Deloitte.

University of Guelph

Privacy Impact Assessment (PIA) for the Student Email Initiative

February 12, 2014

CONFIDENTIAL

Contents

Disclaimer i

Executive Summary i

1 Introduction 1

1.1 Background 1

1.2 Objective and Scope 1

1.3 Approach 2

1.4 Privacy Requirements 2

2 Solution Overview 3

2.1 Overview of Current Email System 3

2.2 Proposed Email Solution 5

2.3 Safeguards and controls provided by the University 7

2.3.1 Privacy-specific controls 7

2.3.2 Security-specific Controls 7

2.3.3 Password settings 8

2.4 Safeguards and Controls provided by Google 11

2.4.1 Physical Security 11

2.4.2 Network Security 11

2.4.3 Logical Controls 12

2.4.4 Data Security Controls 12

2.4.5 Other Controls 12

3 Data Flow Analysis 13

3.1 Description of Personal Information 13

3.2 Collection and Use of Personal Information 13

3.3 Disclosure of Personal Information 14

3.4 Retention and Disposition of Personal Information 15

3.5 Sensitivity of Personal Information 15

4 Privacy Compliance Analysis 16

4.1 Accountability 16

4.2 Identifying Purposes 21

4.3 Consent 22

4.4 Limiting Collection of Personal Information 22
4.5 Limiting Use, Disclosure, and Retention of Personal Information 23
4.6 Accuracy of Personal Information 24
4.7 Safeguards 24
4.8 Openness 26
4.9 Individual Access 26
4.10 Challenging Compliance 26
5 Recommendations Roadmap 28
Appendix A - Risk Ranking Methodology 31
Appendix B - Terminology 33
Appendix C - Supplementary Documents List 34
Appendix D – Interview List 36
Appendix E - Additional Documents 37
Google Apps Acceptable Use Policy 37
University of Guelph Acceptable Use Policy for Information Technology 37

Disclaimer

This privacy impact assessment (PIA), conducted by Deloitte LLP, analyzes the privacy issues related to the transition of student email and calendaring solutions at the University of Guelph from the current email system to the Google Apps for Education suite. This PIA analyzes the privacy implications relating to the collection, use, disclosure, retention, destruction, and protection of personal information involved in the email transition initiative. This PIA is intended to provide policy and strategic planning advice concerning the personal information handling and management practices of University of Guelph and Google and to serve as an educational tool for senior management and staff. This PIA relies on information provided by the University of Guelph project team and does not constitute an audit or assurance engagement as described in the professional standards issued by the Canadian Institute of Chartered Accountants (CICA). Furthermore, the findings and recommendations within this PIA are not a legal opinion or other form of assurance or legal advice with respect to University of Guelph's legal compliance with applicable privacy legislation, best practices or information security standards. Legal compliance remains the responsibility of University of Guelph.

The content of this PIA is subject to change pending stakeholder validation.

This PIA report is intended solely for use by authorized individuals of the University of Guelph. No part of this PIA report may be reproduced or distributed in any form without the prior permission of the University of Guelph.

Executive Summary

University of Guelph (hereinafter referred to as "the University"), located in Guelph, Ontario, is one of Ontario's top rated comprehensive universities. The university has about 23,000 students and 900 staff, and provides 13 degree programs, with primary focus on health, food, the environment and community. In addition to on campus courses and programs, the university provides distance education and remote learning. The university is planning an initiative that will transition students (undergraduate and graduate) to the Google Apps for Education email and calendaring suite from the existing Gryph Mail system. The initiative will move all email and calendaring tools for students into a cloud environment. The goal of the 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. Contract negotiations with Google are currently underway with the roll-out of the new email platform to be completed by fall 2014.

The purpose of this privacy impact assessment (PIA) is to perform a privacy risk assessment and recommend any remediation required to help ensure the protection of personal information in accordance with the privacy legislation to which the University must comply. This includes identifying risks associated with cloud services being offered within a multi-tenancy environment and any jurisdictional legislation that may be applicable over the data based on its geographical location. The assessment should identify the risks based on probability and impact to the organization (rated as high, moderate or low). The remediation recommendations will include policy, procedure or technical controls as well as any recommended contractual language as it relates to privacy for management to further discuss with legal counsel. The PIA findings will be used by the University to help further inform the design and build phases of the project, as well as inform contract negotiations with Google.

The University 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 the University and Google. However, Google is subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) in its dealings with the University. 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, alleviating these concerns will be a key communications challenge that the University will need to address throughout this project. Specifically, 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.

The PIA includes a detailed review of the standard *Google Apps for Education Agreement* and its related *Addendum* that was provided to the University and has noted areas of potential risk related to the current agreement clauses. It is important to recognize the scope of the PIA and thus the identified risks described in the table below relate to the implementation of the student email initiative. This means that the PIA does not necessarily reflect current gaps or weaknesses in the existing corporate privacy program of the University.

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 University 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. Deloitte identified 10 risks or gaps associated with the planned student email transition initiative that relate to both the terms and conditions found within the Google contract as well as issues associated with the configuration and deployment of the solution. Six risks are deemed moderate and 4 risks low (see chapter 4 below). The table below describe the moderate risks.

Table 1: Risk Summarization

#	Risk	Risk Level	Recommendation
1	There is a risk that the current agreement and addendum does not sufficiently mitigate potential privacy risks to a level that is acceptable to management. Although the agreement includes several important privacy-related clauses, it could be further strengthened, especially related to an acknowledgment of FIPPA requirements. *Refer to Section 4.1*	**Moderate**	a. The University should obtain further confirmation related to the disposition of the University data by Google upon expiration of the agreement or deletion of user accounts, specifically if data within backup, cache and other non-active servers will also be disposed, and what period of time would be considered "a *commercially reasonable period of time".* b. Through its contract negotiations with Google, the University management in collaboration with legal counsel should determine the extent to which language in the current agreement covers these considerations or to the extent additional clauses are required. c. Through its contract negotiations with Google, the University should identify specific timelines upon which breach notification is expected to be provided by Google to ensure that the University has adequate time to prepare for/respond to/manage certain breach activities, as required. The University should also further define what type of support and when support is provided when University led activities require escalation to Google. d. It is also recommended that the University ensure that the security controls and metrics that are currently being monitored by the University remain in scope even after transition to the new system either by the University or by Google (e.g., through use of reporting metrics on malware, suspicious account activity).

#	Risk	Risk Level	Recommendation
2	There is a risk that the current third party audit conducted on Google does not include appropriate privacy and security considerations. *Refer to Sections 4.1 and 4.10*	**Moderate**	a. Through its contract negotiations with Google, the University should request to see the most current audit report for Google to ensure privacy and security has been appropriately considered. b. The University should ensure a process is in place to receive and review updated audit reports throughout the life of the contract.
3	There is a risk that the scanning of email content by Google may include the use or retention of personal information that is not consistent with the requirements of FIPPA. Furthermore, without knowing the specific details of how data related to the scanning process will be managed, the University cannot adequately inform students of how their data will be managed under the new email solution. *Refer to Section 4.5*	**Moderate**	Through its contract negotiations with Google, the University should ensure it a) understands Google's management of email content for those mails determined to be a potential threat, b) feels the approach provides adequate privacy and security coverage, and c) includes the necessary reporting clauses to the University around, for example, frequency of occurrence, and activities to contain and mitigate issues (be it isolated or systemic).
4	There is a risk that the University staff and faculty are sending emails to students that contain personal information. *Refer to Section 4.7*	**Moderate**	a. Given the potential sensitivities related to the use of Google as a service provider, the University should ensure faculties and administrative units review their email practices. b. For more sensitive personal information, the University should ensure these data elements are not communicated through email unless they have been appropriately encrypted. c. The University should develop an email best practices guideline detailing the dos and don'ts of email use to ensure safety of personal information.
5	Password security controls are not currently enforced when a student sets-up email access via a mobile device (e.g., phone, iPad). *Refer to Section 4.7*	**Moderate**	Since device and application access requires a password to be set within Google Apps itself, strong password requirements should be set within the Google administration interface.
6	There is an increased risk that emails may be misrouted depending on the type of domain configuration the University selects (i.e., single domain vs. two domains). As a result, the University could see an increase in the unauthorized disclosure of personal information. *Refer to Section 4.7*	**Moderate**	It is recommended that the University utilize separate domains to reduce the risk of misconfiguration or provisioning errors which would result in mis-routed email and possible personal information disclosure.

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

- Develop an action plan to address the risks 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.

This PIA should also be read in conjunction with the Threat Risk Assessment (TRA) conducted on the Google Apps deployment.

Since this is a forward-looking PIA that is not assessing existing systems and processes but a conceptual view of the new email solution, the findings are not necessarily deficiencies as such, but risks that need to be considered and addressed to ensure that privacy concerns are resolved. The PIA is intended to be a ‘living document’ that should be updated throughout the project as the solution is further defined and implemented. Updates can be performed by the University or by an external third party.

1 Introduction

1.1 Background

The University, located in Guelph, Ontario, is one of Ontario's top rated comprehensive universities. The university has about 23,000 students and 900 staff, and provides 13 degree programs, with primary focus on health, food, the environment and community[1]. In addition to on campus courses and programs, the university provides distance education and remote learning.

The University is planning an initiative that will transition the email system used by undergraduate students to the Google Apps for Education email and calendaring suite from the existing Gryph Mail system. As a result, the initiative will move all email and calendaring tools for undergraduate students into a cloud environment. The goal of the 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. Contract negotiations with Google are currently underway, and project implementation that was initially expected to be completed in stages starting in fall 2012 and ending in spring/summer 2013 is currently planned to be completed by fall 2014.

1.2 Objective and Scope

The objective of the Privacy Impact Assessment (PIA) is to perform a privacy risk assessment and recommend any remediation measures required to ensure protection of personal information in accordance with the University privacy requirements and leading practices in relation to adoption of cloud based email services. The scope of this PIA is conceptual in nature and is intended to provide guidance to the University with respect to key considerations for implementing the Google hosted email solution for students in a manner that enhances the privacy of personal information. As such, Deloitte considers this to be a conceptual PIA. This means that Deloitte is evaluating the email solution in its conceptual form and reviewing a standard Google Aps for Education contract. Once the University finalizes the solution architecture and the contract is signed, it is recommended the University update this PIA (e.g., the risk management group or a member of the Office of the Chief Information Officer).

The scope of the PIA is limited to the collection, use, disclosure, and retention of personal information by the University in relation to the student email initiative. The assessment identified the risks based on probability and impact to the organization (rated as high, moderate or low, refer to Appendix A for more information on Deloitte's risk ranking matrix).

The PIA references the clauses within the standard *Google Apps for Education Agreement* and its related *Addendum*.

While the University's Enterprise privacy program is not in scope for this PIA, aspects of the privacy program pertaining to the email initiative have been considered to be in scope. Moreover, this PIA does not assess Google's compliance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

[1] Statement of Work (SoW) - U Guelph PIA and TRA

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 collected during interviews with key university stakeholders and the review of applicable university documentation (refer to Appendix C and D) and does not constitute legal opinion. The PIA is intended for University management in helping with their privacy compliance responsibilities.

1.4 Privacy Requirements

For Ontario public sector institutions such as the University, **personal information** is very broadly defined as, "*recorded information about an identifiable individual …* ", for example, an individual's name and contact information, or more sensitive information such as financial, legal, and medical history. The University 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 Solution Overview

2.1 Overview of Current Email System

Gryph Mail is the University's integrated collaboration suite and features email, calendars, address books, document editing tools, and file storage (briefcase), all accessible from a web browser. Gryph Mail is built on Zimbra, a leading open source messaging and collaboration platform.[2] All students are issued a University of Guelph email address upon admission/registration to the university. As per the University Calendar (graduate and undergraduate), email is considered the primary mode of communication between faculty / administration and the student.[3] As such, students are not permitted to “opt-out” of the university provided email service (i.e., students may not provide the University with a different email address). Moreover, the University considers the student calendar as a binding contract and thus, by extension sees all correspondence with students via the university email account as official and binding.[4] All staff, faculty, students, employees, affiliates, and members of the university community can access Gryph Mail using their central login ID, which can also be used to access other university services such as Internet, downloads, website publishing, Labs and printers.

There are four ways Gryph Mail can be accessed:

- **Web Client:** The web client is the preferred method of accessing email, the calendar, address book and collaboration tools. The web client is accessed through a browser (Internet Explorer, Firefox, and Chrome) by going to mail.uoguelph.ca. There is also a mobile web client that supports smaller screens on smartphones through the device's internet browser. This can be accessed at mail.uoguelph.ca/zimbra/m/zmain

- **ActiveSync/Exchange:** The University allows email clients (such as Outlook) and mobile devices (BlackBerry, Android, iPhone) to connect with Gryph Mail that have ActiveSync/Exchange connection capabilities. This method allows for access to email, calendaring, the address book and tasks.

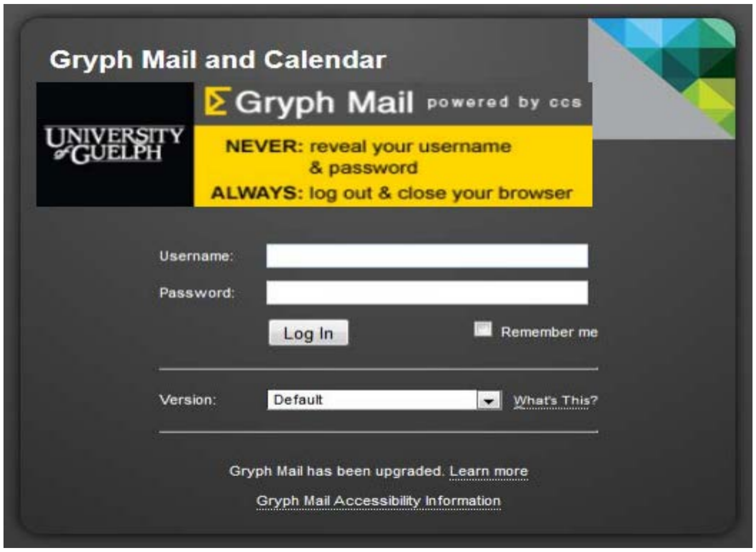
- **IMAP (Internet Mail Access Protocol):** The University allows IMAP as another means for mail clients and mobile devices to connect to Gryph Mail. IMAP only facilitates mail delivery. To access calendaring and other functions, they will have to be set up separately.

- **POP (Post Office Protocol):** The University allows POP to be used for retrieving email but it is not recommended. POP can only receive mail and changes made to mail clients or mobile devices cannot be reflected in Gryph Mail. The University recommends to those who opt to use POP that they do not select "Remove messages from server" in their mail client as this will result in all emails being removed from the mail server and mail only being visible in the mail client using POP.

[2] Zimbra was sold by VMware to Telligent in July 2013, post which Zimbra and Telligent merged into a single company under the Zimbra brand.

[3] The Introduction section of the calendar states that “*The University issued email address is considered an official means of communication with the student and will be used for correspondence from the University. Students are responsible for monitoring their University-issued email account regularly.*”

[4] Per information gathering meetings with the Chief Privacy Officer and the Office of the Registrar. December 16, 2013.



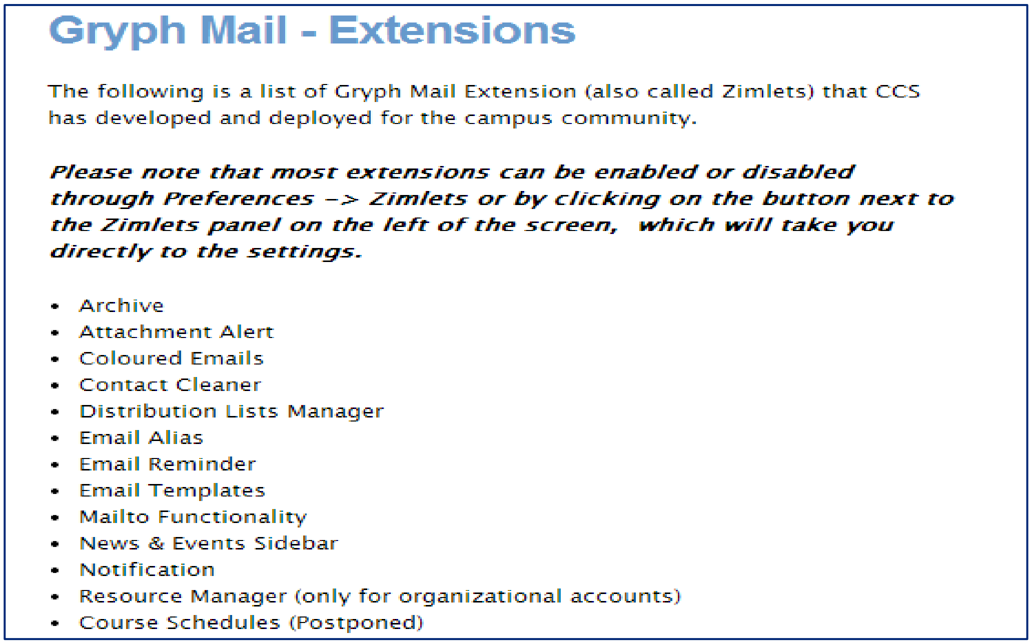
NEVER: reveal your username & password
ALWAYS: log out & close your browser

Version: Default

Gryph Mail has been upgraded. Learn more

Figure 1: Gryph Mail Login page

Gryph Mail also provides users with the option of using extensions, also known as Zimlets. These are like plugins which when installed provide additional functionality to email users. There are a few default Zimlets that ship with Zimbra and some more have been developed by the university's Computing and Communication Services for enhanced utility. For a list of available extensions refer to Figure 2 below:



Gryph Mail - Extensions

The following is a list of Gryph Mail Extension (also called Zimlets) that CCS has developed and deployed for the campus community.

Please note that most extensions can be enabled or disabled through Preferences -> Zimlets or by clicking on the button next to the Zimlets panel on the left of the screen, which will take you directly to the settings.

- Archive
- Attachment Alert
- Coloured Emails
- Contact Cleaner
- Distribution Lists Manager
- Email Alias
- Email Reminder
- Email Templates
- Mailto Functionality
- News & Events Sidebar
- Notification
- Resource Manager (only for organizational accounts)
- Course Schedules (Postponed)

Figure 2: Gryph Mail Extensions

In addition to the Zimbra email suite used for Gryph Mail, the university uses Cisco's IronPort email security appliance. This system is the primary email gateway for the university from the outside world, and all email gets scanned for security risks on the IronPort. Once email has been validated by the IronPort appliance, it is relayed to the Gryph Mail system.

2.2 Proposed Email Solution

The University will migrate its email service for all undergraduate students in the fall of 2014 from the current Zimbra platform to the Google hosted email service, *Google Apps for Education*. Google Apps for Education is a suite of hosted email (i.e. Gmail) and collaboration applications that integrate with Google Docs and Google Calendar enabling a seamless user experience in a university setting. As a Software-as-a-Solution (SaaS) cloud based service, the Google hosted mail service allows users access to their emails through any device with internet access. Google stores and processes all user data in its Data Centers around the world and performs all the backend IT maintenance activities for the service such as software updates, hardware upgrades, maintenance, and security. It is important to note that while the University has selected Google Apps for Education as its new student email service platform, the configuration specifications and division of responsibilities between the University and Google are yet to be finalized. The use of Google as a service provider will include the cross-border transfer of University data (emails and information contained in such emails) and data will be processed in the "United States or any other country." [5]

As the separation of staff / faculty / graduate and undergraduate student email system requires the ability to properly route email between the existing Zimbra solution (staff/faculty/graduate students) and the Google email system (undergraduate students), a method of routing email is required that will ensure email for users that exist gets delivered to the user at the correct system, and that email for non-existent users is properly handled. At the time of this assessment, two separate methods are being considered:

1. **Routing of email based on username**. For this method, all email is addressed to user@uoguelph.ca, and the Internet facing mail gateway performs a lookup to determine the correct email routing. This routing method is shown in Figure 3 below.
2. **Routing of email based on domain**. For this method, a second DNS (Domain Name System)[6] domain is added (for example, student.uoguelph.ca), and email is routed by the gateway based on the domain. In this example, user@uoguelph.ca is routed to the Zimbra system, user@student.uoguelph.ca is routed to the Google email system. This routing method is shown in Figure 4 below.

[5] Google Apps for Education Agreement, Section 1.1 – "*As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data*"

[6] DNS: Domain Name System translates the human readable domain and host names to IP (Internet Protocol) addresses.

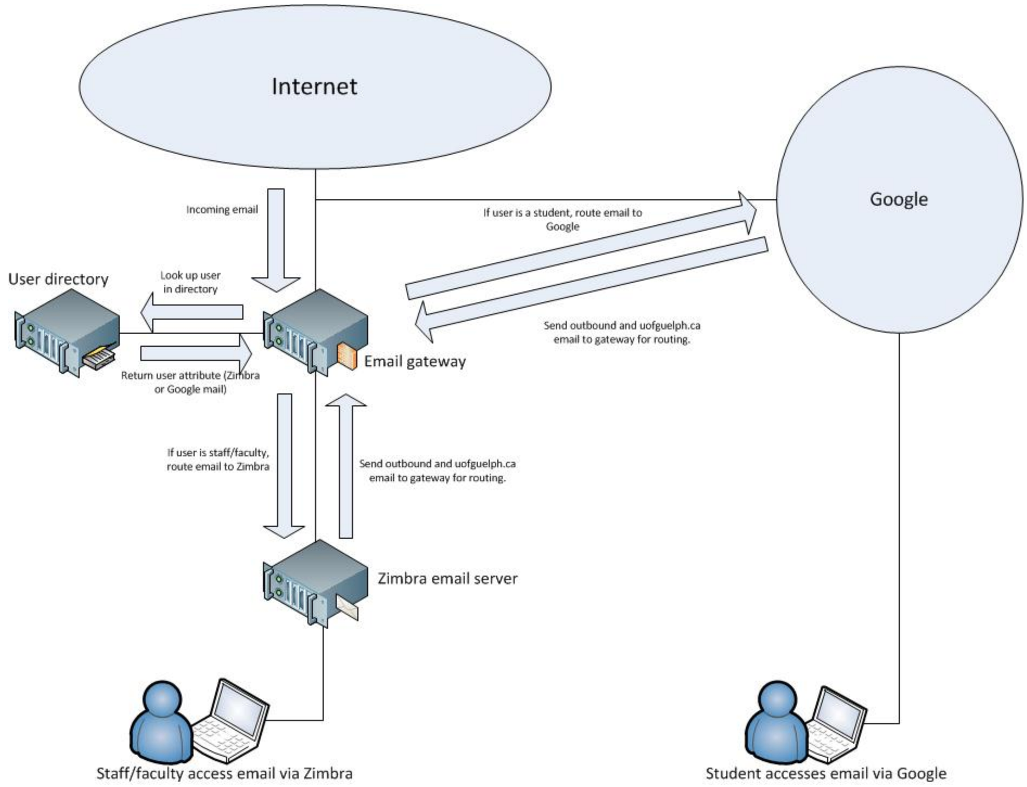

Internet
Google
Incoming email
If user is a student, route email to Google
User directory
Look up user in directory
Send outbound and uofguelph.ca email to gateway for routing.
Email gateway
Return user attribute (Zimbra or Google mail)
If user is staff/faculty, route email to Zimbra
Send outbound and uofguelph.ca email to gateway for routing.
Zimbra email server
Staff/faculty access email via Zimbra
Student accesses email via Google

Figure 3: Conceptual Overview of Single Domain Email Solution

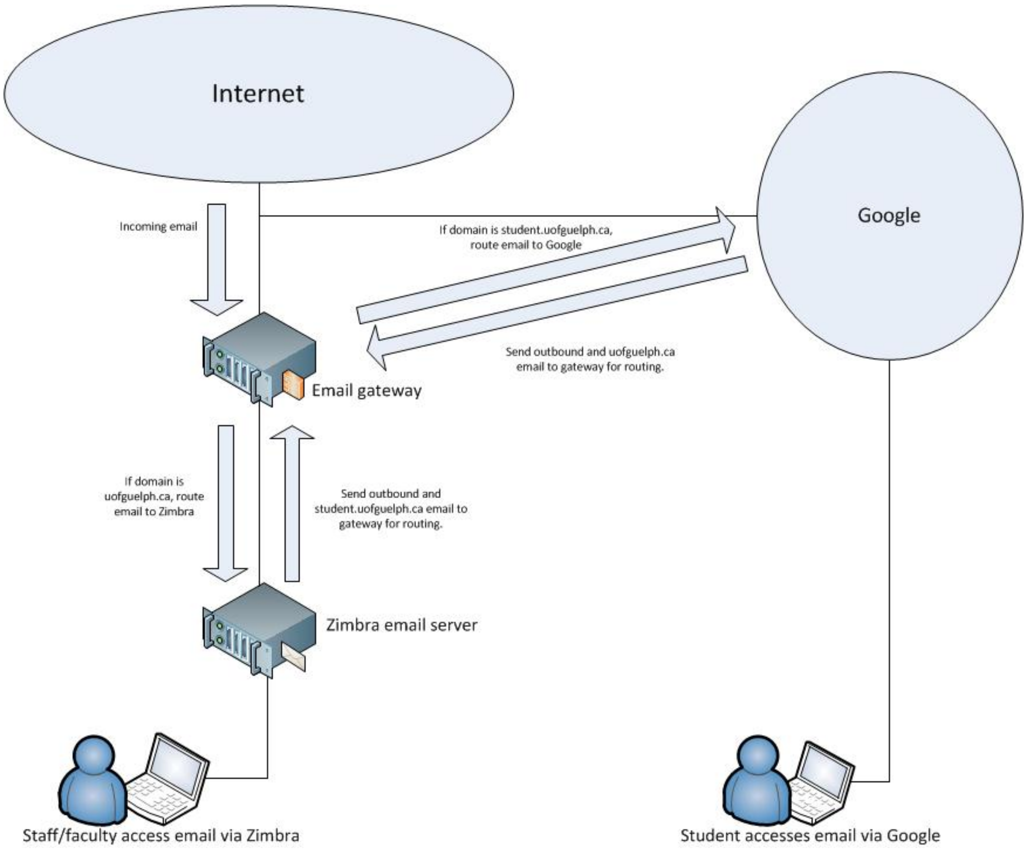

Internet
Google
Incoming email
If domain is student.uofguelph.ca, route email to Google
Send outbound and uofguelph.ca email to gateway for routing.
Email gateway
If domain is uofguelph.ca, route email to Zimbra
Send outbound and student.uofguelph.ca email to gateway for routing.
Zimbra email server
Staff/faculty access email via Zimbra
Student accesses email via Google

Figure 4: Conceptual Overview of Dual Domain Email Solution

2.3 Safeguards and controls provided by the University

2.3.1 Privacy-specific controls

The university has appointed a Chief Privacy Officer (CPO) who is responsible for overseeing all activities in relation to access to information requests and the protection of personal information on behalf of the University's President. The CPO reports into the President's office on all FIPPA related activities.[7]

Staff, faculty and students are informed of the purposes for which the University may collect, use and disclose personal information under its authority as an institution defined in FIPPA through notice of collection statements made available on the university website, certain data collection forms, policies and procedures.[8] In some instances, the University has also provided privacy training to select groups of faculty and staff.[9] While there is no formal privacy policy, there are policies, procedures and/or processes in place with respect to the:

- acceptable use of information technology (refer to Appendix E);
- release of student information;[10] and
- privacy and security incident/breach management.[11]

As required under FIPPA, the CPO prepares an annual privacy report, approved by the University President and submitted to the IPC and has developed a list of personal information banks, which is made publicly available through the university's website.

2.3.2 Security-specific Controls

The University provides several safeguards for the current email system and the campus network as a whole. These safeguards include the following:

Network firewalls
Network firewalls are in place to protect the campus network. Any threats or vulnerabilities identified are dealt with, either through updates or blocking malicious traffic as needed.

Email gateway
Cisco's IronPort email gateway security appliance is used by the University. All sent and received email is scanned by the IronPort for security risks. Most email security risks can be handled by the IronPort, such as viruses, spam and phishing. Once email has been handled by the IronPort, email is relayed to the Gryph Mail system.

Taking into consideration the proposed options being contemplated for implementing Google Apps for Education email for students, all email will still go through the IronPort providing protection from viruses, spam and phishing.

Email gateway monitoring
University IT Security staff, on a regular and periodic basis, monitor activity on the Cisco IronPort email gateway. If a security incident is detected, such as a compromised email account showing unusual activity, incident response procedures are followed to ensure the incident is properly handled and dealt with by the University.

[7] https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/CIO-ITSecurity-02.1-Roles-2009FINAL.pdf
[8] http://www.uoguelph.ca/secretariat/privacy.php
[9] Information gathering meeting with the Gen Gautier. December 16, 2013.
[10] Policy available at: http://www.uoguelph.ca/policies/pdf/ORSInfoReleasePolicy060610.pdf
[11] Information gathering meeting with the Gen Gautier. December 16, 2013. Note: There is a formal breach management response form and workflow but no overarching breach management policy/procedure.

Incident response and management
University IT security staff maintain an incident response process, and include other university departments (CCS, campus police, departmental IT groups) as necessary to handle incidents that occur. Combined with monitoring and helpdesk reporting incidents are responded to in a timely manner.

Security Training and Awareness

In addition to the above noted controls, the university also provides a licensed Security Awareness Course free of charge to all staff, students and faculty. This course, developed by the University and other Universities across Canada to improve IT Security Awareness, will train users in protecting their computing devices and the information held in them from malicious attacks and other cybercrimes and will cover some of the most important topics regarding IT Security.[12]

2.3.3 Password settings

The Central ID is used not only to access to email but also to access other University services, such as internet, labs and printers. The password standards for the Central ID are as follows:[13]

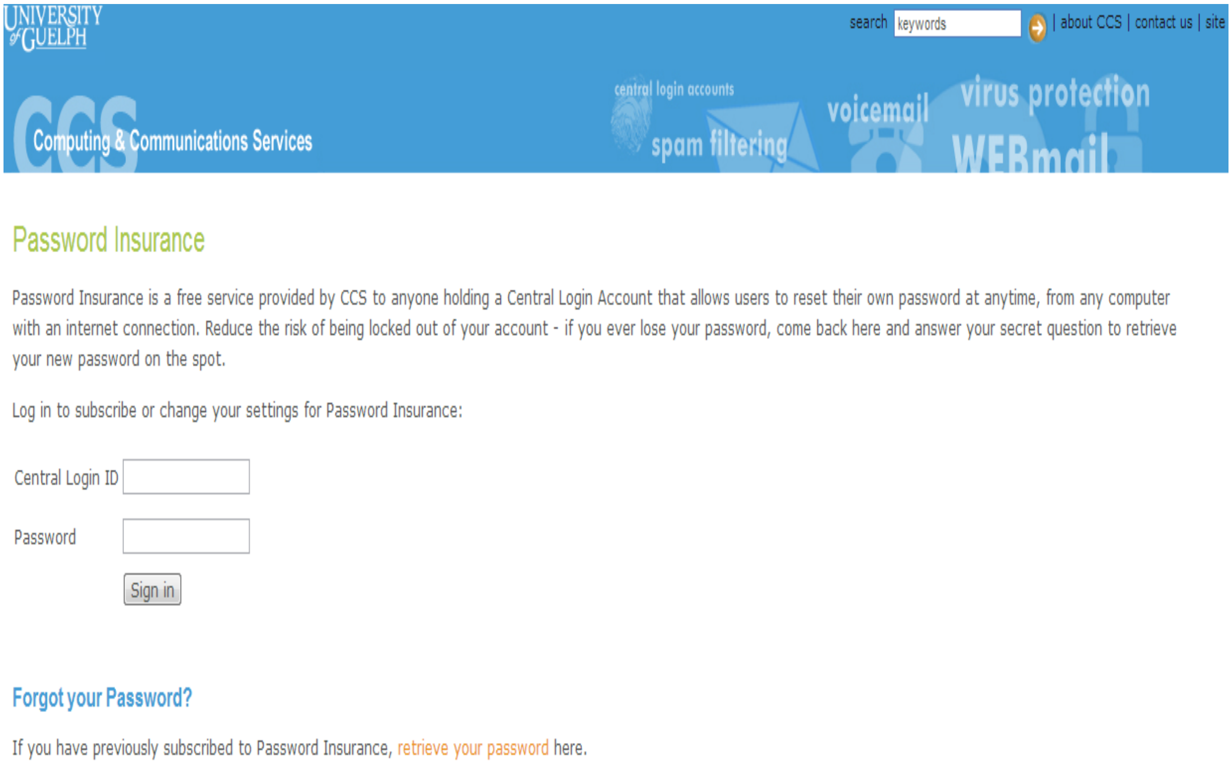
- *case-sensitive*
- *8 to 14 characters in length*
- *hard to guess by somebody else, but easy for user to remember so they don't have to write it down*
- *should not be a word that can be found in a dictionary of any language*
- *should include members of at least three groups of: capital letters, lower case letters, numbers, and simple punctuation or special characters such as $ ( ) ! + - _ . = { }*
- *please note that these characters are not allowed as they may be problematic for some applications: < > ' " ; , @ \ % & `*
- *should be changed regularly*

The initial password that is set during account creation is through a random password generator. There is no requirement that this password be changed during the first login or any subsequent logon and there is no enforcement of any password change requirement. It is important to note that the University's password policy and configuration requirements are designed in a manner that allows the passwords to be leveraged by both new and old systems deployed at the university. This means that many legacy systems may not be able to handle the strong password configurations supported by newer systems.

For changing users' passwords, the University's Computing and Communication Services (CCS) provides a free service called Password Insurance to anyone with a Central Login ID. Using Password Insurance, users can reset their passwords or retrieve forgotten passwords by answering a secret question at any time from any computer connected to the internet. For any queries or issues that cannot be handled by Password Insurance, users can contact the IT Help Desk for support and resolution. Password Insurance can, however, be used to reset / retrieve passwords only if the user had previously subscribed to Password Insurance. Where this is not the case, the user is required to contact the IT Help Desk. For undergraduate students who seek assistance from IT Help Desk for password resets, they must provide their student identification number and be prepared to answer a series of questions to confirm their identity prior to having their password reset. As similar process is followed for faculty, staff and graduate students that seek assistance from the IT Help Desk for password resets.

The Password Insurance home page with a link to retrieve password is shown in Figure 5:

[13] https://www.uoguelph.ca/ccs/apps/password/change/



Password Insurance

Password Insurance is a free service provided by CCS to anyone holding a Central Login Account that allows users to reset their own password at anytime, from any computer with an internet connection. Reduce the risk of being locked out of your account - if you ever lose your password, come back here and answer your secret question to retrieve your new password on the spot.

Log in to subscribe or change your settings for Password Insurance:

Central Login ID

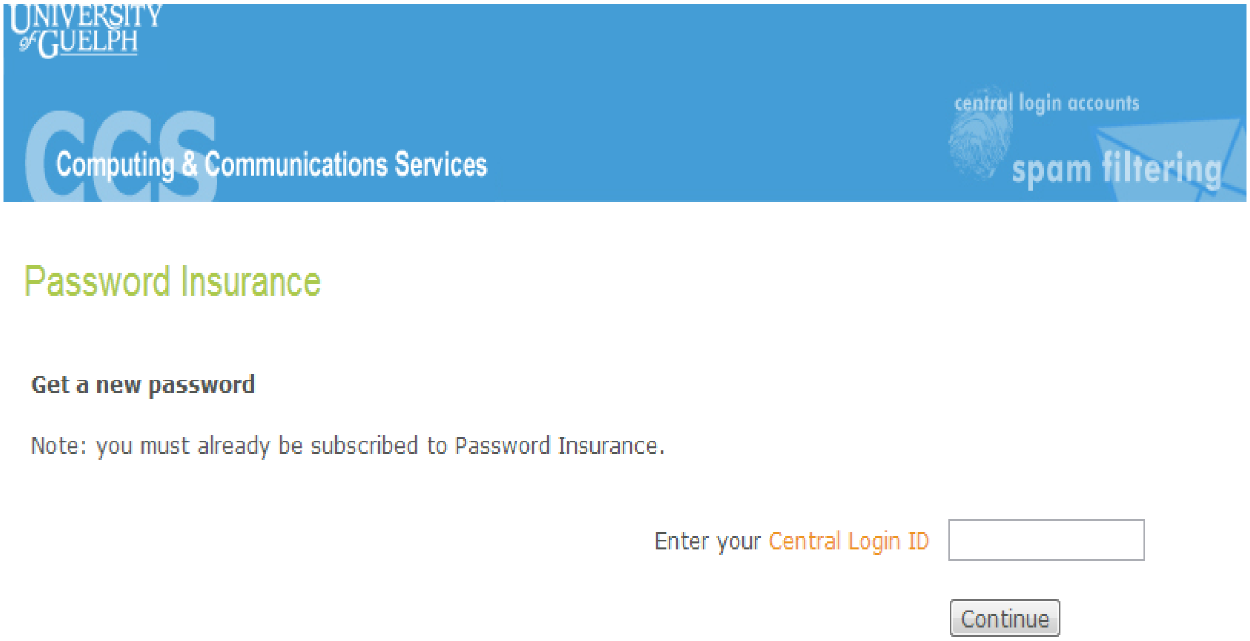
Password

Forgot your Password?

If you have previously subscribed to Password Insurance, retrieve your password here.

Figure 5: Change Password Webpage

The retrieve password page is shown in Figure 6:



Password Insurance

Get a new password

Note: you must already be subscribed to Password Insurance.

Enter your Central Login ID

Figure 6: Retrieve Password Webpage

The current password controls may not be sufficient to ensure adequate security. Legacy systems prevent the University from setting strong password controls. Though the initial password that is set during account creation is through a random password generator, there is no requirement that this password be changed during the first login and subsequently thereafter. This means that there is no enforcement of any password change requirement.

For the integration with Google, users will utilize their Central Login Account to access the Google application suite. Since, in this case the Identity Provider (IDP) and Service Provider (SP) are not in the same organization, a Federated Single Sign-On Solution (SSO) is required to be implemented. The University has implemented a Shibboleth Federated Single Sign-On[14] solution. The process is described in the Figure 7.

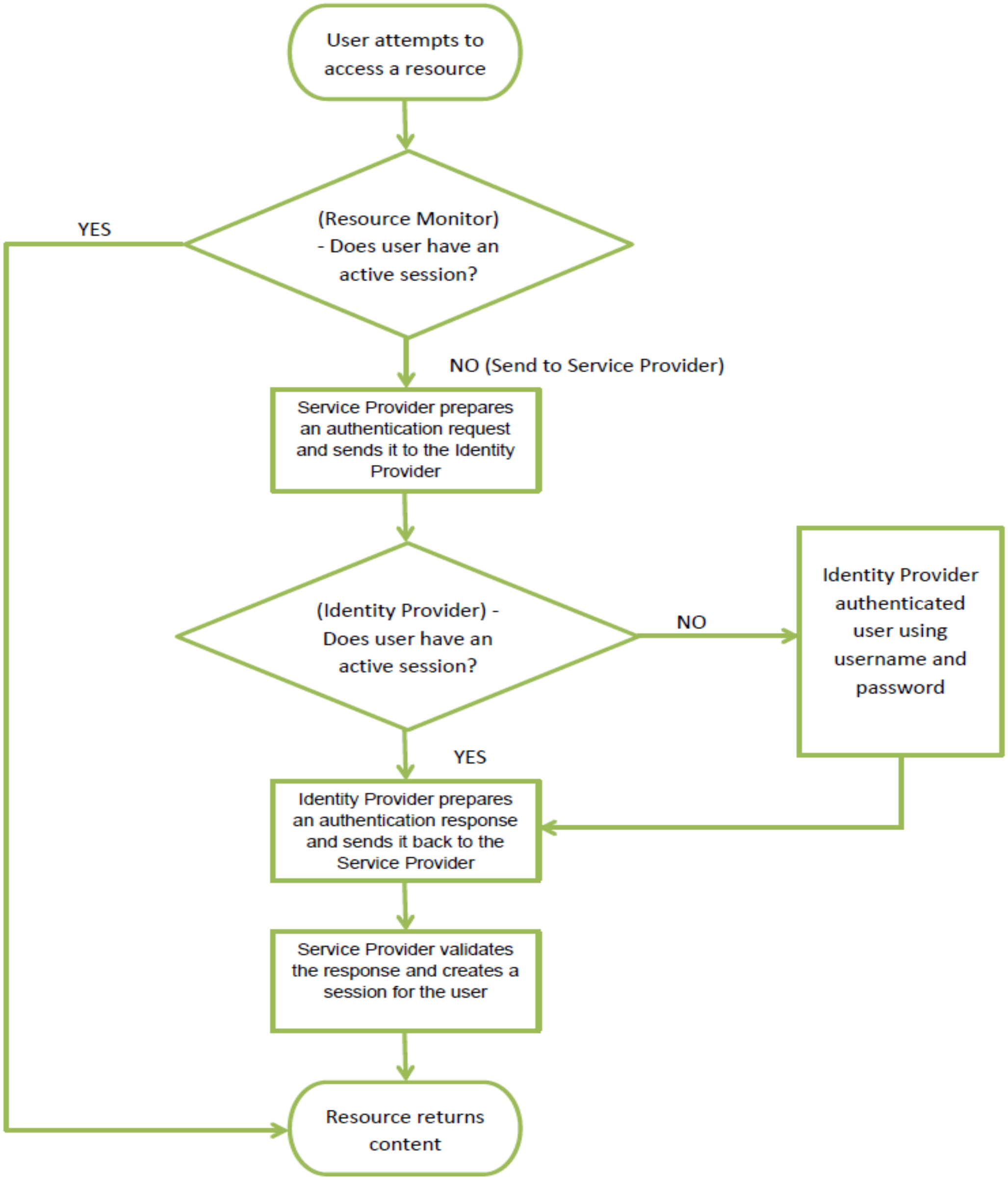

User attempts to access a resource
(Resource Monitor) - Does user have an active session?
YES
NO (Send to Service Provider)
Service Provider prepares an authentication request and sends it to the Identity Provider
(Identity Provider) - Does user have an active session?
NO
Identity Provider authenticated user using username and password
YES
Identity Provider prepares an authentication response and sends it back to the Service Provider
Service Provider validates the response and creates a session for the user
Resource returns content

Figure 7: Single Sign-On Solution

[14] http://shibboleth.net/about/basic.html

In this configuration, users do not have a password within the Google system by default, and are redirected to the University of Guelph IDP server if they do not have a valid session when they connect to the Google application site. In this configuration, all user authentications are provided by the University, and there is a trusted session established between Google and the University to ensure that it is not possible to bypass the authentication system. However, direct access via IMAP or POP3, for example (such as using the mail application in a mobile phone), require a user password to be set within Google to provide this access as SAML (Security Assertion Markup Language)[15] authentication is not supported. This can be done using the standard Google password settings, or by using a passkey generated by Google, similar to the process used for device access when using Google's two factor authentication (in this case, Google generates a 16 character passcode to be entered into the email client).

2.4 Safeguards and Controls provided by Google

The Google Apps for Education Agreement contains an exhibit entitled Security Standards that details the security safeguards that Google undertakes as part of the service provided to universities. This exhibit is summarized in the following sub-sections:

2.4.1 Physical Security

All Data Centers are equipped with a number of safety features to ensure proper protection. There is a round-the-clock security operation with CCTV monitoring and internal and external patrol of the premises. Access is regulated through electronic key access and biometric access control systems and alarms are installed to detect any unauthorized access. Formal procedures are laid out for key card requests which can only be made by Google employees and contractors. All such requests have to be made via email and must be approved by the requestor's manager and data center director. Only authorized Google employees, contractors and visitors are allowed to enter the data center. Every electronic key card use is monitored and recorded each time perimeter doors, shipping and receiving and other critical areas are accessed. All unauthorized and failed access attempts are logged and investigated. Access authorization is restricted based on zones and an individual's job responsibilities. Fire doors at the data center are alarmed.

2.4.2 Network Security

All customer data is transferred through Internet standard protocols and Data Centers are connected via high speed private links for fast and secure data transfer. Multiple layers of network devices and intrusion detection systems are used to protect Google's external attack surface and appropriate purpose built technologies are incorporated into external facing systems. Google's approach to intrusion detection and prevention involves tightly controlling the size and make-up of Google's attack surface through preventative measures, employing intelligent detection controls at data entry points and employing technologies that automatically remedy certain dangerous situations.

[15] https://developers.google.com/google-apps/sso/saml_reference_implementation

2.4.3 Logical Controls

Administrators and End Users must authenticate themselves via a central authentication system or via a Customer's SSO system in order to use the services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator. Internally, Google employs a centralized access management system to restrict personnel access to production servers and access is granted only to a limited number of authorized personnel. LDAP (Lightweight Directory Access Protocol)[16], Kerberos and a Google proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. Approvals are managed by workflow tools that maintain audit records of all changes. Google requires the use of unique user IDs, strong passwords; two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. Where passwords are employed for authentication at Google (e.g., login to workstations), password policies are followed that employ industry standard practices. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., Credit Card data), Google uses hardware tokens.

2.4.4 Data Security Controls

Customer Data is stored in a multi-tenant environment on Google-owned servers and replicated between geographically distributed data centers. Data of various end users is logically isolated at the application layer as well as on a per customer account basis. Disks containing customer data that are decommissioned (due to errors, hardware failure, etc.) are subject to a series of data destruction processes before being reused or destroyed. The data destruction process consists of a multi-step erase process post which it is verified by at least two independent validators. The erase results are then logged by the disk's serial number. If the disk cannot be erased, then it is stored securely until it can be destroyed.

2.4.5 Other Controls

The infrastructure systems are designed to prevent single points of failure by incorporating measures such as dual circuits, switches and networks that help provide redundancy. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures. Data Centers are provided with sufficient power back-up mechanisms. Uninterruptible power supply (UPS) batteries can provide up to 10 minutes of power supply during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. The standby Diesel Generator can take over if back-up power is required for a longer duration. Google servers use a Linux based implementation customized for the Google application environment and customer data is stored using Google proprietary algorithms to augment data security and redundancy.

Note: receipt and review of the third party auditor report on Google controls will enable the University to conduct a due diligence exercise on these controls.

[16] LDAP: Lightweight Directory Access Protocol is a protocol used to access and maintain information directories such as email addresses.

3 Data Flow Analysis

3.1 Description of Personal Information

The following table summarizes the collection, use, disclosure, storage and retention of personal information as it relates to the new student email service.

Table 2: Description of Personal Information

Description of Personal Information Element	Collected By	Format	Purpose of Collection	Used By	Disclosed To	Storage and Retention Site/Period
Username, first name, last name, password, and alias	The University Note: Username is also provided to Google via the University	Electronic	Provisioning of email accounts	The University	N/A	The University – retained for the life of the account
Username, first name, last name, contents of Email	Google via the University[17]	Electronic	Administration of email service on behalf of the University	Not specifically used by Google for Google's own purposes but rather as a service provider to the University	N/A	Google – As specified by the University (Note: to be determined through contract negotiation)

3.2 Collection and Use of Personal Information

The University will not be collecting additional personal information from students as part of the proposed new email solution. The University will be responsible for provisioning student email accounts as is currently the practice and hence will not be providing any information to Google for the same. Rather, Google, in its capacity as a service provider to the University will provide the following example services: email hosting and storage services, service trouble shooting, system maintenance, incident management notification, and monitoring for suspicious activities. This means that ownership of the email contents will remain with the University and any access by Google to student email accounts for the purposes of providing the hosted email service to the University is considered a use of personal information by Google as a service provider (as opposed to a disclosure by the University to Google or alternatively a collection by Google from the University). [18]

[17] Note: Per the contract with Google, Google is acting as a service provider to the University. As such, Google's receipt of/access to email contents is on behalf of the University and considered a "use" under FIPPA.

[18] Section 8.1 of the *Google Apps for Education 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*"

Should the University select the “split domain” option for accounts, the postmaster and abuse alias accounts, in addition to the University administrators, will also be monitored by Google[19], in order to, as indicated by Google “*properly address all reports of spam, abuse, and technical issues*”. If the University selects the single domain option, these accounts will go directly to the University and the University will determine if it will forward the accounts to Google.

Currently, if an email is sent to an email address in the @uoguelph.ca domain that does not exist, the email is bounced back and discarded. An email is then generated to the postmaster@uoguelph.ca indicating that an email was sent back to the sender. The University does not retain a copy of the email. With the proposed email solution, the same behaviour, with respect to emails sent to non-existent accounts in the domain, is expected to be followed.[20] Again, when performing this activity, Google is acting as a service provider and thus is accessing and using personal information on behalf of the university (i.e., no disclosure has taken place between the university and Google).

Google has indicated that there will be no advertising or secondary use of data by Google (for example data mining) to the University student accounts.[21] It is currently unknown to what extent secondary uses of personal information may occur once students graduate and their email accounts become Alumni accounts.

Through the Google Apps Admin Console, administrator privileges can be defined in several ways for the University email administrators and other IT staff.[22] The University 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 access the contents of the University email as a regular function of its services,[23] Google will scan email content for purposes such as spam filtering, anti-virus protection, or malware detection. In cases where the scans detect a potential threat, it has yet to be determined what Google will do with the email (e.g., whether it is captured and further analyzed). (Please refer to Section 4.5)

3.3 Disclosure of Personal Information

Current discussions indicate that the University does not anticipate any new disclosures of personal information as a result of the proposed email solution. However, disclosures by the University or Google may occur as required by law.[24]

[19] 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*.”

[20] Information gathering session with Identity Management and User Authentication team. December 16, 2013.

[21] Section 1.4 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*.”

[22] https://support.google.com/a/answer/172176?hl=en&ref_topic=2785005

[23] Section 7.1 of the *Google Apps for Education 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*.”

[24] Section 7.3 of the *Google Apps for Education 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*.

3.4 Retention and Disposition of Personal Information

The University has developed a Records Retention and Disposition Policy to establish a record retention system for the purposes of ensuring that all University Records are managed in accordance with acceptable Information and Document Management practices. The responsibility for maintaining a records retention program and coordinating the storage or retrieval of records is given to the University Records Management Coordinator.

All emails created using a University issued email account are considered a "business record" subject to FIPPA and thus must be managed in accordance with FIPPA requirements and established best practices. With respect to the service provided by Google, the University may terminate its agreement with Google with 30 days prior written notice.[25] Google indicates that if the University decides to discontinue its use of Google Apps, that there are several options for the migration of the University email data to another solution.[26] Specific contingencies for such a scenario are yet to be determined by the University.

The University has not yet determined for what period of time Google would retain University 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"[27] (Please refer to Section 4.1).

3.5 Sensitivity of Personal Information

The University indicates that there is sensitive personal information that is transmitted and received via student email accounts, although the University can only control what it specifically sends to students. Its email policy does prohibit the inclusion of sensitive personal information (e.g., SIN, health information, financial information as well as the Student ID) within emails or as attachments by faculty and staff. The following examples indicate the types of emails that are sent by faculty/staff to students:

- Campus Police/Parking Services: Notices regarding outstanding bills and appeals.
- The Registrar: Notices regarding important dates and key activities that students must complete. In addition, the Registrar sends out emails containing links to Institutional Research Survey (required for continued government funding).
- Financial Aid/Accounting: Notices regarding payment deadlines, and financial aid requests, information required to complete applications.
- Student Housing and Hospitality services: Use the My Housing Portal to communicate the majority of sensitive information to students although some sensitive is sent through email such as violation of residence contract (e.g. drug use, noise complaints, and sexual assault, some health information (e.g., when students request single rooms) and/or housing transfers.[28] (Please refer to section 4.7)

It is important to note that students often send sensitive personal information about themselves and/or their parents/guardians via email to the University administration in order to receive certain services/benefits (e.g., in order to process/receive student loans and bursaries).[29]

[25] Section 12.2 of the *Google Apps for Education Agreement* indicates "*Customer may terminate this Agreement for any reason (or no reason) with thirty days prior written notice to Google*."

[26] Section 12.3 (ii) of the *Google Apps for Education 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*"

[27] Section 12.3 (iii) of the *Google Apps for Education 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*"

[28] Information gathering meetings held on December 13 and 16, 2013.

[29] Information gathering meetings held on December 13 and 16, 2013.

4 Privacy Compliance Analysis

This chapter provides an analysis of the planned student email system against privacy legal requirements and regulatory best practices. It is intended to help guide immediate next steps with respect to Google contract negotiations as well as business and functional design requirements of the new platform. The chapter describes potential data privacy and security risks resulting from transition to the new email system and recommended course of action to mitigate such risks. The risk rating, mentioned within brackets beside each risk, is calculated based on the Impact and Likelihood for the respective risk and is appropriately color coded. For more information on ranking of risks, please refer to "*Appendix A – Risk Ranking Methodology*"

This chapter is organized around the 10 fair information practice principles defined under the CSA *Model Code for the Protection of Personal Information*; the principles upon which most privacy legislation built. Under each principle, Deloitte describes key activities and controls. Privacy risks and recommendations are identified and described within text boxes within each section, where applicable.

4.1 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* that was provided the University and will form the baseline from which the University will define points for its services negotiation with Google. Contract negotiations with Google are currently underway, and with a projected go-live date of fall 2014. The use of Google as a service provider will include the cross-border transfer of the University data, as Google indicates that the data will be processed in the "United States or any other country".

The University 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 the University 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 the University 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 *Google Apps for Education 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 the University should include in any agreement involving the management of personal information by a third party service provider, as well as a comparison to the current language in the agreement and addendum.

Table 3: Overview of privacy-related clauses

Ownership Ensure Google acknowledges that the personal information is the property of the University	The *Google Apps for Education Agreement* indicates that ownership of the email contents remains with the University. 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*". No action is recommended.
FIPPA Requirements Ensure Google acknowledges it will manage information in a manner that is consistent with the requirements of FIPPA.	Section 4 of the addendum (Acknowledgement Regarding FIPPA) alludes to the access to information provisions of FIPPA by stating that Google will "*utilize commercially reasonable efforts to provide Customer with timely access to End User Accounts and Customer Data*"; however, it does not include any language related to Google's adherence to FIPPA requirements, and in fact states "*Customer is responsible for evaluating whether use of the Services is consistent with its legal obligations under FIPPA*." Ideally there should be a clause that indicates that the use and management of personal information by Google would be consistent with the requirements of FIPPA. There is language in section 7.1 of the agreement that may be enough to satisfy these concerns, although it appears mostly silent on the University requirements or the actual use of the data by Google. 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*." Section 7.4 of the agreement indicates that Google will comply with the requirements of the *Family Educational Rights and Privacy Act* (FERPA), which is US legislation related to the privacy of education records. The requirements of FERPA are different than that of FIPPA, including the definition of educational records in FERPA with that of personal information in FIPPA. Ensuring that Google is treating information in accordance with FERPA is not the same as that of FIPPA. It is recommended the University review section 7.1 of the agreement and determine if it satisfies the University's understanding of its FIPPA requirements.

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 the University 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*. This may however not be completely satisfactory since some local laws may prevent timely notice being given about search and seizure. Section 213 of the USA PATRIOT Act for instance provides an explicit statutory authority for investigators and prosecutors to ask a court for permission to delay temporarily notice that a warrant has been executed. Documentation and notification quality may not contain the sufficient amount of information for Guelph. It is recommended that the University through its negotiations with Google explore if Google can provide an assurance that such non-notified search of University Data would not take place. If that is not possible, then the University should, along with its legal counsel, examine the acceptability of such an eventuality.
Security Ensure Google has implemented security controls that are in accordance with industry best practices	The addendum to the agreement includes ‘Exhibit: Security Standards’, which outlines Google Apps Security Standards, including those related to data center and network security, access and site controls, and data. Refer to recommendations with respect to breach notification and auditing below for specific risk mitigation activities as they relate to security.
Breach Notification Ensure Google promptly notifies the University of breaches that potentially affect the confidentiality or integrity of the University data.	Section 1 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*.” Based upon the clauses above, it is not known how long Google may take prior to notifying the University, or how long it will take to restore the reasonable integrity of the system. The University may wish to work with Google to identify specific timelines upon which breach notification is expected to be provided by Google to ensure that the University has adequate time to prepare for/respond to/manage certain breach activities, as required. Note: Deloitte recognizes that Google may not be willing to negotiate specific timelines. The University should also further define what type of support and when support is provided when University led activities require escalation to Google. It is also recommended that the University ensure that the security controls and metrics that are currently being monitored by the University remain in scope even after transition to the new system either by the University or by Google (e.g., through use of reporting metrics on malware, suspicious account activity). Finally, it is recommended that the University use this opportunity to formalize its own privacy breach management policy and procedure and communicate expectations around breach management to all

	faculty and staff.
Audit Ensure Google independently assesses its privacy and security on a regular basis, and the results of an audit are available to the University.	Exhibit: Security Standards of the addendum to the agreement include 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 its ISO/IEC 27001:2005 Certification or a comparable certification ("ISO Certification") for Google Apps Core Services. Google will update the Audit Report at least every eighteen (18) months.*" The Standard for Attestation Engagement 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. It is recommended that through its contract negotiations with Google, the University request to see the most current audit report for Google to ensure privacy and security has been appropriately considered. The University 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 Ensure protocols around the retention of personal information are well-defined and there are clauses to enable the termination of the relationship between the university and Google.	The University may terminate its agreement with Google with 30 days prior written notice. Section 12.2 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 the University decides to discontinue its use of Google Apps, that there are several options for the migration of the University's email data to another solution, Section 12.3 (ii) of the *Google Apps for Education 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*" The University has not yet determined for what period of time Google will retain the University data after the expiration of its agreement with Google; however, Google indicates that data would be overwritten within a "commercially reasonable period of time". Section 12.3 (iii) of the *Google Apps for Education 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.*" It is also not clear if Google will eventually delete the University data from its backup, cache and other non-active servers. Similarly, when a user account is deleted, the agreement does not provide any information regarding retention of data in such accounts. While Google's support page states that a deleted user account can be restored up to five days after deletion post which all data will be lost[30], the agreement does not include any clause to guarantee timely deletion and disposal of such data. It is recommended that the University through its negotiations with Google obtain a confirmation on the period of time Google will retain University data after expiration of the agreement or after deletion of a user account and that Google will delete University data from non-active servers as well.

[30] https://support.google.com/a/answer/33314?hl=en&ref_topic=4388359

In addition, once the new email service is live, University personnel may need to contact Google for resolution of issues both general service issues as well as issues relating to privacy and/or security controls. Such a process should be defined in the service level agreements (SLAs) with Google, defined through the Google contract. In the absence of a defined process for resolution of issues involving Google, the resolution of issues may take longer than necessary. The University's own help desk may also experience an increased volume of calls relating to a) the new platform, and b) the protection of personal information.

In the box below, Deloitte has identified the following risks and recommendations related to the execution of the Google agreement:

Privacy Risk and Recommendations

Risk:

1. There is a risk that the current agreement and addendum does not sufficiently mitigate potential privacy risks to a level that is acceptable to management. Although the agreement includes several important privacy-related clauses, it could be further strengthened, especially related to an acknowledgment of FIPPA requirements. (Moderate)

Recommendations:

a. The University should obtain further confirmation related to the disposition of the University data by Google upon expiration of the agreement or deletion of user accounts, specifically if data within backup, cache and other non-active servers will also be disposed, and what period of time would be considered "a commercially reasonable period of time".
b. Through its contract negotiations with Google, the University management in collaboration with legal counsel should determine the extent to which language in the current agreement covers these considerations or to the extent additional clauses are required.
c. Through its contract negotiations with Google, the University should identify specific timelines upon which breach notification is expected to be provided by Google to ensure that the University has adequate time to prepare for/respond to/manage certain breach activities, as required. The University should also further define what type of support and when support is provided when University led activities require escalation to Google.
d. It is also recommended that the University ensure that the security controls and metrics that are currently being monitored by the University remain in scope even after transition to the new system either by the University or by Google (e.g., through use of reporting metrics on malware, suspicious account activity).

Risk:

2. There is a risk that the current third party audit conducted on Google does not include appropriate privacy and security considerations. (Moderate)

Recommendations:

a. Through its contract negotiations with Google, the University should request to see the most current audit report for Google to ensure privacy and security has been appropriately considered.
b. The University should ensure a process is in place to receive and review updated audit reports throughout the life of the contract.

Risk:

3. There is a risk that, once the new email service is live, in the absence of a defined process for resolution of service issues (both general and pertaining to privacy / security controls) between the University and Google, the resolution of issues may take longer than necessary and might also lead to the University's help desk experiencing an increased volume of calls relating to a) the new platform, and b) the protection of personal information. (Low)

Recommendations:

a. It is recommended that the University identify key contacts at Google to whom issues may be escalated. The University may also need to increase its help desk services to end users throughout the transition period. (Also refer to recommendations associated with risk 4 below.)

4.2 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 the University 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. The University's notice to students regarding collection of personal information is contained in the Academic Calendar which serves as a contract with students. The notice regarding Collection, Use and Disclosure of Personal Information states:

"*Personal information is collected under the authority of the University of Guelph Act (1964), and in accordance with Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) http://www.e-laws.gov.on.ca/index.html. This information is used by University officials in order to carry out their authorized academic and administrative responsibilities and also to establish a relationship for alumni and development purposes. Certain personal information is disclosed to external agencies, including the Ontario Universities Application Centre, the Ministry of Training, Colleges and Universities, and Statistics Canada, for statistical and planning purposes, and is disclosed to other individuals or organizations in accordance with the Office of Registrarial Services Departmental Policy on the Release of Student Information.*

For details on the use and disclosure of this information call the Office of Registrarial Services at the University at (519) 824-4120 or see http://www.uoguelph.ca/registrar/registrar/index.cfm?index."[31]

Additionally, the University's notice statement is also made available on the University website and on specific data collection forms.

In the box below, Deloitte has identified the following risks and recommendations related to identifying principles:

Privacy Risk and Recommendation

Risk:

4. There is a risk that the current Privacy Notice statement to students may not appropriately inform students of how their personal information will be managed under the new email system, resulting in subsequent distrust or complaints related to the new email solution. (Low)

Recommendations:

a. The University should ensure that the Privacy Notice statement be further refined and updated to include:

  i. The potential uses of student email data by Google (this still needs to be confirmed by the University as further discussed in to Section 3.5)

  ii. That all email sent to the abuse and postmaster aliases, will also be monitored by Google (subject to domain approach selected by the University)

  iii. The retention of data by Google (this still needs to be confirmed by the University

[31] http://www.uoguelph.ca/registrar/calendars/undergraduate/current/pdffiles/calendar.pdf

as further discussed in Section 3.5)

iv. The contractual safeguards that the University has implemented between itself and Google

b. The University should also explore posting the Privacy Notice statement on the login page of the new email service, so that it is easily accessible and available to Students.

c. Finally, to help mitigate concerns around the use of a service provider where personal information is hosted / stored outside of Canada, it is recommended that the University implement a communications plan that includes that describes Google's role, the oversight of Canadian and US laws, and the safeguards/due diligence undertaken by the University to protect personal information. This information should be made available in multiple mediums, including: the Student Association website, main University website, and through faculties, the administration and the Privacy Office.

d. The University should draft a statement explaining that student data might be processed outside Canada, describing the associated risks and obtain explicit consent from Students before transitioning them to the new system.

.

4.3 Consent

Privacy Principle:

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

The University has indicated that all undergraduate student accounts will be transitioned to the new system. As part of agreeing to the conditions of admission/enrolment at the University, the student has also agreed to provide the University with the information necessary to provision and administer the university email service. However, with the new system student data will be stored and processed outside Canada, As such, it is important that the University ensure its privacy notices (i.e., notice of collection) include an adequate level of description relating to its student email service (refer to section 4.3 above).

4.4 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.

The University will not be collecting additional personal information from students as part of the proposed new email solution. Since the University will be responsible for provisioning the user accounts as is the practice currently, there is no need for the University to provide any information to Google for this purpose. As such, Google will be acting as a service provider to the University. This means that ownership of the email contents will remain with the University and any access by Google to student email accounts for the purposes of providing the hosted email service to the University is considered a use of personal information by Google as a service provider (as opposed to a disclosure by the University to Google or alternatively a collection by Google from the University). [32]

Refer to recommendation 4 under Notice with respect to expanding the current notice statement to include services provided by Google.

[32] Section 8.1 of the *Google Apps for Education 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*"

4.5 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 contents of the University's 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.
- While the abuse and postmaster alias accounts will be monitored by the University's email administrator under the proposed email solution, all email sent to these email addresses may also be monitored by Google[33], in order to, as indicated by Google, "*properly address all reports of spam, abuse, and technical issues*". (Refer to Section 3.2 for additional commentary.)

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.

In the box below, Deloitte has identified the following risks and recommendations to limiting use, disclosure and retention of personal information:

Privacy Risk and Recommendation

Risk:

5. There is a risk that the scanning of email content by Google may include the use or retention of personal information that is not consistent with the requirements of FIPPA. Furthermore, without knowing the specific details of how data related to the scanning process will be managed, the University cannot adequately inform students of how their data will be managed under the new email solution. (Moderate)

Recommendation:

a. Through its contract negotiations with Google, the University should ensure it a) understands Google's management of email content for those mails determined to be a potential threat, b) feels the approach provides adequate privacy and security coverage, and c) includes the necessary reporting clauses to the University around, for example, frequency of occurrence, and activities to contain and mitigate issues (be it isolated or systemic).

Google has indicated that there will be no advertising or secondary use of data by Google (for example data mining) related to current University student accounts.[34] The terms of the Apps for Education agreement related to the information in a student's email account remains in effect even after a student has graduated.

[33] 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*."

[34] Section 1.4 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*."

Google indicates that if the University decides to discontinue its use of Google Apps, that there are several options for the migration of the University's email data to another solution. Section 12.3 (ii) of the *Google Apps for Education 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*". The University has not yet determined for what period of time Google will retain the University data after the expiration of its agreement with Google, as Google only indicates that data will be overwritten "within a *commercially reasonable period of time"*.

4.6 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.

No risks or recommendations were identified relating to accuracy of personal information.

4.7 Safeguards

Privacy Principle:

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

The addendum to the agreement includes 'Exhibit: Security Standards', which outlines Google Apps Security Standards, including those related to data center and network security, access and site controls, and data. Based on the review of this documentation, Google's security standards meet or exceed University requirements for the protection of personal information.

As it relates to the emailing of sensitive personal information via email (in body or within an attachment), the consultants found that there are some instances where such information is being emailed by staff to students. On the one hand, it is not possible to control what students send via email to faculty/staff, however, there is an opportunity to better control for what faculty/staff send to students. While the university does inform students that the use of email is an unsecure means of communication (e.g., within the "*Steps to Protect One's Techno-privacy"*[35] article) there is no formal guideline/best-practice document on email use and etiquette. Also, the University has not instituted an encryption policy/solution for emailing. Note: it is understood that such a tool would be most effective for faculty/staff – to – faculty/staff emailing.

With respect to managing Google email accounts, the University will need to specify one or more administrators responsible for managing these end-user accounts. Such Administrators may have the ability to access, monitor, use and disclose data available within the accounts. As such, it is important that the University implement controls to monitor/audit administrator accounts in order to identify and/or mitigate intentional or unintentional data breaches. The University should consider leveraging current monitoring processes in place under the Zimbra system.

Because the University will be splitting student email from staff and faculty, a mechanism must be in place to sort incoming email to the correct server. If a single domain is maintained, additional information needs to be saved for each user in the University's LDAP directory so that the primary Cisco Ironport gateway can properly route email between the staff/faculty server and the Google servers. To minimize configuration errors that could lead to mis-routed email, it is recommended to use a different DNS domain for student email addresses when they are moved to Google mail.

[35] The document can be found at: http://www.uoguelph.ca/secretariat/technoprivacy/

Finally, whether or not the University updates its password security requirements for the central ID, these password requirements may not be duly enforced via Google. This means that a student could use a simple password when accessing email via a mobile device (e.g., phone, iPad) and in turn, the student's account may be more susceptible to hacking.

In the box below, Deloitte has identified the following risks and recommendations safeguarding personal information:

Privacy Risk and Recommendation

Risk:

6. There is a risk that the University staff and faculty are sending emails to students that contain personal information. (Moderate)

Recommendation:

a. Given the potential sensitivities related to the use of Google as a service provider, the University should ensure faculties and administrative units review their email practices.
b. For more sensitive personal information, the University should ensure these data elements are not communicated through email unless they have been appropriately encrypted.
c. The University should develop an email best practices guideline detailing the dos and don'ts of email use to ensure safety of personal information. These guidelines should be readily available to students and faculty and form part of the overall email transition communications plan.

Risk:

7. There is a risk of intentional or unintentional breach by administrators with access to End User Data. (Low)

Recommendation:

a. It is important to note that the risks posed by administrators are likely the same under the Google system as with the Zimbra system. As such, it is recommended that the University follow its current protocols when verifying the credentials and credibility of the Administrators, providing them with frequent and periodic training about security best practices, and auditing their work routinely to detect any inadequacies so that a resolution may be found before there is an incident.

Risk:

8. Password security controls are not currently enforced when a student sets-up email access via a mobile device (e.g., phone, iPad). (Moderate)

Recommendation:

a. Because device and application access requires a password to be set within Google Apps itself, strong password requirements should be set within the Google administration interface.

Risk:

9. There is an increased risk that emails may be misrouted depending on the type of domain configuration the University selects (i.e., single domain vs. two domains). As a result, the University could see an increase unauthorized disclosure of personal information. (Moderate)

Recommendation:

a. It is recommended that the University utilize separate domains to reduce the risk of misconfiguration or provisioning errors which would result in mis-routed email and possible personal information disclosure.

4.8 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 the University are available through the University website[36] and through the University Privacy Policy.[37] Further details regarding management of personal information of students is also available in the Academic Calendars which serves as a contract with the students. A key consideration for this initiative is providing students information on the nature of the relationship between the University and Google, and how Google will manage their personal information as a service provider acting on behalf of the University. Refer to recommendation 3 above for information on updates to the University Notice statements and a communications plan.

The implementation of a new email solution for students should not require any changes to the University's current Directory of Records.[38]

4.9 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 the University related to their email account and user identity, which the University would be able to provide, although such a scenario is unlikely given the student would already know these elements.

Emails sent from a student account to an University faculty or administration will 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.

No privacy risks or recommendations were identified relating to individual access.

4.10 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 University Secretary/CPO and/or the Information and Privacy Coordinator. Contact information for the Secretary and Coordinator are available through the University website[39]. 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 the University and Google, Exhibit: Security Standards 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*

[36] http://www.uoguelph.ca/secretariat/privacy/

[37] http://www.uoguelph.ca/info/privacyguidelines/ProtectionofPrivacyandAccesstoInformation.pdf

[38] https://www.uoguelph.ca/secretariat/offices/bog/directory-records-and-personal-information-banks-–-function

[39] https://www.uoguelph.ca/secretariat/offices/bog/questions-about-access-information-or-protection-privacy

report or a comparable report ("Audit Report") and its ISO/IEC 27001:2005 Certification or a comparable certification ("ISO Certification") for Google Apps Core Services. Google will update the Audit Report at least every eighteen (18) months"

In the box below, Deloitte has identified the following risks and recommendations related to challenging compliance:

Privacy Risk and Recommendation

Risk:

10. There is a risk that the current third party audit conducted on Google does not include appropriate privacy and security considerations. (Moderate)

Recommendation:

a. Through its contract negotiations with Google, the University should request to see the most current audit report for Google to ensure privacy and security has been appropriately considered. The University should ensure a process is in place to receive and review updated audit reports throughout the life of the contract.

5 Recommendations Roadmap

Based on the risk findings and recommendations above, Deloitte has provided a recommendations roadmap below. This roadmap is designed to assist the University in appropriately planning its mitigation activities by identifying those that should be completed in the shorter-term (i.e., those directly associated with the Google contract negotiations) vs. those that can be completed in preparation for go-live (i.e., those associated with establishing the email service configuration, operational environment or communications to faculty/staff/students).

The table below describes the recommendation and suggested timelines for the same:

Table 4: Recommendations Roadmap

#	Privacy Risk	Recommendation	Timelines for implementation
1	There is a risk that the current agreement and addendum does not sufficiently mitigate potential privacy risks to a level that is acceptable to management. Although the agreement includes several important privacy-related clauses, it could be further strengthened, especially related to an acknowledgment of FIPPA requirements. (Moderate)	- The University should obtain further confirmation related to the disposition of the University data by Google upon expiration of the agreement or deletion of user accounts, specifically if data within backup, cache and other non-active servers will also be disposed, and what period of time would be considered "a commercially reasonable period of time". - Through its contract negotiations with Google, the University management in collaboration with legal counsel should determine the extent to which language in the current agreement covers these considerations or to the extent additional clauses are required. - Through its contract negotiations with Google, the University should identify specific timelines upon which breach notification is expected to be provided by Google to ensure that the University has adequate time to prepare for/respond to/manage certain breach activities, as required. The University should also further define what type of support and when support is provided when University led activities require escalation to Google. - It is also recommended that the University ensure that the security controls and metrics that are currently being monitored by the University remain in scope even after transition to the new system either by the University or by Google (e.g., through use of reporting metrics on malware, suspicious account activity).	Short term (0-3 months)
2	There is a risk that the current third party audit conducted on Google does not include appropriate privacy and security considerations. (Moderate)	- Through its contract negotiations with Google, the University should request to see the most current audit report for Google to ensure privacy and security has been appropriately considered. - The University should ensure a process is in place to receive and review updated	Short term (0-3 months)

		audit reports throughout the life of the contract.	
3	There is a risk that, once the new email service is live, in the absence of a defined process for resolution of service issues (both general and pertaining to privacy / security controls) between the University and Google, the resolution of issues may take longer than necessary and might also lead to the University's help desk experiencing an increased volume of calls relating to a) the new platform, and b) the protection of personal information. (Low)	- It is recommended that the University identify key contacts at Google to whom issues may be escalated. The University may also need to increase its help desk services to end users throughout the transition period. (Also refer to recommendations associated with risk 4 below.)	Short term (0-3 months)
4	There is a risk that the current Privacy Notice statement to students may not appropriately inform students of how their personal information will be managed under the new email system, resulting in subsequent distrust or complaints related to the new email solution. (Low)	- The University should ensure that the Privacy Notice statement be further refined and updated - The University should also explore posting the Privacy Notice statement on the login page of the new email service, so that it is easily accessible and available to Students. - To help mitigate concerns around the use of a service provider where personal information is hosted / stored outside of Canada, it is recommended that the University implement a communications plan that includes that describes Google's role, the oversight of Canadian and US laws, and the safeguards/due diligence undertaken by the University to protect personal information. This information should be made available in multiple mediums, including: the Student Association website, main University website, and through faculties, the administration and the Privacy Office. - The University should draft a statement explaining that student data might be processed outside Canada, describing the associated risks and obtain explicit consent from Students before transitioning them to the new system.	Medium term (3-6 months)
5	There is a risk that the scanning of email content by Google may include the use or retention of personal information that is not consistent with the requirements of FIPPA. Furthermore, without knowing the specific details of how data related to the scanning process will be managed, the University cannot adequately inform students of how their data will be managed under the new email solution (Moderate)	- Through its contract negotiations with Google, the University should ensure it a) understands Google's management of email content for those mails determined to be a potential threat, b) feels the approach provides adequate privacy and security coverage, and c) includes the necessary reporting clauses to the University around, for example, frequency of occurrence, and activities to contain and mitigate issues (be it isolated or systemic).	Short term (0-3 months)
6	There is a risk that the University staff and faculty are sending emails to students that contain personal information. (Moderate)	- Given the potential sensitivities related to the use of Google as a service provider, the University should ensure faculties and administrative units review their email practices. - For more sensitive personal information, the University should ensure these data elements are not communicated through email unless they have been appropriately encrypted. - The University should develop an email best practices guideline detailing the dos and don's of email use to ensure safety of personal information. These guidelines should be readily available to students and faculty and form part of the overall	Medium term (3-6 months)

			email transition communications plan.	
7	There is a risk of intentional or unintentional breach by administrators with access to End User Data. (Low)	-	It is important to note that the risks posed by administrators are likely the same under the Google system as with the Zimbra system. As such, it is recommended that the University follow its current protocols when verifying the credentials and credibility of the Administrators, providing them with frequent and periodic training about security best practices, and auditing their work routinely to detect any inadequacies so that a resolution may be found before there is an incident.	
8	Password security controls are not currently enforced when a student sets-up email access via a mobile device (e.g., phone, iPad). (Moderate)	-	Because device and application access requires a password to be set within Google Apps itself, strong password requirements should be set within the Google administration interface.	Medium term (3-6 months)
9	There is an increased risk that emails may be misrouted depending on the type of domain configuration the University selects (i.e., single domain vs. two domains). As a result, the University could see an increase unauthorized disclosure of personal information. (Moderate)	-	It is recommended that the University utilize separate domains to reduce the risk of misconfiguration or provisioning errors which would result in mis-routed email and possible personal information disclosure.	Short term (0-3 months)
10	There is a risk that the current third party audit conducted on Google does not include appropriate privacy and security considerations. (Moderate)	-	Through its contract negotiations with Google, the University should request to see the most current audit report for Google to ensure privacy and security has been appropriately considered. The University should ensure a process is in place to receive and review updated audit reports throughout the life of the contract.	Short term (0-3 months)

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.

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.

Impact

The impact to the University 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	**Moderate**	**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.[40] 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*."

Acronyms

CTO	Chief Technology Officer
FIPPA	Freedom of Information and Protection of Privacy Act
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

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

Appendix C - Supplementary Documents List

Google Agreements

- Apps for Education
- University of Guelph - Addendum

Documents Related to University of Guelph Policies and Procedures

- Protection of Privacy and Access to Information at Guelph: http://www.uoguelph.ca/info/privacyguidelines/ProtectionofPrivacyandAccesstoInformation.pdf
- Acceptable Use Policy and Guidelines: http://www.uoguelph.ca/web/aupg/
- Software as a Service Enterprise Guidelines: https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/Software-as-a-ServiceEnterpriseGuidelines.pdf
- Policy on Release of Student Information: http://www.uoguelph.ca/policies/pdf/ORSInfoReleasePolicy060610.pdf
- Record Retention and Disposition Policy: http://www.uoguelph.ca/policies/pdf/Record%20Retention%20and%20Disposition%20Policy.pdf
- Departmental Privacy Policies: https://www.uoguelph.ca/secretariat/offices/bog/privacy-policies
- Mass Electronic Mail Policy: http://www.uoguelph.ca/info/massemail/
- Guidelines on making an Information Request under FIPPA: https://www.uoguelph.ca/secretariat/offices/bog/how-make-information-request-under-fippa
- Guidelines on making a privacy complaint: https://www.uoguelph.ca/secretariat/offices/bog/how-make-privacy-complaint
- End-Point Encryption Policy: http://www.uoguelph.ca/cio/content/end-point-encryption-policy
- Academic Calendar: http://www.uoguelph.ca/registrar/calendars/
- Information Technology Security Policy Framework: https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/CIO-ITSecurity-00-PolicyFramework-2009Approved_0.pdf
- Information Technology Security Program: https://www.uoguelph.ca/cio/content/it-security-program
- Major IT Security Management Policy: https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/CIO-ITSecurity-09.1-MajorIncidents-Approved-2011MAY_0.pdf

- IT Contracting Guidelines:
  https://www.uoguelph.ca/cio/content/it-contracting-guidelines
- External Contracting Guideline and sample:
  https://www.uoguelph.ca/cio/sites/uoguelph.ca.cio/files/CIO-Guidelines-ContractGuidelines.pdf

Documents Related to University of Guelph Deployment

- Project Plan

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

- IT Security (Garret Bos and Fazil Rasheed)
- CCS IT Help Desk (Brian Thomson, Vince Tan, Jill Hogg)
- CCS [Access Control and Networks] (Tom O'Hare, Leon Loo, Leo Song)
- CCS [Identity Management / User Authentication] (Hugh Smith, Matt Searle, Zdenek Nejedly)
- AVP institutional research and planning; Registrar (Brian Pettigrew)
- Associate, Registrar [Admission Services domestic/international students] (Deanna McQuarrie)
- Associate, Registrar [Enrollment Services] (Sharon Anthony)
- Associate, Registrar [Student Financial Services] (Manuela Sheehy)
- Student Housing; IS Manager (Nathan Griff)
- Student Housing; Research and Special Projects (Julie West)
- Privacy Officer (Gen Gauthier)
- Project Sponsor/Manager (Gayleen Gray)
- CIO (Rebecca Graham)`
- Students Association (Julia Forrester, Chris Archibald)
- Manager of Applications and Integration (Fazil Rasheed)
- Student Services (Shannon Thibideau)
- Associate VP, Student Services (Brenda Whiteside)
- Director, Campus Police (Robin Begin)

Appendix E - Additional Documents

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.

University of Guelph Acceptable Use Policy for Information Technology

1. Purpose and Jurisdiction

The purpose of this policy is to define the acceptable use of Information Technology (IT) Resources in support of the mission of the University of Guelph. It builds on the principles of accountability, transparency, privacy, and fairness, to support a functional environment for work and study in which these resources are protected. This policy applies to anyone who uses or accesses any IT Resource belonging to, under the control or in the custody of, the University of Guelph.

2. Definitions

For the purposes of this policy, the following terms are defined as follows:
Account – includes any username, access code, password, PIN, token, credential, or other authentication which has been assigned to Authorized Users to use any University IT Resource.
Authorized – means specific access rights granted in accordance with University governance or policies.
Authorized User – means a member of the University of Guelph community, who is an employee, student, alumni, associate, or other individual who has been granted specific rights by a University signing officer, or someone delegated in accordance with University governance or policies to use any University IT Resource.
Community Standards – means behaviour or material which the average member of the University Community would reasonably tolerate.
Information Technology (IT) Resource – means any information, data, software, hardware, system, or network belonging to, under the control or in the custody of the University, regardless of who administers it.

Information Technology (IT) Security Officer – means the University employee or designate who is responsible for enforcing the Acceptable Use Policy
Personal Information – means recorded information about an identifiable individual, and as defined in federal and provincial privacy legislation
System Administrator – means an individual responsible and authorized to establish or maintain and provide technical support for a University IT Resource.

3. Acceptable Use

The University of Guelph authorizes the University community to use its Information Technology Resources to fulfill and advance the University's teaching, learning, research, service, administrative, and community development missions.

In addition, the University permits limited personal use of these resources, provided this use does not violate any law, statute, or University policy. Users who require a private means of computing and sending electronic communications should utilize a personal device unconnected to the University's IT network**.**

The University respects the privacy of all users of its IT Resources, and uses reasonable efforts to maintain confidentiality of Personal Information. Circumstances may arise in which such privacy cannot be maintained. Such circumstances include, but are not limited to:

1. Access to Personal Information may be granted to an Authorized User, System Administrator or agent to meet legitimate University business needs and operational requirements, or in the event that an Authorized User is unavailable, or has his or her access revoked.
2. The University may audit, access or restore any IT resource within its environment when it has reasonable grounds to suspect a breach of acceptable use or a possible violation of any law or University policy.

Such access will be subject to the authorization of the appropriate Vice-President (or designate) in consultation with the Provost.

Authorized Users must exercise good judgment in determining what is acceptable use of IT Resources with due regard to this policy, other University policies and Community Standards. Some activities may be appropriate in a specific context (e.g. for authorized academic and research purposes), while some are not appropriate in any context.
Authorized Users have an obligation to take all reasonable steps (e.g. password protection and strengthening) to protect the confidentiality, integrity, and availability of IT Resources and report encountered vulnerabilities to the Information Technology Security Officer. Failure to do so may constitute a breach of this policy.

Examples of a Breach of Acceptable Use

Unless explicitly authorized, a breach of acceptable use includes, but is not limited to:

1. Allowing others to access your assigned personal Account
2. Failure to exercise reasonable care in safeguarding Accounts and information
3. Accessing someone else's personal Account
4. Seeking information on passwords or information belonging to others
5. Breaking or attempting to circumvent licensing or copyright provisions
6. Copying, deleting, intercepting, or examining someone else's files, programs, or information
7. Attempting to collect, use, or disclose, the Personal Information of others
8. Using IT resources to harass or bully others
9. Attempting to circumvent information security provisions or exploit vulnerabilities
10. Using IT Resources (e.g. University computing account or workstation) for unauthorized commercial purposes
11. Any interference with the ability of others to use IT Resources whether it is disruptive or not
12. Falsifying or misrepresenting your identity
13. Viewing or using pornographic or offensive material in a work, study, or public location
14. Distributing or disseminating pornographic or offensive material in any location

4. Outcomes

If the integrity or security of an IT Resource is compromised or at risk the Information Technology (IT) Security Officer may direct the locking or quarantining of an Account or resource at his or her sole discretion. Upon reasonable belief by the IT Security Officer that a violation of this policy (AUP) may have occurred, the IT Security Officer or designate will conduct an investigation.

If access to any Personal Information is required, authorization will be requested of the appropriate Vice-President (or designate) in consultation with the Provost.

If insufficient evidence of a violation of the AUP is found, the investigation will be closed and involved parties notified where appropriate.

The IT Security Officer will issue a written decision regarding the alleged policy violation within a reasonable timeframe, normally 30 days. Actions noted below may be initiated upon determination of a violation of this policy.

An Authorized User affected by this decision may file an appeal to the Chief Information Officer (CIO). The Authorized User will have 10 calendar days from the issuance of a written decision to file an appeal with the CIO. The CIO may confirm, rescind, or modify the decision. The decision of the CIO is considered final**.**

If a violation is determined to have occurred, the following actions may be initiated by the IT Security Officer:

Class or severity	**Possible outcomes**
Minor violation of the AUP	Warning
Serious or repeated violation of the AUP	Escalation to appropriate authority or disciplinary process and/or restrictions on access or use
Possible violation of another University policy or regulation	Forward for investigation by applicable process under the applicable policy or regulation
Possible violation of federal, provincial, or municipal law or statute	Forward for investigation to Campus Community Police

5. Related University Policies

This Acceptable Use Policy prohibits any use of IT Resources which potentially violates any other University of Guelph policy, code or agreement, constitutes academic or non-academic misconduct, or which violates federal, provincial, or municipal laws or regulations.

In addition to outcomes under the AUP, such violations may be prosecuted under those laws and policies. Any information resulting from an investigation under the AUP may be shared for the purposes of such prosecutions.

Some of these policies include:

- Human Rights Policy
- Graphics Standards Guide
- Mass Electronic Mail Policy
- Protection of Privacy and Access to Information
- Release of Student Information
- Residence Community Living Standards
- Student Rights and Responsibilities
- University Undergraduate or Graduate Calendars
- Human Resources Policies
- Collective Agreements or other Employment Agreements

A more comprehensive list of applicable University policies is maintained by the University Secretariat at http://www.uoguelph.ca/policies/.

6. Departmental AUPs

Departments may have Departmental Acceptable Use Policies to meet their specific operational requirements. An Authorized User using Departmental IT Resources is bound by the Departmental AUP. In the event of a conflict between the Departmental AUP and this policy, this policy prevails.

Essential Components of Departmental AUPs are:

1. A copy of the Departmental AUP must be available to all employees of that department
2. Definition or description of Departmental IT Resources which the Departmental AUP applies to
3. One or more locations where the current University and departmental AUPs may be found.
4. List of user responsibilities and expectations specific to the use of Departmental IT Resources with clear examples of unacceptable actions of activities
5. An indication of actions and examinations considered routine with regard to Departmental IT Resources
6. How suspected violations of the Departmental AUP are handled
    a. Department Chair for violations specific to the Departmental AUP
    b. IT Security Officer for issues related to the University AUP
7. The circumstances under which accounts or access to Departmental IT Resources is terminated or restricted

Any Departmental AUP will be submitted for review to the Chief Information Officer or designate prior to implementation. Review will be completed within a reasonable timeframe, normally 30 days.

For additional information regarding Google Apps for Education, please visit the following website: http://www.google.com/apps/intl/en/edu/university.html.