

Existing students will have the contents of current their email accounts migrated to their new Google email accounts upon activation of their Google account (the student would be able to first delete any content in their current account they did not want migrated). Note that as Google is acting as a service provider to uOttawa, and the agreement indicates ownership of the email contents remains with uOttawa, the provision of information from uOttawa to Google is considered a use of the personal information as opposed to either a disclosure by uOttawa to Google (or alternatively a collection by Google from uOttawa).

Currently there are email accounts (postmaster@uottawa.ca, spamabuse@uottawa.ca, abuse@uottawa.ca and antivirus@uottawa.ca) which are monitored by uOttawa's email administrator. These accounts would continue to be monitored by the uOttawa email administrator under the proposed email solution; however, all email sent to the addresses abuse@uottawa.ca and postmaster@uottawa.ca, will also be monitored by Google, in order to, as indicated by Google "*properly address all reports of spam, abuse, and technical issues*".

Google has indicated that there will be no advertising or secondary use of data by Google (for example data mining) related to current uOttawa student accounts.

Through the Google Apps Admin Console, administrator privileges can be defined in several ways for uOttawa email administrators and other IT staff. uOttawa expects that current roles/access will be similar under the proposed email solution to the current email solution. uOttawa will also be able to suspend or delete student email accounts at any point in time through the Admin Console.

Although Google indicates it will not as a regular function of its services access the contents of uOttawa email, Google will scan email content for purposes such as spam filtering, anti-virus protection, or malware detection.

2.2.2 Disclosure of Personal Information

uOttawa indicates that it does not anticipate any new disclosures of personal information as a result of the proposed email solution. Of note, disclosures by uOttawa or Google may occur as required by law.

2.2.3 Retention and Disposition of Personal Information

uOttawa email administrators are able to purge trash folders and spam folders in order to free up space, but do not have the ability to set any additional retention policies different than the default Google settings. Messages in the trash folder are deleted permanently after 30 day. If a user has deleted a message permanently, by clicking 'delete forever' in the spam or trash folder, or through uOttawa's domain email retention policies, it is not possible to recover the message. It is also impossible to recover messages after an administrator deletes a user's account. uOttawa has not retained Google's vault service (backups of data), but users could decide to use this service on their own (although Google would charge a fee).

uOttawa may terminate its agreement with Google with 30 days prior written notice. Google indicates that if uOttawa decides to discontinue its use of Google Apps, that there are several options for the migration of uOttawa's email data to another solution. uOttawa has not yet determined for what period of time Google would retain uOttawa data after the expiration of its agreement with Google; however, Google does indicate that data would be overwritten within a "commercially reasonable period of time"

2.3 Description of Personal Information

This section summarizes the collection, use, disclosure, storage and retention of personal information managed.

Personal Information (e.g. name, address, SIN number)	Collected by	Type of Format	Purpose of Collection	Used by	Disclosed to	Storage, Retention and Disposal
Username, first name, last name, and alias[8]	Google via uOttawa	Electronic	Provisioning of Email Accounts	uOttawa Google	-	uOttawa – retained for the life of the account Google – until requested to be removed by user
Mobile account password (terms a token)	Google	Electronic	To allow student to use mobile services	Google	-	Google - until requested to be removed by user
Contents of Email (for opt in students)	Google via uOttawa	Electronic	Administration of Email	Not specifically used by Google	-	Google - until requested to be removed by user
Content of Email (for opt out student)	*Email is directed to a third party email address provided by the student*					

2.4 Sensitivity of Personal Information

uOttawa indicates that there is potentially sensitive personal information that is transmitted and received by student e-mail accounts, although uOttawa can only control what it specifically sends to students. This may include information about a student's financial aid, housing, or replies to a student's inquiries to uOttawa administration or faculty on a variety of matters.

[8] If a student has chosen a Full Name Email Address (these are cosmetic but point to the original email they were assigned), uOttawa will have a process to identify to Google that both email addresses are for the same contact

3 Privacy Compliance Analysis

3.1 Accountability

Privacy Principle:

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with privacy requirements.

This section references the clauses within the standard *Google Apps for Education Agreement* and its related *Addendum* signed October 4, 2012. The use of Google as a service provider will include the cross-border transfer of uOttawa data, as Google indicates that the data will be processes in the "United States or any other country".

uOttawa is subject to FIPPA, and must ensure information is managed in accordance with the requirements of FIPPA. As FIPPA does not apply to private sector service providers such as Google, the most effective means to require that an outside service provider respects the statutory requirements of FIPPA is to ensure there are relevant privacy clauses in any contractual agreement between uOttawa and Google.

A noted privacy concern in recent years related to a Canadian organization's utilization of service providers with operations outside of Canada is that the organization's information will be subject to the laws of the country where it is stored or accessible from, including expansive and covert search and seizure laws, such as the *USA PATRIOT Act*. Although some of the actual risks may be overstated, alleviating these concerns will be a key communications challenge that uOttawa will need to address throughout this initiative. It should be noted that given that Canadian search and seizure laws are fairly similar to United States law (to the extent of the powers provided to government), the close collaboration and ongoing sharing of information between Canadian and US agencies, and the ability of Canadian authorities to obtain warrants for US authorities through mechanisms such as mutual legal assistance treaties, it is possible that data managed in Canada by a Canadian company could in theory end up in the hands of US authorities, which highlights that an agreement with any service provider, regardless of location, should consider the privacy risks/implications of the relationship, and that a transfer of data across borders should not necessarily cause grave concern in and of itself.

A review of the current agreement and addendum includes several important clauses related to third party request notification, audit, security, breach notification, and other considerations. Risks have been identified related to adherence to FIPPA requirements and the retention of personal information. The table below provides an overview of the privacy-related clauses that uOttawa should include in any agreement involving the management of personal information by a third party service provider, as well as a comparison to the language in the agreement and addendum.

Ownership Ensure Google acknowledges that the personal information is the intellectual property of uOttawa	The *Google Apps for Education Agreement* indicates that ownership of the email contents remains with uOttawa. Section 8.1 of the agreement indicates that "*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*".

FIPPA Requirements Ensure Google acknowledges it will manage information in a manner that is consistent with the requirements of FIPPA.	Ideally there would be a clause that indicates the use and management of personal information by Google would be consistent with the requirements of FIPPA. Although such a clause is not present, there is language in section 10.1 and 7.1 of the agreement that satisfies these concerns. Section 10.1 of the agreement indicates that "*Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law).*" . Section 7.1 of the agreement indicates that "*Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates, employees and agents in violation of this Section.*"
Disclosure to Authorities Ensure that if Google is compelled to disclose personal information for the purpose of complying with a subpoena or warrant, the service provider notifies uOttawa before this disclosure occurs.	Section 7.3 of the agreement indicates that "*Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.*
Security Ensure Google has implemented and will maintain robust security standards.	The addendum to the agreement, includes 'Attachment A', which outlines Google Apps Security Standards, including those related to data center and network security, access and site controls, and data.
Breach Notification Ensure Google promptly notifies uOttawa of breaches that potentially affect the confidentiality or integrity of uOttawa data.	Section 2d of the addendum to the agreement indicates: "*Security Breach Notification. 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.*" uOttawa should ensure there remain designated contact individuals at uOttawa and Google to actively manage the relationship around such matters as breach identification and response.
Audit Ensure Google independently assesses its privacy and security on a regular basis, and the results of an	Section 2c of the addendum to the agreement includes the following clause on audits: "*During the Term, Google will maintain its Standard for Attestation Engagement No. 16 audit report or a comparable report ("Audit Report") and will update the Audit Report at least every eighteen (18) months. On Customer's*

audit are available to uOttawa.	*written request during the Term, Google will provide Customer a copy of such Audit Report in accordance with Google's policy as to the distribution thereof (including that such Audit Report must be returned or destroyed within 10 days of receipt and no copies of the report may be made).*" The Standard for Attestation Engagements No. 16, is an attestation standard issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and is an attestation standard intended for service organizations for purposes of reporting on the design of controls and their operating effectiveness. uOttawa should ensure a process is in place to receive and review updated audit reports throughout the life of the contract.
Termination and Retention of Data	uOttawa may terminate its agreement with Google with 30 days prior written notice, Section 12.1 of the agreement indicates "*Customer may terminate this Agreement for any reason (or no reason) with thirty days prior written notice to Google.*" Google indicates that if uOttawa decides to discontinue its use of Google Apps, that there are several options for the migration of uOttawa's email data to another solution, Section 10.3 (ii) of agreement indicates "*Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google's then-current rates, if applicable, for the Services*" Google indicates that data would be overwritten within a "commercially reasonable period of time". Section 12.3 (iii) of the agreement indicates that "*after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active servers and overwriting it over time*", and (iv) indicates "*upon request each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party.*" Through discussions between uOttawa and Google, Google indicates that a commercially reasonable period of time means that uOttawa will have adequate time to remove its data. Additionally, Google has an entire team dedicated to moving uOttawa information out of Google Apps (should it choose to do so) called the Data Liberation Front.

3.2 Identifying Purposes

Privacy Principle:

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

FIPPA requires that uOttawa provides appropriate notice to students when it collects personal information that includes (per s. 39(2) of FIPPA):

- the legal authority for the collection;
- the principal purpose or purposes for which the personal information is intended to be used; and,
- the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

Ideally such a notice would be provided at each point where a student can either login or manage their email account. Currently these login and email management pages have a link to uOttawa's Privacy Policy, which does contain the elements outlined above.

uOttawa has developed a comprehensive *Terms of Service* that outlines the management of personal information through the use of the service (refer to **Appendix E**). Furthermore, and as outlined in the *Terms of Service*, the use of uOttawa Google Apps for Education Service is governed by Google's Acceptable Use Policy (refer to **Appendix E**), Privacy Notice, and related Terms of Service.

3.3 Consent

Privacy Principle:

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

All students are able to opt out of using Google email for their university email address. If a student opts out, they will still have an @uottawa.ca email address but email sent to this address will be forwarded to a separate email address provided by the student through the opt out process. Emails sent to students that opt out will not go through the Google infrastructure but stay within the uOttawa email infrastructure. For students who initially opt in, they can still opt out at a later time.

3.4 Limiting Collection of Personal Information

Privacy Principle:

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

uOttawa will not be collecting additional personal information from students as part of the new email solution. Through the utilization of the Google Apps Directory Sync (GADS), the information uOttawa needs to provide to Google for the provisioning of email accounts is limited to username, first name, and last name. GADS performs a one-way synchronization of the uOttawa Google Apps user accounts to match the user data in the uOttawa LDAP server.

Note that as Google is acting as a service provider to uOttawa, and the provision of information from uOttawa to Google is considered a use of the personal information as opposed to a disclosure by uOttawa to Google (or alternatively a collection by Google from uOttawa).

3.5 Limiting Use, Disclosure, and Retention of Personal Information

Privacy Principle

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Although Google indicates it will not as a regular function of its services access the contents of uOttawa email, there are instances where this may potentially occur, specifically:

- Google will scan email content for purposes such as spam filtering, anti-virus protection, or malware detection. To the extent the scans detect a potential threat, it has yet to be determined what Google will do with the email, for instance, if it is captured and further analyzed.
- Currently there are email accounts (postmaster@uottawa.ca, spamabuse@uottawa.ca, abuse@uottawa.ca and antivirus@uottawa.ca) which are monitored by uOttawa's email administrator. These accounts will continue to be monitored by the uOttawa email administrator under the proposed email solution; however, all email sent to the addresses abuse@uottawa.ca and postmaster@uottawa.ca, will also be monitored by Google[9], in order to, as indicated by Google, "*properly address all reports of spam, abuse, and technical issues*".

FIPPA (s.41) allows for the use of personal information for a purpose for which it was obtained or compiled or for a consistent purpose. The scanning of email content for purposes such as spam filtering, anti-virus protection, or malware detection can be considered a consistent or reasonable use of the information, as this is required to provide a reliable and secure email service. FIPPA (s.43) defines a consistent use as a use in which an individual might reasonably have expected.

Through discussions between uOttawa and Google related to the extent Google staff would have access to emails that were identified as virus, spam or abuse emails, Google indicated that: "*Access to the client's data is controlled through authorization and authentication technologies, ensuring that only those specifically authorized to view, update, or delete data can do so. This access must be approved by the appropriate data owner, manager, or other executives, as dictated by Google's security policies. Access rights and levels are based on the employee's job function and role, using the concepts of least-privilege and need-to-know to ensure that access is commensurate with defined responsibilities. Approvals are managed by workflow tools that maintain audit records of all changes.*"

Google has indicated that there will be no advertising or secondary use of data by Google (for example data mining) related to current uOttawa student accounts[10]. The terms of the Apps for Education agreement related to the information in a student's email account remains in effect even once a student has graduated.

Google indicates that if uOttawa decides to discontinue its use of Google Apps, that there are several options for the migration of uOttawa's email data to another solution. Refer to **Section 3.1** - Termination and Retention of Data.

For an individual student, Google provides several options for the migration of data from the Google Apps email service to another email service.

---

[9] Section 1.3 of the *Google Apps for Education Agreement* indicates that the "c*ustomer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Google may monitor emails sent to these aliases for Customer Domain Names to allow Google to identify Services abuse.*"

[10] Section 1.4a of the *Google Apps for Education Agreement* indicates that "*The default setting for the Services is one that does not allow Google to serve Ads. Customer may change this setting in the Admin Console, which constitutes Customer's authorization for Google to serve Ads. If Customer enables the serving of Ads, it may revert to the default setting at any time and Google will cease serving Ads.*"

3.6 Accuracy of Personal Information

Privacy Principle:

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

The accuracy of the actual content of student emails should not be a significant accuracy-related privacy risk; as student email is being directly created and sent by the student. Emails sent from faculty and administration to students will not be impacted by the switch to Google as faculty and administration accounts will remain on their current system and these emails may be considered business records and subject to FIPPA and other requirements.

3.7 Safeguards

Privacy Principle:

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information

The addendum to the agreement includes 'Attachment A', which outlines Google Apps Security Standards, including those related to data center and network security, access and site controls, and data. It is possible that the safeguards that have been implemented by Google related to the protection of email are more robust than those that currently exist at uOttawa.

Once a student has signed up for the service, the student needs to access the Password Management tool and set a new password. uOttawa has implemented new strong password requirements that are:

- Minimum of eight characters;
- One special character (&,%,$, etc.); and,
- One capital and one lowercase letter.

uOttawa e-mails pay-related information to students who are employees. There is also potentially additional sensitive personal information that is transmitted and received by student e-mail accounts, although uOttawa can only control what it specifically sends to students. uOttawa does indicate to students that the use of email is an unsecure means of communication. For example, the login webpage includes a link to *Email tips and best practices*[11], which includes guidance such as "*Don't put confidential, personal or emotional content when replying to an email*", and below the section on email tips and best practices is a *Netiquette* section, which states, "*Don't rely on the privacy of email, especially from work, but respect the privacy of others.*"

Information sent from faculty or administration to student email accounts may include information about a student's financial aid, housing, or replies to a student's inquiries related to other matters. A draft Email Policy (Policy CCS-ISP04) has been developed that indicates that "*Unless they have been authorized by the information owner, a user of UO email account holders are prohibited from using email to transmit confidential, personal or restricted information to internal or external parties*". The draft policy has not yet been formally reviewed or approved.

Privacy Risk and Recommendation

There is a risk that uOttawa staff and faculty are sending emails to students that contain personal information, and given the potential sensitivities related to the use of Google as a service provider, uOttawa should ensure faculties and administrative units review their email practices. As uOttawa works towards developing a formal email policy, consider items such as:

- For personal information that is not particularly sensitive, uOttawa may want administration and faculty to ensure that consent has been obtained from the student for its communication through email.
- For more sensitive personal information, uOttawa may want administration and faculty to ensure

[11] uOttawa's email tips and best practices is available at: www.ccs.uottawa.ca/email/overview.html#tips

these data elements are not communicated through email unless they have been appropriately encrypted.

3.8 Openness

Privacy Principle:

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

The privacy practices of uOttawa are available through the uOttawa website[12] and through the uOttawa Privacy Policy[13]. A key consideration for this initiative is providing students information on the nature of the relationship between uOttawa and Google, and how Google will manage their personal information as a service provider acting on behalf of uOttawa. uOttawa has developed a comprehensive Terms of Service that outlines the management of personal information through the use of the service (refer to Appendix E), and has developed a website explaining the use of Google Apps at uOttawa, this includes a Privacy FAQ[14],

The implementation of a new email solution for students should not require any changes to uOttawa's current Directory of Records.[15]

3.9 Individual Access

Privacy Principle:

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

A student could request information about themselves from uOttawa related to their email account and user identity, which uOttawa would be able to provide, although such a scenario is unlikely given the student would already know these elements. uOttawa would also be able to indicate to a student what information has been provided to Google in order to facilitate the creation and management of their email account, and uOttawa expects to communicate this to students during the initial opt in process (refer to Section 3.2).

Emails sent from a student account to uOttawa faculty or administration may be subject to FIPPA requirements related to access to an individual's personal information, although emails within faculty and administration email accounts are not impacted by the switch to Google as faculty and administration accounts will remain on their current system and these emails would continue to be treated in their current manner.

3.10 Challenging Compliance

Privacy Principle:

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Students may make a complaint or inquiry related to the management of personal information to the uOttawa FIPPA Coordinator. Contact information for the FIPPA Coordinator is available through the

[12] www.uottawa.ca/privacy/home.html

[13] http://web5.uottawa.ca/admingov/policy_90.html

[14] www.uottawa.ca/googleapps/en/privacy.html

[15] www.uottawa.ca/privacy/directory.html

uOttawa website[16] and through the uOttawa Privacy Policy.[17] Students can also contact the Office of the Information and Privacy Commissioner of Ontario directly.

Related to monitoring and compliance with the terms of the agreement between uOttawa and Google, Attachment A of the addendum to the agreement includes the following clause on audits: "*During the Term, Google will maintain its Standard for Attestation Engagement No. 16 audit report or a comparable report ("Audit Report") and will update the Audit Report at least every eighteen (18) months. On Customer's written request during the Term, Google will provide Customer a copy of such Audit Report in accordance with Google's policy as to the distribution thereof (including that such Audit Report must be returned or destroyed within 10 days of receipt and no copies of the report may be made).*"

uOttawa should ensure a process is in place to receive and review updated audit reports throughout the life of the contract. Refer to **Section 3.1** - Audit.

---

[16] www.uottawa.ca/privacy/home.html

[17] http://web5.uottawa.ca/admingov/policy_90.html

Appendix A - Risk Ranking Methodology

The overall risk rating was determined based on two factors: 1) the probability that an adverse event could occur; and 2) the impact on the program should an adverse event occur.

1. Probability

The probability that personal information breach or adverse event will occur was considered. This involves assessing whether a threat (e.g. an uninformed employee) will exploit a control (e.g. recycles instead of shredding personal information). Probability was rated as "high", "moderate", or "low". These ratings are assigned as follows:

Probability Rating

Rating	Description
Low	There is little to no likelihood that a data breach or adverse event will occur.
Moderate	There is some likelihood that a data breach or adverse event will occur.
High	A data breach or adverse event has already materialized or is likely to occur in the future.

2. Impact

The impact to uOttawa should a data breach or adverse event actually occur was also considered and rated as "high", "moderate", or "low" as follows:

Impact Rating

Rating	Description
Low	The risk non-compliance with privacy requirements and/or adverse impact to the financial or program operations or reputation is low. Regulatory action would be very unlikely in the event of non-compliance. Volume and/or sensitivity of personal information impacted would be low. Financial, reputational, operational
Moderate	Risk of non-compliance with privacy requirements and/or adverse impact to the financial or program operations or reputation is of a more urgent nature. Some measures may need to be taken to address immediate issues and/or prevent potential threats from materializing. Regulatory action may involve a notice of violation and/or require some corrective actions. Volume and/or sensitivity of personal information affected would be moderate.
High	Risk of non-compliance with privacy requirements and/or adverse impact to the financial or program operations or reputation is imminent, or may have already materialized. Corrective measures should be taken immediately to remediate issues and/or prevent potential threats from materializing. There would likely be national/international media coverage. Regulatory action would be a significant. The volume and/or sensitivity of personal information impacted would be high.

The overall risk rating is calculated based on the probability and impact. For example, if the probability of a risk occurring is low and the impact is moderate, the overall rating would be "low" (see table below).

Overall Risk Rating

Probability	Impact: Low	Impact: Moderate	Impact: High
High	Moderate	High	High
Moderate	Low	Moderate	High
Low	Low	Low	Moderate

Appendix B - Terminology

Definitions

FIPPA	The *Freedom of Information and Protection of Privacy Act* (FIPPA) is a two-part Act dealing with access to information and protection of personal privacy. The Act covers the Ontario government including ministries, agencies, Cabinet Office and Premier's Office.
Information and Privacy Commissioner of Ontario (IPC)	The role of the Information and Privacy Commissioner of Ontario (IPC) is set out in FIPPA and related privacy legislation.[18] The IPC acts independently of government to uphold and promote open government and the protection of personal privacy. Under its statutory mandate, the IPC is responsible for: • resolving appeals from refusals to provide access to information; • investigating privacy complaints about information held by government organizations and health information custodians; • ensuring that the government organizations and health information custodians comply with the provisions of the *Acts*; • educating the public about Ontario's access and privacy laws; and, • conducting research on access and privacy issues, and providing advice and comment on proposed government legislation and programs.
Personal Information	FIPPA defines "personal information" as information about an identifiable individual, for example, an individual's name and contact information, or more sensitive information such as financial and medical history.
Personal Information Bank (PIB)	FIPPA defines a Personal Information Bank (PIB) as "*a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual.*"
Privacy	The IPC describes "privacy" as "*... having the ability to control or influence the way in which information about you is collected, used and disclosed.*"

[18] The *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*

Acronyms

CTO	Chief Technology Officer
FIPPA	Freedom of Information and Protection of Privacy Act
GADS	Google Apps Directory Sync
IPC	Information and Privacy Commissioner
OUAC	Ontario Universities' Application Centre
PIA	Privacy Impact Assessment
SaaS	Software as a Service
SIN	Social Insurance Number
SIS	Student Information System

Appendix C - Supplementary Documents List

Google Agreements

- Google Apps for Education Agreement and Addendum, signed October 4, 2012

Documents Related to uOttawa Policies and Procedures

- uOttawa Policy 108 – Electronic Data Processing Security (last updated 2007)
- *Draft* uOttawa Policy ISP01 – Document and Information Classification Policy (February 2012)
- *Draft* uOttawa Policy ISP02 – Access Management Policy (February 2012)
- *Draft* uOttawa Policy ISP03 – Password Control Policy (February 2012)
- *Draft* uOttawa Policy ISP04 – Email Policy (December 19 2012)
- Policy 90 – Access to Information and Protection of Privacy
  http://web5.uottawa.ca/admingov/policy_90.html
- Notice of Collection of Personal Information (section 9 of Policy 90) Procedure 20-5 – Handling Access to Information Requests and Privacy Breach Complaints
  http://web5.uottawa.ca/admingov/procedure_20-5.html
- Policy 14a) – Student Record
  http://web5.uottawa.ca/admingov/policy_14a.html
- Policy 108 – Electronic Data Processing Security
  http://web5.uottawa.ca/admingov/policy_108.html
- Policy 23 – University of Ottawa Archives
  http://web5.uottawa.ca/admingov/policy_23.html
- Procedure 20-4 – Records Retention Periods
  http://web5.uottawa.ca/admingov/procedure_20-4.html
- Records Retention Schedule
  http://web5.uottawa.ca/admingov/documents/records_retention_schedule_2008.pdf
- Registrar's Third Party Authorization Form
  www.registrar.uottawa.ca/Portals/43/Registrar/REGI3200.pdf

Documents Related to uOttawa Deployment

- Cloud Computing Contract Issues
- Email Account Creation and Distribution Rules, October 2012
- Process Overview Diagram, January 2013
- Workflow of Processes for New Students, February 11, 2013
- PIA Feedback from other Institutions
- Replacement of Student Email - Business case v1 (May 2012)
- Set and Remove Forwarding Address

- Full Name Email Address
- Student Opt-out
- API SAML Single Sign
- Password Length Requirements
- Backups and Restores
- Helpdesk Roles and Tools
- Email Routing
- Google Apps Active Directory Sync
- Email Migration
- Terms of Service – uOttawa Google Apps for Education Service, Final, March 1, 2013

Applicable Legislation, Policies, and Guidelines

Legislation

- *Freedom of Information and Protection of Privacy Act*
  www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
- Ontario Regulation 459
  www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900459_e.htm
- Ontario Regulation 460
  www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900460_e.htm

Leading Practice and Guidance

- Generally Accepted Privacy Principles (GAPP) published by the Canadian Institute of Chartered Accountants (CICA) (May 2006)
  www.cica.ca/index.cfm/ci_id/36529/la_id/1.htm
- Privacy by Design (PbD)
  http://privacybydesign.ca
- Privacy in the clouds, A White Paper on Privacy and Digital Identity: Implications for the Internet, Information and Privacy Commissioner of Ontario
  www.ipc.on.ca/images/resources/privacyintheclouds.pdf
- Modelling Cloud Computing Architecture Without Compromising Privacy: A *Privacy by Design* Approach
  www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf

Appendix D – Interview List

- Senior Programmer Analyst, Computing and Communications Services
- Systems Administrator, Office Of The Registrar
- Legal Counsel, Legal Services
- Access to Information and Privacy Coordinator, Office Of The Vice-President, Governance
- Manager, Consulting and Technical Services, Computing and Communications Services
- Manager Communications, Strategic Enrollment Management
- Project Officer and Editor, Strategic Enrollment Management
- Communications Officer, Communications Directorate
- Communications Officer - Strategic Communications, Computing and Communications Services
- Systems Analyst, Computing and Communications Services
- Network Specialist, Computing and Communications Services
- Security and Access Coordinator, Computing and Communications Services
- Senior Analyst, Computing and Communications Services
- Information Technology Manager, Computing and Communications Services
- Programmer Analyst, Computing and Communications Services

Appendix E - Additional Documents

User Code of Conduct for Computing Resources

Guiding Principle

The University of Ottawa's computing resources are intended to support its educational and research activities.

Code Violations and Discipline

Violations to the User Code of Conduct, complaints about violations, and disciplinary measures against violators are governed by applicable laws and regulations and by University policies, regulations, employment contracts or collective agreements.

Definitions

1. **Account:** Any account number, access code, user identification code or authorization code granted for a computing resource.
2. **Computing Resource:** Includes, but is not limited to, computers, peripherals, software, data, network infrastructure, other hardware owned or managed by the University of Ottawa.
3. **User:** Any person who has been provided with an account or computing resources.

User Commitment and Responsibility

Users accept and agree that they are responsible for all use of their account and computing resources and further accept to abide by the User Code of Conduct set out below.

Rights of the University of Ottawa

The University reserves the right to remove material from an account or computing resource and to suspend access to an account or computing resource pending investigation into suspected violations of the User Code of Conduct.

The University does not sponsor or endorse a user's data or the content of a user's account or personal Web page.

Specific Responsibilities of Users

Under the User Code of Conduct, users must:

1. Use only the account for which they have been authorized by the University, and comply with all restrictions applying to this account.
2. Prevent unauthorized access for every single account and computing resource provided to them by using passwords and other controls, and keep these passwords and access controls confidential at all times.
3. Never impersonate other users or any other person.
4. Ensure their accounts and computing resources are used only for authorized activities.
5. Never use accounts and computing resources for personal commercial purposes or financial gain.
6. Prevent their accounts and computing resources from being used by other people, including family, friends, acquaintances and other third parties.

7. Never send, display or store obscene or pornographic material or any other material that is subject to applicable laws or regulations.
8. Never send harassing communications or send unauthorized and unsolicited bulk electronic mail.
9. Never intercept or try to intercept network communications (such as e-mail messages, user-to-user dialogue) not intended specifically for them.
10. Never interfere or attempt to interfere with any account or computing resources, as this could impair their normal operation.
11. Never use accounts or computing resources to try to gain unauthorized access to non-University resources.
12. Use sound security devices and methods to protect accounts and computing resources, such as regular password changes, anti-virus software and regular data back-up.
13. Comply with all copyright, trademarks and trade-name rights and licences in all software or other material

Google Apps Acceptable Use Policy

Use of the Services is subject to this acceptable use policy ("AUP").

If not defined here, capitalized terms have the meaning stated in the applicable contract ("Agreement") between customer, reseller or other authorized user ("You") and Google.

You agree not to, and not to allow third parties or Your End Users, to use the Services:

- *to generate or facilitate unsolicited bulk commercial email;*
- *to violate, or encourage the violation of, the legal rights of others;*
- *for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;*
- *to intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;*
- *to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;*
- *to alter, disable, interfere with or circumvent any aspect of the Services;*
- *to test or reverse-engineer the Services in order to find limitations, vulnerabilities or evade filtering capabilities;*

Your failure to comply with the AUP may result in suspension or termination, or both, of the Services pursuant to the Agreement.

Terms of Service – uOttawa Google Apps for Education Service

uOttawa Google Apps for Education Service is powered by Google Inc. and encompasses your email account and all other services made available to you by Google Inc via the uOttawa Google Apps for Education Service. By using the uOttawa Google Apps for Education Service, you agree to the terms listed below.

Use:

1. Your use of uOttawa Google Apps for Education Service is governed by Google Inc.'s Acceptable Use Policy, Privacy Notices and other Google Inc. Terms of Service. Future changes to these will apply so you are responsible for consulting them on a regular basis to ensure that your use conforms to the most recent versions.

2. You may not use the uOttawa Google Apps for Education Service for anything other than your own use: you may not sell, resell, lease or the functional equivalent to a third party, or attempt to reverse engineer or create a similar account or service through the use of or access to the uOttawa Google Apps for Education Service. Export controlled information cannot be stored, transferred or shared via the uOttawa Google Apps for Education Service. For more information on export controlled restrictions placed on your data, consult the Office of Risk Management's Controlled Goods Program webpage.

3. Your use must also comply with applicable laws and with applicable uOttawa policies, procedures and regulations as they relate to your use of the uOttawa Google Apps for Education Service. This includes policies such as the uOttawa User Code of Conduct for Computing Resources.

Compliance

4. The uOttawa email administrator (CCS) and Google Inc. jointly manage the abuse@uottawa.ca inbox, where students can report spam, abuse and technical issues.

5. uOttawa has the ability to enable and disable your access to the uOttawa Google Apps for Education Service.

6. uOttawa further reserves the right to access, disclose or preserve content or information associated with your uOttawa Google Apps for Education Service necessary to enable you to use the uOttawa Google Apps for Education Service, to administer and ensure compliance with the Google Apps for Education Agreement, with uOttawa policies, procedures, regulations and necessary to comply with laws, legal processes in Canada or foreign jurisdictions, or necessary to protect uOttawa, the uOttawa community or the public.

Privacy and Security

7. Personal information collected by uOttawa in connection with the provision of the uOttawa Google Apps for Education Service is collected in accordance with uOttawa's Policy 90 on Access to Information and Protection of Privacy. You agree that uOttawa may collect your username, first name, last name and an encrypted version of your password for the purposes of and those consistent with the provision of the uOttawa Google Apps for Education Service and so that Google Inc. can use this information to authenticate the individual and provide them with access to the uOttawa Google Apps for Education Service.
8. Google Inc. will retain a user account until it is deleted from Google Apps, and this will lead to all of the user's information being deleted as well. Deleted mail is purged after 30 days and is non-recoverable.

9. Your data will be stored and processed by Google Inc. in whole or in part in the United States or in such other country in which Google Inc. or its agents maintain facilities. Use of the uOttawa Google Apps for Education Service means that your personal information may be subject to United States laws regarding disclosure, such as The Patriot Act, and uOttawa cannot guarantee protection against

possible disclosure of content residing in the United States or other foreign jurisdiction. Your use of the uOttawa Google Apps for Education Service constitutes your consent to transfer your personal information out of Canada and acknowledgement that your data may be disclosed to, among other governments, the United States governments, law enforcement or regulatory agencies through the laws of the United States. For further information about how your personal data is treated, see Google Inc.'s Privacy Policy.

10. To ensure protection against anticipated threats or hazards to the security of data, Google Inc. assures that its facilities used to store and process data will adhere to the same security standards no less protective than the security standards at facilities where Google Inc. stores and processes its own information. Google will notify uOttawa of a security breach by Google, following the discovery or notification of such security breach after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. You are also responsible for taking reasonable measures within your means to maintain the security and privacy of your content and protecting against privacy breaches, for example: for more sensitive personal information, you should ensure these data elements are not communicated unless they have been encrypted.

Limitation of Liability

11. Any warranties associated with the uOttawa Google Apps for Education Service are those of Google Inc. If the uOttawa Google Apps for Education Service is not functioning correctly, fails or there is a breach in data privacy, uOttawa is not responsible or liable to you for any content, applications or services provided to you or accessible by you through the uOttawa Google Apps for Education Service.

Additional Info

Consult the uOttawa Google Apps for Education website for additional information and updates.

If you do not agree, you may choose not to use uOttawa Google Apps for Education Service. In such case, notify GoogleApps@uOttawa.ca and provide uOttawa with an alternative personal email address. Failing to provide an alternate email address will mean that you are at risk of not receiving official uOttawa communications directed to or concerning you.

If you agree to these terms, Please select "I agree to the Terms of Service"

Privacy FAQ

The University is committed to maintaining and protecting the confidentiality and privacy of our students' personal information.

Before implementing this new email service, we looked at the privacy implications and ways to help ensure that personal information is protected in accordance with the University's policies on personal information and with applicable legislation governing personal information.

As part of the implementation, we:

- looked at different service provider options;
- conducted our own internal review of our privacy needs in relation to student email
- consulted with Canadian universities that had already implemented, or were in the process of implementing, a cloud-based student email solution;
- consulted students in a pilot project prior to selecting a service provider
- initiated a Privacy Impact Assessment (PIA) with a view to identifying major risks and implementing remediation measures to help reduce those risks; and
- consulted with the University's Access to Information and Privacy Coordinator and with Legal Services.

Will Google own the data that is stored in Google or passes through Google servers?
Google does not own student data. Data in @uOttawa.ca Google accounts is the property of the University of Ottawa and/or the student, the end user. The agreement that the University of Ottawa has entered into with Google has no impact on the intellectual property rights or ownership of student data.

What steps has the University taken to ensure that my privacy is protected?
We have taken the appropriate steps to ensure that your privacy rights, as outlined in the University's policies on personal information, are safeguarded. Email content and passwords are not shared with Google.

Google is also committed to your privacy and to ensuring the confidentiality and security of your personal information. Their security policies include provisions on the protection of your data against threats and unauthorized access.

What personal information is shared with Google?
A limited amount of student information is shared with Google in order to create a Google-powered student email account. The following personal information is provided: first name, last name, username, and email address to validate against our authentication services.

Will Google log my activity or scan my content?
Google has some access to your account as explained in the Terms of Service. Google has agreed that the University is not granting Google any rights, implied or otherwise, to content. Google is not permitted to conduct data mining. Google has also agreed that the default setting is that Google is not permitted to include advertising in our student accounts.

Google employees may be granted temporary access to your email for troubleshooting purposes or to ensure the integrity of the services provided, but only with the approval of University of Ottawa Administrators.

Can Google share my personal information with any third parties?
No. Our agreement with Google states that Google is not allowed to share students' personal information.

Who is responsible for protecting the data stored in or sent from my @uOttawa.ca Google account?

Students continue to be responsible for how they use and share confidential information (including personal information) in accordance with University Policy 80, Computing and Information Processing, and the Code of Conduct for Computing Resources. Students have an obligation to promote responsible, ethical and secure use of services. Google is also responsible for protecting and maintaining the security standards of the facilities it uses to store and process end-user data.

Where is my @uOttawa.ca Google account data stored?
Student account data is stored at one of Google's global facilities; access to these facilities is governed by the laws of the jurisdiction in which the data is stored, including the U.S. *Patriot Act*. Account data may be stored in multiple locations to protect information against system failures and IT security risks. For further information about how your personal data is treated, see Google Inc.'s Privacy Policy.

How secure is my information?
Google offers a number of features to keep your information secure. However, any email may be the target of Internet predators, which is why it is important to have a strong password and not to share your confidential information with others. It is best practice to assume that your email is not 100% private, regardless of the service provider. Never provide your password or other personal, secure information via email.

Gmail's tips on keeping your account secure.

Read more about the importance of passwords on the CCS website.

Ontario's Information and Privacy Commissioner issued a discussion paper entitled "If You Want To Protect Your Privacy, Secure Your Gmail" (2009).

Are users offered any spam protection?
Google includes spam protection with their service. Spam is automatically directed to a spam folder and purged after 30 days. The service also includes safeguards for virus checks and verifications before downloading data. However, not all spam protection is 100% effective. It is still up to you to exercise some caution when communicating with unfamiliar sources or downloading attachments.

For more information about applicable University policies:

- Access to Information and Protection of Privacy
- Code of Conduct for Computing Resources
- Electronic Data Processing Security
- Computing and Information Processing
- FIPPA FAQ

More questions?
If you have questions about the functionality of your uOttawa email account, contact Computing Help Centre at 613-562-5800 ext 6555 or by filling out the Computing assistance request form. For general questions related to your personal information, see the University's Policy on Access to Information and Protection of Privacy or contact the Access to Information and Privacy Coordinator.